




**User manual**



**M!DGE3**  
**GPRS/UMTS/HSPA+/LTE**  
**router**


**Quick start**



**Hardware**



**Configuration**



**Parameters**



**fw 2.1.0.0**  
2023-07-28  
version 1.04



---

## Table of Contents

|  |    |
|--|----|
| Important Notice .....   | 7  |
| 1. Quick guide .....   | 8  |
| 2. Product .....   | 10 |
| 2.1. Dimensions .....  | 11 |
| 2.2. Connectors .....  | 13 |
| 2.3. Indication LEDs .....   | 20 |
| 2.4. Extension .....   | 22 |
| 2.5. Ordering codes .....  | 23 |
| 3. Accessories .....   | 25 |
| 4. Installation .....  | 26 |
| 4.1. Step-by-step checklist .....                                  | 26 |
| 4.2. Minimal required settings to set-up cellular connection ..... | 26 |
| 4.3. Mounting .....  | 27 |
| 4.4. Antenna installation .....                                    | 30 |
| 4.5. Antenna feed line .....                                       | 30 |
| 4.6. Grounding .....   | 30 |
| 4.7. Connectors .....  | 31 |
| 4.8. Power supply .....  | 31 |
| 5. MIDGE3 in detail .....  | 32 |
| 5.1. Combination of IP and serial communication .....              | 32 |
| 5.1.1. Detailed Description .....                                  | 32 |
| 6. Web interface .....   | 33 |
| 6.1. Supported web browsers .....                                  | 34 |
| 6.2. Changes to commit .....                                       | 35 |
| 6.3. Notifications .....   | 37 |
| 6.4. User menu .....   | 38 |
| 6.5. Remote access .....   | 38 |
| 6.6. Refresh settings .....  | 39 |
| 6.7. Status overview .....   | 40 |
| 6.8. Help .....  | 40 |
| 6.9. Shortcuts .....   | 41 |
| 7. Settings .....  | 42 |
| 7.1. Interfaces .....  | 42 |
| 7.1.1. Ethernet .....  | 42 |
| 7.1.1.1. Network interfaces .....                                  | 42 |
| 7.1.1.2. Ports .....   | 44 |
| 7.1.2. COM .....   | 45 |
| 7.1.2.1. COM port parameters .....                                 | 45 |
| 7.1.2.2. Common Protocol parameters .....                          | 47 |
| 7.1.2.3. Individual protocol parameters .....                      | 49 |
| 7.1.2.3.1. None .....  | 50 |
| 7.1.2.3.2. Async link .....  | 50 |
| 7.1.2.3.3. COMLI .....   | 50 |
| 7.1.2.3.4. DNP3 .....  | 52 |
| 7.1.2.3.5. DF1 .....   | 52 |
| 7.1.2.3.6. IEC101 .....  | 54 |
| 7.1.2.3.7. Mars-A .....  | 54 |
| 7.1.2.3.8. Modbus RTU .....  | 55 |
| 7.1.2.3.9. PR2000 .....  | 56 |
| 7.1.2.3.10. Siemens 3964(R) .....                                  | 57 |
| 7.1.2.3.11. SAIA S-Bus .....                                       | 59 |

|  |     |
|--|-----|
| 7.1.2.3.12. RDS .....                              | 61  |
| 7.1.2.3.13. UNI .....                              | 62  |
| 7.1.3. Terminal servers .....                      | 64  |
| 7.1.4. Cellular .....                              | 65  |
| 7.1.4.1. MAIN/EXT .....                            | 65  |
| 7.1.4.1.1. Parameters .....                        | 66  |
| 7.1.4.1.2. Cellular profiles .....                 | 66  |
| 7.1.4.1.3. Link testing .....                      | 69  |
| 7.1.4.1.4. Profile switching .....                 | 70  |
| 7.1.4.2. SIM1 and SIM2 .....                       | 72  |
| 7.1.4.3. Cooperation with other services .....     | 72  |
| 7.1.5. Status .....                                | 72  |
| 7.2. Routing .....                                 | 73  |
| 7.2.1. Static .....                                | 73  |
| 7.2.1.1. Loopback addresses .....                  | 75  |
| 7.2.2. Babel .....                                 | 76  |
| 7.2.2.1. Description .....                         | 76  |
| 7.2.2.2. Common - Common settings .....            | 78  |
| 7.2.2.3. Network - Interfaces .....                | 79  |
| 7.2.2.4. Static rules .....                        | 81  |
| 7.2.2.5. Import filter .....                       | 82  |
| 7.2.2.6. Export filter .....                       | 83  |
| 7.2.3. OSPF .....                                  | 85  |
| 7.2.3.1. OSPF Common - Common settings .....       | 86  |
| 7.2.3.2. OSPF Network - Areas and interfaces ..... | 86  |
| 7.2.3.2.1. Areas and interfaces .....              | 86  |
| 7.2.3.2.2. Neighbors .....                         | 88  |
| 7.2.3.2.3. Networks .....                          | 88  |
| 7.2.3.3. OSPF Static rules .....                   | 89  |
| 7.2.3.4. OSPF Import filter .....                  | 90  |
| 7.2.3.5. OSPF Export filter .....                  | 91  |
| 7.2.4. BGP .....                                   | 92  |
| 7.2.4.1. BGP Common - Common settings .....        | 93  |
| 7.2.4.2. BGP Neighbors .....                       | 94  |
| 7.2.4.3. BGP Static rules .....                    | 95  |
| 7.2.4.4. BGP Import IGP filter .....               | 96  |
| 7.2.4.5. BGP Export IGP filter .....               | 97  |
| 7.2.4.6. BGP Import OUT rules .....                | 98  |
| 7.2.4.7. BGP Export OUT filter .....               | 99  |
| 7.2.5. Link management .....                       | 100 |
| 7.3. Firewall .....                                | 101 |
| 7.3.1. Firewall L2 .....                           | 101 |
| 7.3.2. Firewall L3 .....                           | 102 |
| 7.3.2.1. Forward .....                             | 102 |
| 7.3.2.2. Input .....                               | 104 |
| 7.3.2.3. Output .....                              | 105 |
| 7.3.3. NAT - Network address translation .....     | 107 |
| 7.3.3.1. Source NAT .....                          | 107 |
| 7.3.3.2. Destination NAT .....                     | 110 |
| 7.3.3.3. Cooperation with other services .....     | 113 |
| 7.4. VPN .....                                     | 113 |
| 7.4.1. IPsec .....                                 | 113 |

|   |     |
|---|-----|
| 7.4.1.1. IPsec settings .....                         | 115 |
| 7.4.1.2. IPsec associations .....                     | 115 |
| 7.4.1.2.1. Traffic selector .....                     | 119 |
| 7.4.1.3. Interaction with DNAT .....                  | 119 |
| 7.4.2. GRE L2 .....                                   | 120 |
| 7.4.3. GRE L3 .....                                   | 121 |
| 7.5. Security .....                                   | 122 |
| 7.5.1. User access .....                              | 124 |
| 7.5.2. Local authentication .....                     | 124 |
| 7.5.2.1. User Accounts .....                          | 124 |
| 7.5.2.2. Settings .....                               | 126 |
| 7.5.3. Credentials .....                              | 127 |
| 7.5.3.1. General .....                                | 127 |
| 7.5.3.2. Credentials .....                            | 127 |
| 7.5.3.3. Read-only keys .....                         | 128 |
| 7.5.3.4. Settings .....                               | 129 |
| 7.5.3.5. Organisation .....                           | 129 |
| 7.5.3.6. Passphrase complexity rules .....            | 130 |
| 7.5.3.7. Creating Local Certification Authority ..... | 130 |
| 7.5.4. Remote authentication .....                    | 130 |
| 7.5.5. Tamper reset .....                             | 132 |
| 7.6. Device .....                                     | 134 |
| 7.6.1. Unit .....                                     | 134 |
| 7.6.1.1. General .....                                | 134 |
| 7.6.1.2. Service USB .....                            | 134 |
| 7.6.1.3. Time .....                                   | 136 |
| 7.6.1.3.1. Time .....                                 | 137 |
| 7.6.1.3.2. NTP servers .....                          | 138 |
| 7.6.1.4. Sleep mode .....                             | 138 |
| 7.6.1.4.1. Wake-up parameters .....                   | 138 |
| 7.6.1.4.2. Go to sleep parameters .....               | 139 |
| 7.6.1.5. GNSS (GPS) .....                             | 140 |
| 7.6.1.5.1. Cooperation with other services .....      | 141 |
| 7.6.2. Configuration .....                            | 141 |
| 7.6.3. Events .....                                   | 146 |
| 7.6.4. SW keys .....                                  | 146 |
| 7.6.5. Firmware .....                                 | 148 |
| 7.6.5.1. Local .....                                  | 148 |
| 7.6.5.1.1. Patch files .....                          | 150 |
| 7.7. Services .....                                   | 151 |
| 7.7.1. SNMP .....                                     | 151 |
| 7.7.2. SMS .....                                      | 154 |
| 7.7.2.1. Parameters .....                             | 155 |
| 7.7.2.2. SMS numbers .....                            | 155 |
| 7.7.2.3. SMS commands .....                           | 156 |
| 7.7.3. GNSS server .....                              | 157 |
| 7.8. Advanced .....                                   | 157 |
| 8. Diagnostics .....                                  | 159 |
| 8.1. STATUS overview .....                            | 159 |
| 8.2. Overview .....                                   | 160 |
| 8.2.1. Measurements .....                             | 160 |
| 8.2.2. Statistics .....                               | 160 |

|  |     |
|--|-----|
| 8.3. Information .....                                   | 161 |
| 8.3.1. Network Interfaces .....                          | 161 |
| 8.3.2. Routing .....                                     | 163 |
| 8.3.3. Firewall .....                                    | 163 |
| 8.3.3.1. Firewall L2 .....                               | 163 |
| 8.3.3.2. Firewall L3 .....                               | 164 |
| 8.3.3.3. NAT .....                                       | 164 |
| 8.3.4. Quality of service .....                          | 165 |
| 8.3.5. Device .....                                      | 166 |
| 8.3.5.1. System information .....                        | 166 |
| 8.3.5.2. Advanced information .....                      | 166 |
| 8.3.6. Diagnostic package .....                          | 166 |
| 8.4. Events .....  | 168 |
| 8.5. Statistics .....                                    | 169 |
| 8.5.1. Parameters .....                                  | 170 |
| 8.5.2. Serial protocol statistics .....                  | 171 |
| 8.5.3. Ethernet statistics .....                         | 172 |
| 8.5.4. Cellular statistics .....                         | 172 |
| 8.5.4.1. Cellular interface statistics .....             | 173 |
| 8.5.4.2. Cellular state statistics .....                 | 174 |
| 8.5.4.3. Cellular signal statistics .....                | 174 |
| 8.5.4.4. Measurements .....                              | 175 |
| 8.6. Monitoring .....                                    | 175 |
| 8.6.1. Settings .....                                    | 176 |
| 8.6.1.1. Overview .....                                  | 176 |
| 8.6.1.2. Interfaces .....                                | 176 |
| 8.6.1.3. General .....                                   | 179 |
| 8.6.2. File output .....                                 | 179 |
| 8.6.3. Console output .....                              | 180 |
| 8.7. Tools .....   | 180 |
| 8.7.1. ICMP ping .....                                   | 180 |
| 8.7.2. RSS ping .....                                    | 181 |
| 8.7.3. Routing .....                                     | 183 |
| 8.7.4. System .....                                      | 183 |
| 8.8. Syslog .....  | 184 |
| 9. Technical parameters .....                            | 185 |
| 10. Safety, regulations, warranty .....                  | 191 |
| 10.1. Safety instructions .....                          | 191 |
| 10.2. High temperature .....                             | 192 |
| 10.3. Battery disposal .....                             | 192 |
| 10.4. Instructions for Safe Operation of Equipment ..... | 192 |
| 10.5. SW license .....                                   | 192 |
| 10.6. EU Compliance .....                                | 194 |
| 10.6.1. RoHS, WEEE and WFD .....                         | 194 |
| 10.6.2. EU Declaration of Conformity RED .....           | 195 |
| 10.6.3. Simplified EU declaration of conformity .....    | 195 |
| 10.7. Warranty .....                                     | 197 |
| 10.8. M!DGE3 maintenance .....                           | 198 |
| A. Abbreviations .....                                   | 200 |
| Revision History .....                                   | 202 |

## Important Notice

### Copyright

© 2023 RACOM. All rights reserved.

Sole owner of all rights to this User manual is the company RACOM s. r. o. (in this manual referred to under the abbreviated name RACOM). Drawing written, printed or reproduced copies of this manual or records on various media or translation of any part of this manual to foreign languages (without written consent of the rights owner) is prohibited.

Products offered may contain software proprietary to RACOM. The offer of supply of these products and services does not include or infer any transfer of ownership.

### 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.

RACOM reserves the right to make changes in the technical specification or in this product function or to terminate production of this product or to terminate its service support without previous written notification of customers.

### 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!DGE3 are used in an appropriate manner within a well-constructed network. M!DGE3 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!DGE3, or for the failure of M!DGE3 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 applicability for its application.
- 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.

# 1. Quick guide

M!DGE3 is a widely configurable and compact cellular router. All you have to do to put it into operation is to connect it to an antenna and a power supply and configure it using a PC (tablet, smartphone) and a web browser.

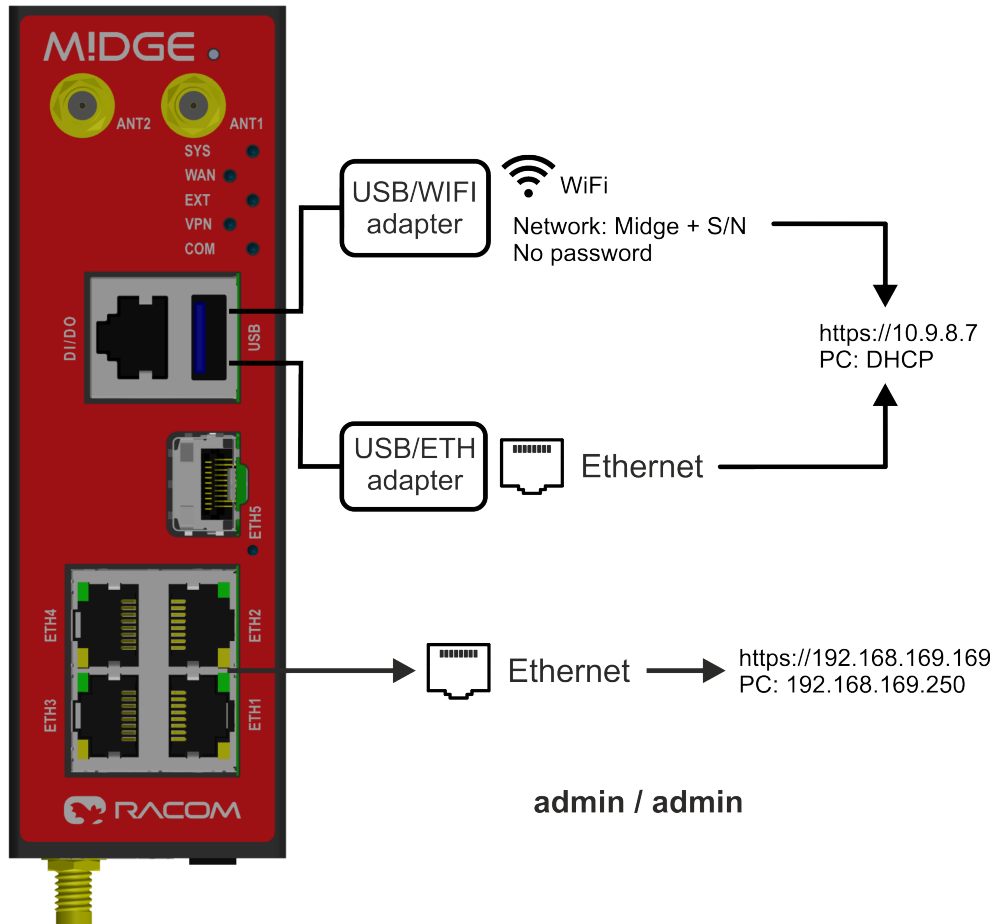


Fig. 1.1: Connecting M!DGE3 to a PC over WiFi, ETH/USB adapter, ETH interface

**Default password for "admin" account is "admin". Change the password before deploying unit to a network.**

To configure M!DGE3 you can connect it to your PC in three ways:

### PC (tablet, smartphone) connected via WiFi adapter

External WiFi adapter Part No. OTH-USB/WIFI-W2 (an optional accessory of the M!DGE3 see *USB adapter*<sup>1</sup>) needs to be used. Any other adapter will not work correctly when connected to M!DGE3 unit. Connect your PC, tablet or smartphone to M!DGE3 WiFi AP first. Its default SSID is Midge S/N. By default, the WPA2 PSK is disabled, so no password is required. The WiFi adapter contains a built-in DHCP server, so if you have a DHCP client in your PC (as most users do), you do not need to set anything up. The default IP address of M!DGE3 unit, for access over the USB adapter, is 10.9.8.7.

<sup>1</sup> [https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories\\_ethusb](https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb)



**PC connected via ETH/USB adapter**

External ETH/USB adapter Part No. OTH-USB/ETH-XR (an optional accessory of the M!DGE3 see *ETH/USB adapter*<sup>2</sup>). The ETH/USB contains a built-in DHCP server, so if you have a DHCP client in your PC as most users, you do not need to set anything up. The default IP address of M!DGE3 unit, for access over the ETH/USB adapter, is 10.9.8.7.

**PC connected directly to an ETH port**

The default IP address for access via ETH ports is 192.168.169.169.

Set a static IP address in PC within 192.168.169.0/24 (e.g. 192.168.169.250, subnet mask 255.255.255.0).

**Important**

When you change the M!DGE3 ETH address to a different IP address/mask, the IP address of your PC might be necessary to be updated to match the same subnet (mask).

**Note**

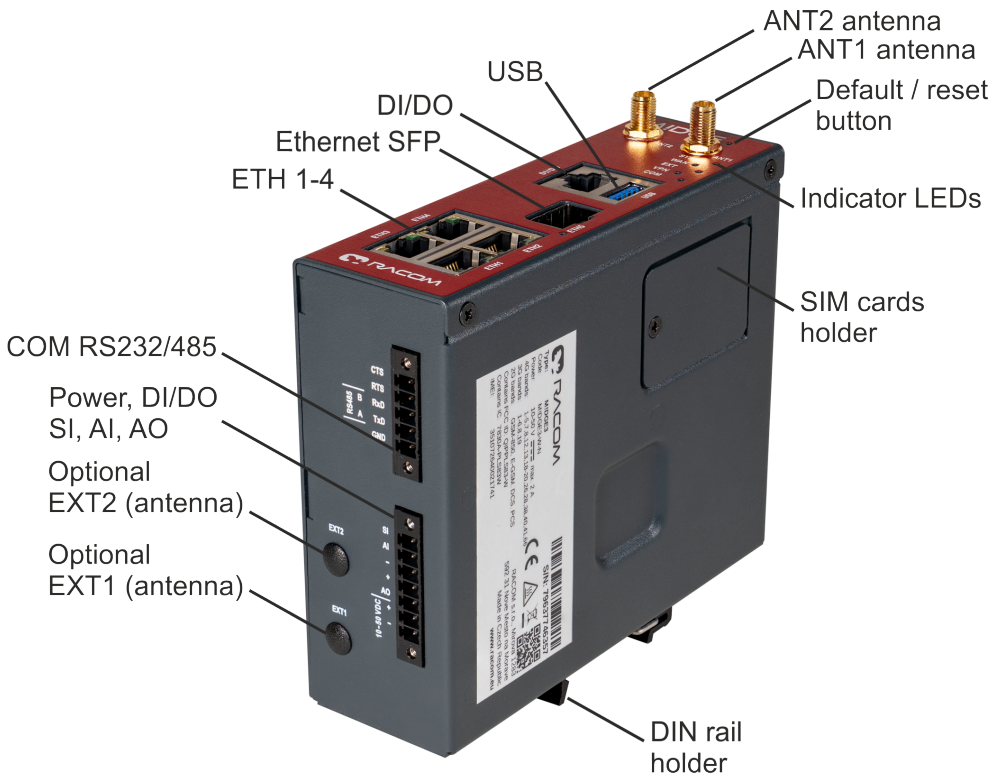
**HTTPS** - For security reasons the http protocol with SSL encryption can be used for the communication between the PC and M!DGE3. The HTTPS protocol requires a security certificate. You must install this certificate into your web browser. The first time you connect to the M!DGE3, your computer will ask you for authorisation to import the certificate into your computer. The certificate is signed by the RACOM s.r.o. certification authority. It meets all security regulations and you need not to be concerned about importing it into your computer. Confirm the import with all warnings and exceptions that your browser may display during installation.

**Note**

If you do not have the USB adapter or you have forgotten the password, you can reset the access parameters to defaults, see *Section 2.2.8, "HW button"*.

<sup>2</sup> [https://www.racom.eu/eng/products/radio-modem-riplex.html#accessories\\_ethusb](https://www.racom.eu/eng/products/radio-modem-riplex.html#accessories_ethusb)

## 2. Product



M!DGE3 is a cellular router platform designed for any real-time environment. M!DGE3 cellular routers are native IP devices, with Linux OS that have been designed with attention to detail, performance and quality.

M!DGE3 is built into a rugged metal casing that allows for multiple installation possibilities, see *Section 4.3, "Mounting"*.

## 2.1. Dimensions

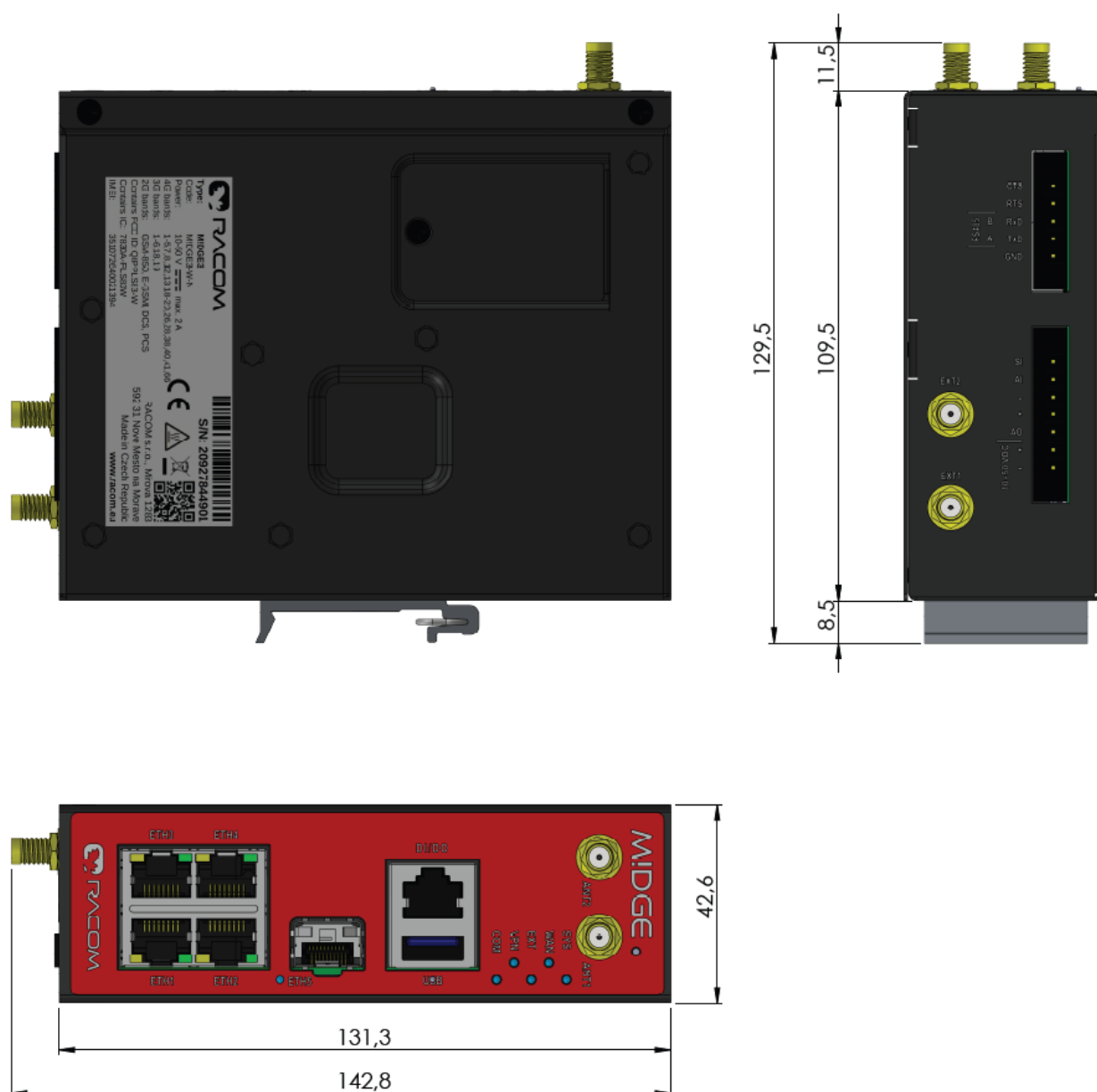


Fig. 2.1: M!DGE3 dimensions

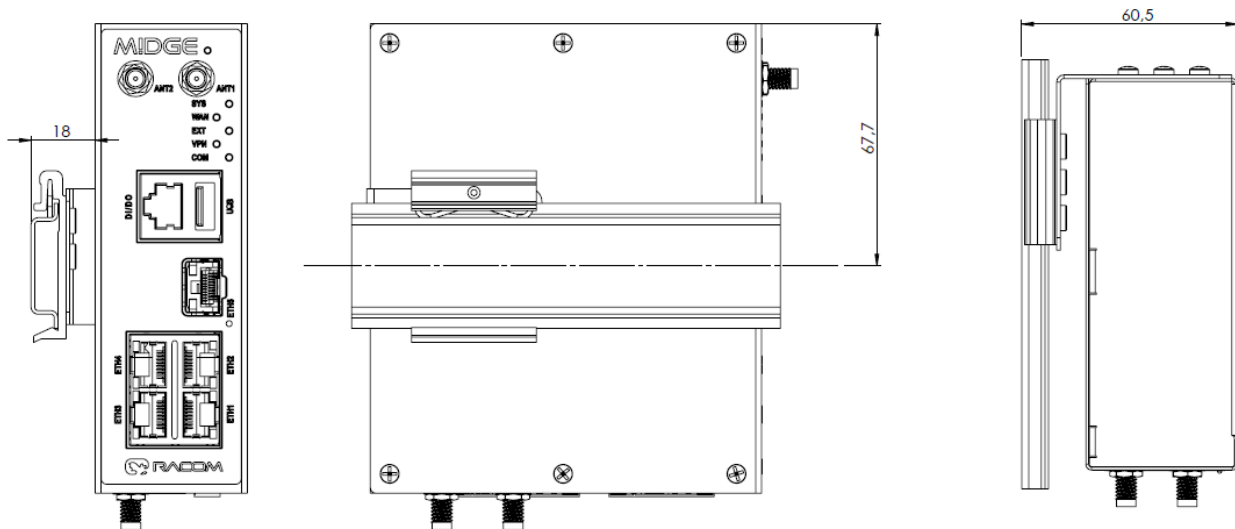


Fig. 2.2: MIDGE3 Edge-bracket dimensions

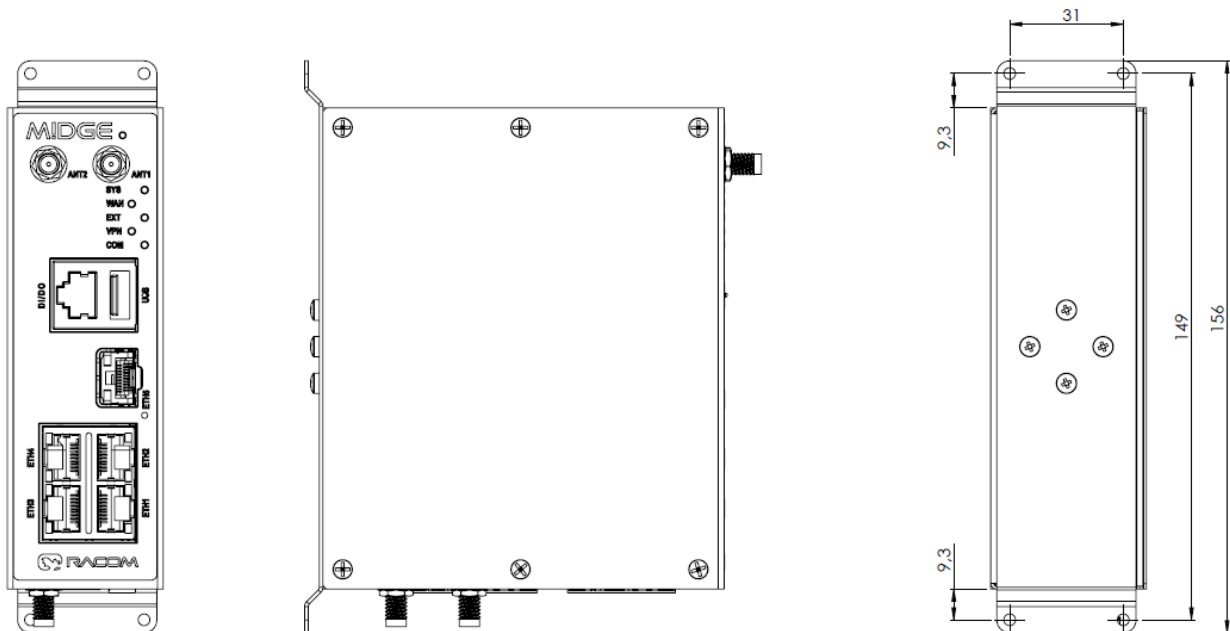


Fig. 2.3: MIDGE3 flat bracket dimensions

For more information see *Section 4.3.1, "DIN rail mounting"* and *Section 4.3.2, "Flat mounting"*.

## 2.2. Connectors

All connectors are located on the front and bottom panel. The front panel contains even LEDs. The HW button is located on the front panel as well (close to the upper edge).



Fig. 2.4: Connectors

### 2.2.1. Antenna

An antenna can be connected to M!DGE3 via SMA female 50  $\Omega$  connector.

M!DGE3 is equipped with two connectors. The ANT1 connector will be used for common transmitting and receiving single antenna installation. The ANT2 connector will be used as a second MIMO connector.



Fig. 2.5: Antenna connectors



#### Warning

M!DGE3 cellular router may be damaged when operated without an antenna or a dummy load.

### 2.2.2. Power and Control

This rugged connector connects to a power supply and it contains control signals. A plug with screw-terminals and retaining screws for power and control connector is supplied with each M!DGE3. It is Tyco 7 pin terminal block plug, part No. 1776192-7, contact pitch 3.81 mm. The connector is designed for electric wires with a cross section of 0.5 to 1.5 mm<sup>2</sup>. Strip the wire leads to 6 mm (1/4 inch). Isolated cables should receive PKC 108 or less end sleeves before they are inserted in the clip. Insert the cables in the wire ports, tightening securely.

**Tab. 2.1: Pin assignment**

| Pin | Labeled | Signal   |
|-----|---------|--|
| 1   | SI      | SLEEP INPUT<br>• pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis)<br>• max. 50 VDC    |
| 2   | AI      | HW ALARM INPUT<br>• pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis)<br>• max. 50 VDC |
| 3   | -       | -(GND) – for SLEEP IN, HW ALARM INPUT  |
| 4   | +       | +(POWER) – for HW ALARM OUTPUT   |
| 5   | AO      | HW ALARM OUTPUT<br>open drain output max. 50 VDC, 1 A  |
| 6   | +       | + POWER (10 to 50 V)<br>Undervoltage threshold 8.5 VDC<br>Overvoltage threshold 55 VDC                       |
| 7   | -       | - POWER (GND)  |

Pins 3 and 7 are connected internally.  
 Pins 4 and 6 are connected internally.  
 Minus pole (GND) is internally connected with casing.

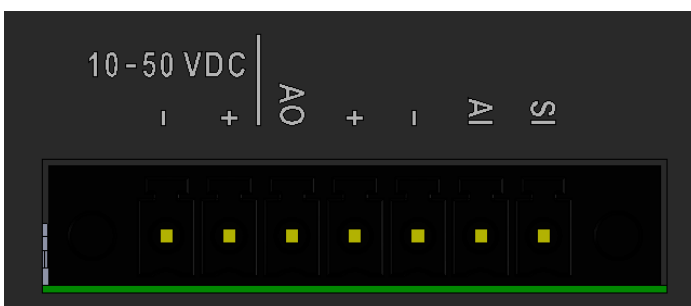


Fig. 2.6: Supply connector

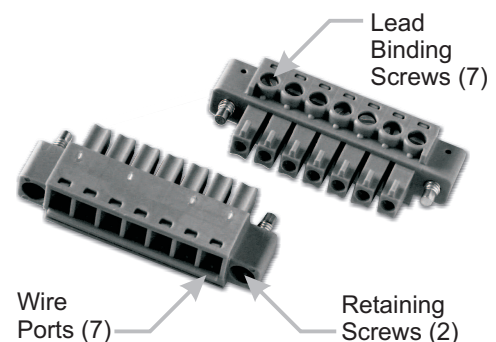


Fig. 2.7: Power and Control - cable plug

#### HW ALARM INPUT

HW ALARM INPUT is a digital input. If grounded (e.g. by connecting to pin 3), an external alarm is triggered.

**HW ALARM OUTPUT**

HW ALARM OUTPUT is a digital output.

**POWER**

The POWER pins labelled + and - serve to connect a power supply 10–50 VDC. The requirements for a power supply are defined in *Section 4.8, “Power supply”* and *Chapter 9, Technical parameters*.

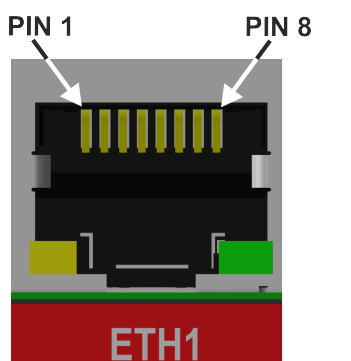
### 2.2.3. ETH1 - ETH4

Standard RJ45 connectors for Ethernet connection. M!DGE3 has 10/100/1000Base-T Auto MDI/MDIX interfaces so it can connect to 10 Mb/s, 100 Mb/s or 1000 Mb/s Ethernet network. The speed can be selected manually or recognized automatically by M!DGE3. M!DGE3 is provided with Auto MDI/MDIX function which allows it to connect over both standard and cross cables, adapting itself automatically.

#### Pin assignment

Tab. 2.2: Ethernet to cable connector connections

| Pin | Signal | Direct cable   | Crossed cable  |
|-----|--------|----------------|----------------|
| 1   | TX+    | orange – white | green – white  |
| 2   | TX-    | orange         | green          |
| 3   | RX+    | green – white  | orange – white |
| 4   | —      | blue           | blue           |
| 5   | —      | blue – white   | blue – white   |
| 6   | RX-    | green          | orange         |
| 7   | —      | brown – white  | brown – white  |
| 8   | —      | brown          | brown          |



### 2.2.4. ETH5 (SFP)

ETH5 is a standard SFP slot for 10/100/1000 Mb/s Ethernet SFP modules, user exchangeable with maximal power consumption 1.25 W. Both fibre optic and metallic Ethernet SFP modules are supported. For optical both single and dual mode fibre optics Ethernet modules (= 2 or 1 fibers) can be used. CSFP modules are not supported. RACOM offers all mentioned types of SFP modules, tested to be M!DGE3 compatible as a standard accessory.

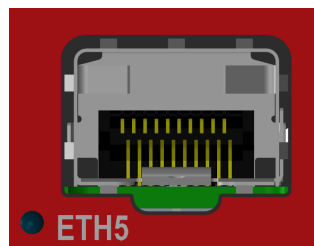


Fig. 2.8: SFP slot

The SFP status LED is located just next to the slot. It is controlled by SFP module. Its function is specific for each SFP module. The typical behavior is an indication the received signal from the fibre optic or metallic link to be within operational range.



#### Important

It is strongly recommended to use a high quality SFP module with industry temperature range. The SFP modules listed in Accessories are thoroughly tested by RACOM and are guaranteed to function with M!DGE3 units. It is possible to use any other SFP module, but RACOM cannot guarantee they will be completely compatible with M!DGE3 units.



## 2.2.5. COM

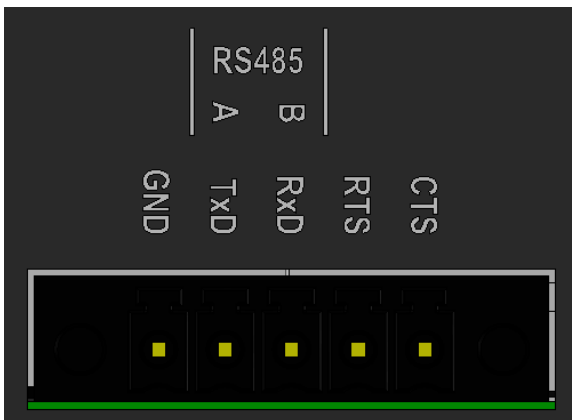
MIDGE3 provides serial interface COM terminated by 5 pin terminal connector which is supplied with each MIDGE3 unit. It can be configured as RS232 or RS485. It is Tyco 5 pin terminal block plug, part No. 1776192-5, contact pitch 3.81 mm. The connector is designed for electric wires with a cross section of 0.5 to 1.5 mm<sup>2</sup>. Strip the wire leads to 6 mm (1/4 inch). Isolated cables should receive PKC 108 or less end sleeves before they are inserted in the clip. Insert the cables in the wire ports, tightening securely.

RS232 of MIDGE3 is a hard-wired DCE (Data Communication Equipment) device. Equipment connected to the serial port of MIDGE3 unit should be DTE (Data Terminal Equipment).

RS485 of MIDGE3 is not galvanic isolated and it is not terminated.

**Tab. 2.3: COM pin description**

| Terminal block | COM – RS232 |         | COM – RS485 |         |
|----------------|-------------|---------|-------------|---------|
|                | Signal      | In/ Out | Signal      | In/ Out |
| 1              | CTS         | Out     | —           |         |
| 2              | RTS         | In      | —           |         |
| 3              | RxD         | Out     | line B      | In/Out  |
| 4              | TxD         | In      | line A      | In/Out  |
| 5              | GND         |         | GND         |         |




MIDGE3 keeps pin 6 DSR at the level of 0 (state ON, approx. +6.2 V) by RS232 standard permanently.

## 2.2.6. USB

MIDGE3 uses USB 3.0, Host A interface. USB interface is wired as standard:

**Tab. 2.4: USB A Pinout Cable Assembly**

| Pin | Signal     | Wire   |
|-----|------------|--------|
| 1   | VBUS       | Red    |
| 2   | D-         | White  |
| 3   | D+         | Green  |
| 4   | GND        | Black  |
| 5   | StdA_SSRX- | Blue   |
| 6   | StdA_SSRX+ | Yellow |
| 7   | GND_DRAIN  | GROUND |
| 8   | StdA_SSTX- | Purple |



| Pin   | Signal     | Wire            |
|-------|------------|-----------------|
| 9     | StdA_SSTX+ | Orange          |
| Shell | Shield     | Connector Shell |

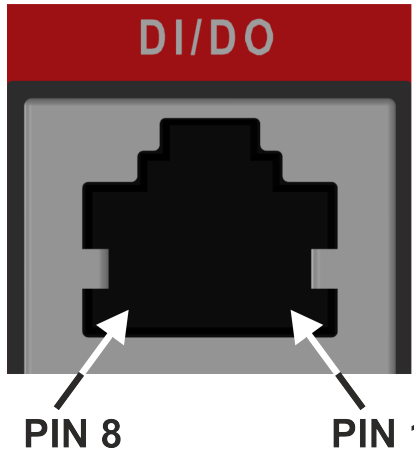
The USB interface is designed for the connection to an external ETH/USB adapter or a WiFi adapter. They are optional accessories to MIDGE3, for more details see [www.ripex/accessories](http://www.ripex/accessories)<sup>1</sup>. The adapters are used for service access to web configuration interface of MIDGE3 unit.

The USB connector also provides power supply (5 V / 0.5 A). It can be used to temporarily power a connected device, for instance a telephone. The USB connector should not be used as permanent source of power supply.

### 2.2.7. DI/DO

**Tab. 2.5: Digital Inputs and Outputs**

| Pin | Description | Signal  |
|-----|-------------|---|
| 1   | DI1+        | Digital input (differential) - Positive - (P) |
| 2   | DI1-        | Digital input (differential) - Negative - (N) |
| 3   | GND         | Ground  |
| 4   | DO1         | Digital Output 1                              |
| 5   | DO2         | Digital Output 2                              |
| 6   | GND         | Ground  |
| 7   | DI2         | Digital Input 2                               |
| 8   | DI3         | Digital Input 3                               |



The diagram shows a connector labeled 'DI/DO' with a red header. Below the header is a black connector housing. Two white arrows point to the bottom pins of the housing, labeled 'PIN 8' on the left and 'PIN 1' on the right.

Digital Outputs:

- Open drain output max. 50 VDC, 0.2 A

Isolated differential digital input:

- Input voltage difference (P-N) > 1.9 VDC Logic "H"
- Input voltage difference (P-N) < 1.1 VDC Logic "L"
- Maximum differential voltage 50 V

Digital inputs:

- Schmitt-triggered inverted input
- Pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis)
- Max. 50 VDC

<sup>1</sup> [https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories\\_ethusb](https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb)

## 2.2.8. HW button



Fig. 2.9: HW button

HW button is placed on the right side of M!DGE3, next to the logo.

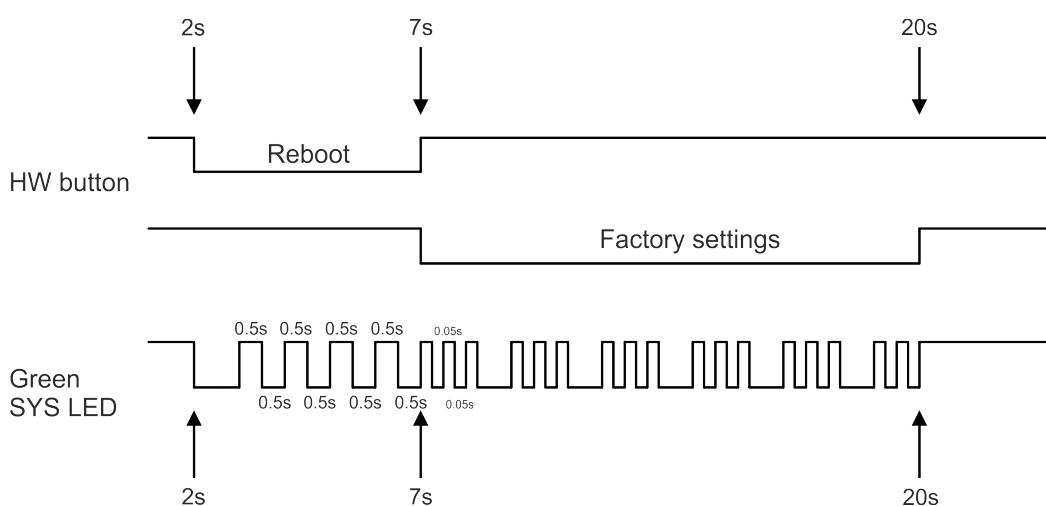


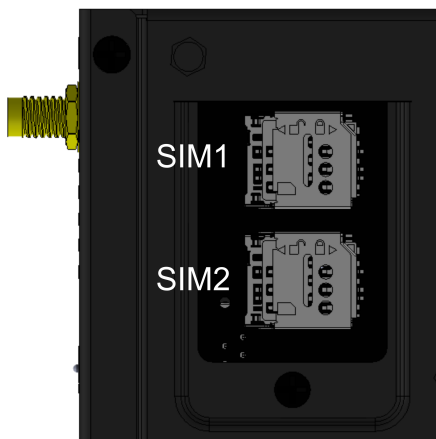
Fig. 2.10: HW button scheme

### HW button operation

- Press less than 2 seconds - Nothing happens
- Press from 2 up to 7 seconds - Reboot is performed on button release
- Press from 7 up to 20 seconds - Factory settings are performed on button release
- Press more than 20 seconds - Nothing happens

## 2.2.9. SIM cards

Two SIM card holders for Micro SIM (3FF) are available under the screwed cover on the M!DGE3 right side.



**Warning**

Disconnect M!DGE3 unit from a power supply before opening the cover and manipulating with SIM cards.

### 2.3. Indication LEDs

LEDs indicator is placed on M!DGE3's front panel.



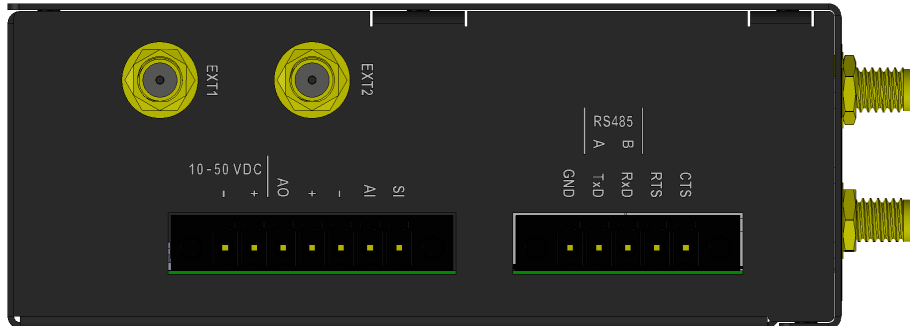
Fig. 2.11: Indication LEDs

Tab. 2.6: Key to LEDs

| LED  | Colour               | Style   | Function  |
|--|----------------------|---|---|
| SYS  | Green                | Permanently lit                                 | System OK   |
|  |                      | Flashing - period 500 ms                        | Reset button pushed   |
|  |                      | Three fast (50 ms) flashes - pause (500 ms)     | Reset button factory reset  |
|  | Red                  | Permanently lit                                 | Alarm <sup>1</sup>  |
|  |                      | Flashing regularly - period 500 ms              | Serious system error  |
| Orange   | Permanently lit      | Unit is starting                                |   |
| WAN  | Green / Orange / Red | Permanently lit, or flashing in 1 sec intervals | Permanently lit - connected to the cellular network. Color signalizes signal strength<br>Flashing - connecting into the cellular network. |
| EXT  | Green                | According to the used extension module          | Activity of extension module (like GPS fix, LTE connected, ...)<br><i>LED behavior detailed description</i>                               |
|  | Red                  | Permanently lit                                 | Alarm of extension module   |
| VPN  | Red                  | Permanently lit                                 | Pending   |
| COM  | Green                | Permanently lit                                 | Data receiving  |
|  | Orange               | Permanently lit                                 | Data transmitting   |
| <sup>1</sup> An Alarm is triggered by any event with severity Error or higher (see Section 8.4, "Events"). |                      |   |   |

## 2.4. Extension

M!DGE3 cellular router can be delivered with additional (optional) second cellular module, GPS extension or COM extension. In case of Cellular or GPS it comes with two additional SMA connectors installed on the bottom panel (EXT1, EXT2). Activity of any extension module is signaled on M!DGE3's front panel (EXT LED).



### 2.4.1. Cellular

It is recommended to use both antennas (MIMO diversity) for the LTE connection. In case of using only one antenna, attach it to the EXT1 connector.

When the 2<sup>nd</sup> cellular module is used, LED behavior of this extension is signaled by Green / Orange / Red LED

- Permanently lit - Connected to the cellular network (color signalize signal strength)
- Flashing in 1 sec interval - Connecting into the cellular network

### 2.4.2. GPS - pending

M!DGE3 cellular router will be equipped with the GPS receiver with time pulse output. EXT1 connector is used for connection of the active GPS antenna, EXT2 connector is used for the precise time pulse output.

### 2.4.3. COM2 - COM3

The 2nd and 3rd COM ports are available when the Extension module 'C' (2 x RS232) is installed. In such a case: The DI/DO connector is used as a connector for COM2 and COM3.

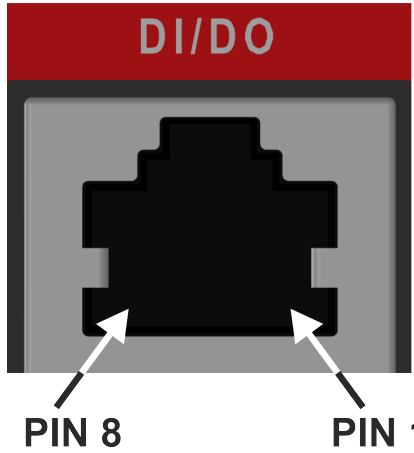
COM2 and COM3 parameters:

COM2: RS232 - 5 pin (RxD, TxD, GND, RTS, CTS) 600 b/s to 2 Mb/s

COM3: RS232 - 3 pin (RxD, TxD, GND) 2.4 kb/s to 921.6 kb/s

Tab. 2.7: DI/DO connector used by Extension module 'C'

| Pin | Signal   | In / Out |
|-----|----------|----------|
| 1   | RxD COM3 | Out      |
| 2   | TxD COM3 | In       |
| 3   | GND      |          |
| 4   | CTS COM2 | Out      |
| 5   | RTS COM2 | In       |
| 6   | GND      |          |
| 7   | RxD COM2 | Out      |
| 8   | TxD COM2 | In       |



## 2.5. Ordering codes

# M!DGE3-W-G (SFP)

Trade name

Gen. Main

Ext.

SW keys

Type

Code

Order code

**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 does not have any number in this position.

Possible values: **3**

### Main

Possible values:

**N** – not used

**W** – Main cellular module, *Bands W*

Bands:

W – 4G/3G/2G, Global

**Ext.** – Extension module embedded in mPCIe slot

Possible values:

**N** – not used

**W** – Extension cellular module, *Bands W*; Part No.: mPCIe-W

Bands:

*W* – 4G/3G/2G, Global

**G** – Extension GPS (GNSS) module; *Bands G*; Part No.: mPCIe-GPS

**C** – Extension 2× RS232; *Bands C*; Part No.: mPCIe-COMS

Only one option for mPCIe slot is possible.

**SW keys** – if unit is ordered with SW keys, all keys are specified in this bracket. SW key can be ordered independently for specific S/N anytime later on.

Possible values:

**SFP** – enables SFP interface; Part No.: M!DGE3-SW-SFP

**Type** – specific product type

Possible values:

**M!DGE3**

**Code** – part of order code which is printed on Product label on the housing (SW keys are not HW dependent and can be ordered later on, so they are not printed on Product label).

**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 *E-shop*<sup>2</sup>.

---

<sup>2</sup> <https://webservice-new.racom.eu/main/eshop.list?t=10>



### 3. Accessories

Whole accessory list is available on *RACOM*<sup>1</sup> website.

1. Edge-bracket
2. Flat-bracket
3. USB adapters (ETH, WiFi)  
[https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories\\_ethusb](https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb)
4. Demo case  
[https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories\\_democase](https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_democase)

---

<sup>1</sup> <https://www.racom.eu/eng/products/cellular-router-midge.html#accessories>

## 4. Installation

### 4.1. Step-by-step checklist

1. Mount M!DGE3 into cabinet (*Section 4.3, "Mounting"*).
2. Install antenna (*Section 4.4, "Antenna installation"*).
3. Install feed line (*Section 4.5, "Antenna feed line"*).
4. Ensure proper grounding (*Section 4.6, "Grounding"*).
5. Run cables and plug-in all connectors except from the SCADA equipment (*Section 2.2, "Connectors"*).
6. Apply power supply to M!DGE3.
7. Connect configuration PC (*Ripex2 "Connecting"*).
8. Configure M!DGE3.
9. Test radio link quality (e.g. using Monitoring tool).
10. Connect the SCADA equipment.
11. Test your application.

### 4.2. Minimal required settings to set-up cellular connection

1. Enter the PIN code for the particular SIM card, if required (SETTINGS > Interfaces > Cellular > SIM1/SIM2).
2. Enable and Configure the Access Point Name (APN) (SETTINGS > Interfaces > Cellular > MAIN/EXT > Enable & Add/Edit Cellular profile).
3. Add default route 0.0.0.0/0 via WWAN (MAIN or EXT) (SETTINGS > Routing > Static) or other routing rule required.
  - No route is added automatically, required routes must be added manually.
  - Without such routes, unit will be connected to the cellular network, but not communicating with any other device/IP.
4. Save the changes.
5. Check functionality
  - SETTINGS > Interfaces > Cellular > Status > Show more (<)
  - DIAGNOSTICS > Tools > ICMP ping
  - DIAGNOSTICS > Statistics > Cellular statistic tables (Interface, State, Signal)
6. In case of any issues, download a detailed Diagnostic package (DIAGNOSTICS > Information > Diagnostic package), include all the information except User credentials and send it to [support@racom.eu](mailto:support@racom.eu)<sup>1</sup>.

---

<sup>1</sup> <mailto:support@racom.eu>

## 4.3. Mounting

### 4.3.1. DIN rail mounting

M!DGE3 cellular modem is directly mounted to the DIN rail by a holder (which comes with the modem).

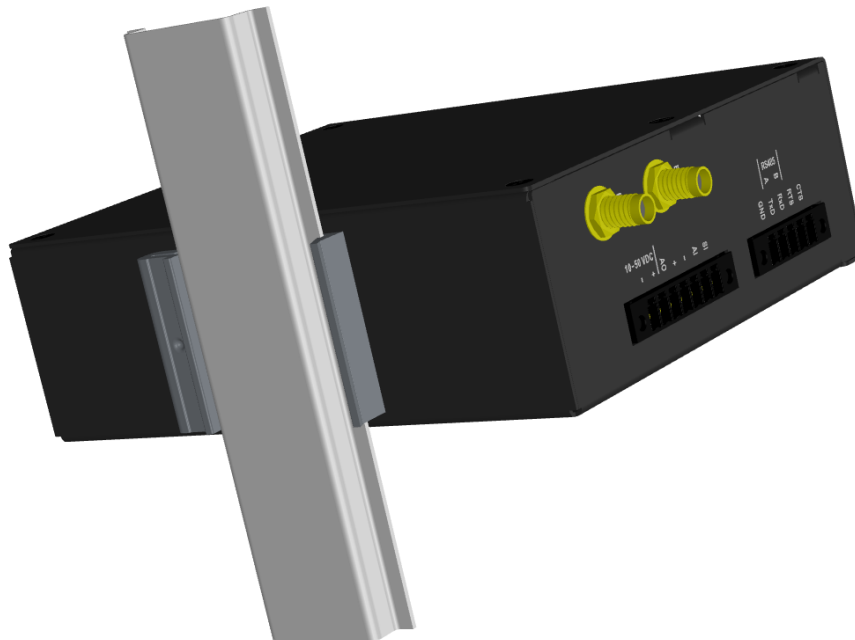


Fig. 4.1: DIN rail

Using this mounting M!DGE3 can be mounted in different angles (by 90° clockwise/counter clockwise).



For edged mounting to the DIN rail, Edge-bracket (optional accessory) is used. Use solely the M4×5 mm screws that are supplied.



Fig. 4.2: Edged mounting to DIN rail

### 4.3.2. Flat mounting

For flat mounting directly to the support you must use the Flat bracket (an optional accessory). Use solely the M4×5 mm screws that are supplied.



Fig. 4.3: Flat mounting using Flat bracket

## 4.4. Antenna installation

The type of antenna best suited for the individual sites of your network depends on the layout of the network and your requirements for signal level at each site.

The antenna should never be installed close to potential sources of interference, especially electronic devices like computers or switching power supplies.

### Additional safety recommendations

Only qualified personnel with authorization to work at heights are entitled to install antennas on masts, roofs and walls of buildings. Do not install the antenna in the vicinity of electrical lines. The antenna and brackets should not come into contact with electrical wiring at any time.

The antenna and cables are electrical conductors. During installation electrostatic charges may build up which may lead to injury. During installation or repair work all open metal parts must be temporarily grounded.

The antenna and antenna feed line must be grounded at all times.

Do not mount the antenna in windy or rainy conditions or during a storm, or if the area is covered with snow or ice. Do not touch the antenna, antenna brackets or conductors during a storm.

## 4.5. Antenna feed line

The antenna feed line should be chosen so that its attenuation does not exceed 3 to 6 dB as a rule of thumb. Use 50  $\Omega$  impedance cables only.

The shorter the feed line, the better. If MIDGE3 is installed close to antenna, the data cable can be replaced by an Ethernet cable for other protocols utilizing the serial port, see *Section 7.1.3, "Terminal servers"*.

Always follow the installation recommendations provided by the cable manufacturer (bend radius, etc.). Use suitable connectors and install them diligently. Poorly attached connectors increase interference and can cause link instability.

## 4.6. Grounding

To minimize the odds of the transceiver and the connected equipment receiving any damage, a safety ground (NEC Class 2 compliant) should be used, which bonds the antenna system, transceiver, power supply, and connected data equipment to a single-point ground, keeping the ground leads short.

The MIDGE3 cellular router is generally considered adequately grounded if the supplied flat mounting brackets are used to mount the cellular router to a properly grounded metal surface. If the cellular router is not mounted to a grounded surface, you should attach a safety ground wire to one of the mounting brackets or a screw on cellular router's casing.

If the antenna is installed outside the building, it is strongly recommended to install an appropriate lightning protection system where the antenna cable enters the building.

**Note**

All cabling, groundings and lightning protection must comply with the applicable standards and regulations.

## 4.7. Connectors

M!DGE3 uses standard connectors. Use only standard counterparts to these connectors.

You will find the pin-outs of connectors in *Section 2.2, "Connectors"*.

## 4.8. Power supply

We do not recommend switching on power supply of the M!DGE3 unit before connecting the antenna and other devices. Connecting the RTU and other devices to M!DGE3 while powered increases the likelihood of damage due to the discharge of difference in electric potentials.

M!DGE3 may be powered from any well-filtered 10 to 50 VDC power source. To avoid radio channel interference, the power supply must meet all relevant EMC standards. Never install a power supply close to the antenna. Connector (- pins) is internally connected to the casing of the M!DGE3 unit.

## 5. M!DGE3 in detail

### 5.1. Combination of IP and serial communication

M!DGE3 enables combination of IP and serial protocols within a single application.

Five independent terminal servers are available in M!DGE3. Terminal server is a virtual substitute for devices used as serial-to-TCP(UDP) converters. It encapsulates serial protocol to TCP(UDP) and vice versa eliminating the transfer of **TCP overhead** .

If the data structure of a packet is identical for IP and serial protocols, the terminal server can serve as a converter between TCP(UDP)/IP and serial protocols (RS232, RS485).

#### 5.1.1. Detailed Description

Generally, a Terminal server (also referred to as Serial server) enables connection of devices with a serial interface to a M!DGE3 over the local area network (LAN). It is a virtual substitute for the devices used as serial-to-TCP(UDP) converters.

Examples of the use:

A SCADA application in the center should be connected to the network via 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!DGE3. This type of connection between M!DGE3 SCADA and application is beneficial in the following circumstances:

- There is no hardware serial interface on the computer
- Serial cable between M!DGE3 and computer would be too long. E.g. the M!DGE3 is installed very close to the antenna to reduce feed line loss.
- LAN already exists between the computer and the point of installation

In special cases, the Terminal server can reduce network load from TCP applications. A TCP session can be terminated locally at the Terminal server in M!DGE3. User data are extracted from the TCP messages and processed as if it came from a COM port. When the data reaches the destination M!DGE3, it can be transferred to the RTU either via the serial interface or via TCP (UDP), using the Terminal server again. Please note, that M!DGE3 Terminal server implementation also supports the dynamical IP port change in every incoming application datagram. In such a case the M!DGE3 sends the reply to the port from which the last response has been received. This feature allows to extend the number of simultaneously opened TCP connections between the M!DGE3 and the locally connected application up to 10 on each Terminal server.



## 6. Web interface

M!DGE3 can be easily managed from your computer using a web browser. If there is an IP connection between the computer and the respective M!DGE3, you can simply enter the IP address of any M!DGE3 in the network directly in the browser address line and log in. However, it is not recommended to manage an over-the-air connected M!DGE3 in this way, because high amounts of data would have to be transferred over the Cellular channel.

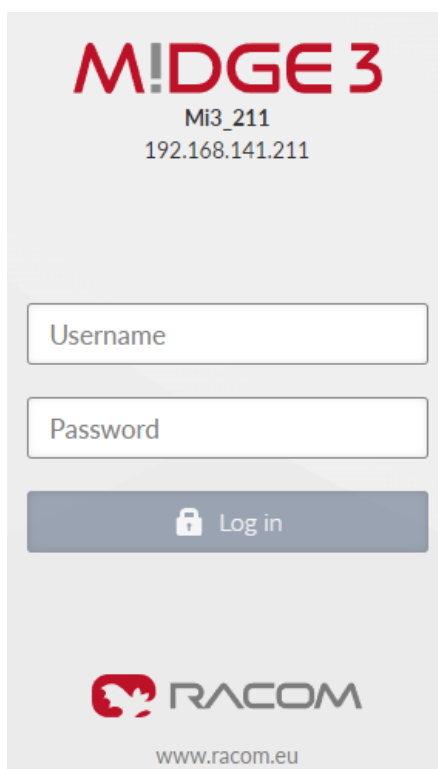
When you need to manage an over-the-air connected M!DGE3 (recommended), log-in to a M!DGE3, which your computer is connected to using either a cable (via LAN) or a high-speed WAN. The M!DGE3 which you are logged-in to in this way is called Local. Then you can manage any remote M!DGE3 in the network over-the-air in a throughput-saving way: all the static data (e.g. Web page graphic objects) is downloaded from the Local M!DGE3 and only information specific to the remote unit is transferred over the Cellular channel. M!DGE3 accessed in such a way is called Remote.

You can also connect to a RipEX2 unit to the hybrid networks in a same way.

For the sake of security only HTTPS protocol is used for the connection between the web browser and M!DGE3 unit. If the `http://...` is used into the web browser address line, the communication is immediately automatically redirected to HTTPS protocol.

For better protection against unauthorized access to the network there is a timer build within the M!DGE3 unit and the web interface (set to 24 hours by default), which is monitoring user activity. In case of user inactivity, the connection between the web interface and the unit will be interrupted (i.e. automatic logout). Timer is automatically launched in parallel both In the unit and in the web browser. In case of changing the timer setting, we recommend to logout and login, so the correct initialization of timeout inactivity can occur.

### Login page



M!DGE3  
Mi3\_211  
192.168.141.211

Username

Password

Log in

RACOM  
www.racom.eu



**Note**

Web interface for M!DGE3 is identical to RipEX2.

The login page informs you about the Unit name and IP address of the M!DGE3 unit you are trying to log in.

The login page allows changing of the language of the whole web interface (English language is default).

Web interface is designed for usage on all kinds of equipment - with different screen sizes and screen resolutions. Most of the pictures depicted in this User manual are taken on the desktop type of screen resolution.



**Note**

A mechanism against brute-force attack is implemented. When wrong combination of the Account / Password is entered you have to wait a while for the following attempt. The time is growing with every wrong attempt.

**Web page header**



The header of each web page contains:

- Unit name
- IP address of the M!DGE3 unit you are connected to
- Remote access button
- Identification of the current web page (2<sup>nd</sup> or 3<sup>rd</sup> level of the menu)
- Changes to commit button
- Notifications button
- Refresh settings button
- User menu button

**6.1. Supported web browsers**

Supported web browsers for desktop are current versions of:

- Edge
- Chrome
- Firefox
- Safari

Supported Web browsers for mobile equipment are current versions of:

- Safari for iOS
- Chrome for Android

**Note**

For safety reasons, it is recommended to use a web browser without any extensions (especially extensions, which could get access to data).

## 6.2. Changes to commit

M!DGE3 is capable of remembering changes, which were done in its configuration and collecting them in a Changes to commit "basket". All changes of configuration parameters are highlighted by different color.

|                 |       |   |
|-----------------|-------|---|
| Type            | RS485 | ▼ |
| Baud rate [b/s] | 9600  | ▼ |
| Data bits       | 8     | ▼ |
| Parity          | Even  | ▼ |
| Stop bits       | 1     | ▼ |
| Idle [ms]       | 20    |   |
| MRU [B]         | 1000  |   |
| Flow control    | None  | ▼ |

To access the Changes to commit "basket", click on the Changes button (top right corner in the Web page header) or use "Ctrl+Alt+C" shortcut.

Changes to commit "basket" collects all changed settings, which:

- Are separated in the menu alphabetically. Alphabetical separation is sorted hierarchically according to the name of items in the menu.
- Are displayed in the menu (including the path of their placement) and provided with a link for a quick transfer to its original placement.
- Carry an information about their changed values ("Old value" → "New value").

## Web interface

Unit time: 2022-10-25 09:54:35 (UTC+2)

STATUS  
SETTINGS  
DIAGNOSTICS  
ADVANCED

CHANGES TO COMMIT

Reset changes

[Return to configuration](#)

**Your current changes**

Settings > Interfaces > Ethernet > Network interfaces > Ports > 4 > 3

Settings > Interfaces > Ethernet > Network interfaces > Ports > 3

ID: 2  
Parent ID: 1  
Enable port: On  
Bridges: ETH4  
VLAN row: 0

Settings > Interfaces > Ethernet > Network interfaces > Ports > 5 > 4

Settings > Interfaces > Ethernet > Network interfaces > Ports > 5

ID: 6  
Parent ID: 0  
Enable port: On  
Bridges: ETH4  
VLAN row: 0

Send configuration   Download as file

From this page, it is possible to:

- Return to configuration - return to the last changed value's configuration menu.
- Reset changes - all changes will be reset back to their previously set value (not default).
- Send configuration - Apply (Save to the unit) all the changes.

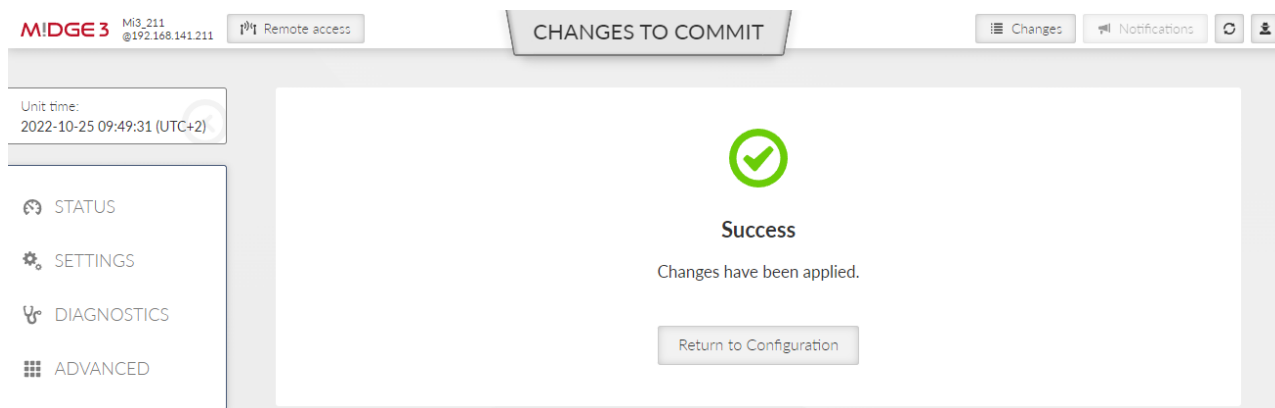
Unit time: 2022-10-25 09:47:40 (UTC+2)

STATUS  
SETTINGS  
DIAGNOSTICS  
ADVANCED

CHANGES TO COMMIT

Applying changes

This could take some time. Please wait.



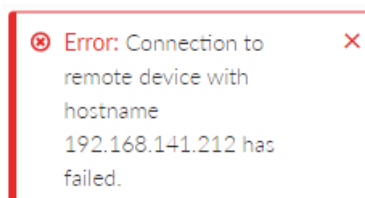
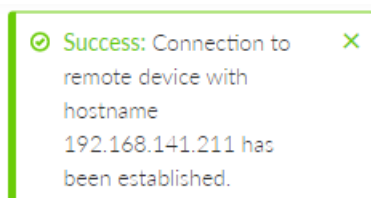
### 6.3. Notifications

With M!DGE3 new way of showing important system events to the user is introduced. It is called Notification Center and is used consistently throughout the interface. Notification Center is located on the top right corner of the interface. It exists in two forms: active notification display and full Notification Center. Both the active notification display and the full Notification Center are displayed either below the top header of the interface or in the right hand sidebar depending on the size of user's display. The behavior is responsive so in case the user needs to make the browser window narrower, the notification center automatically changes place to use the most efficient location.



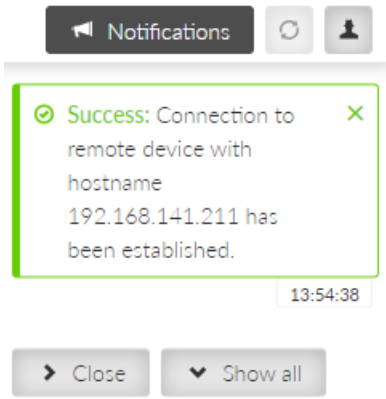
#### Note

To access Notification Center it is possible to use shortcut "Ctrl+Alt+N".



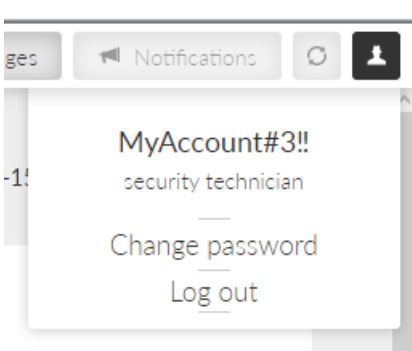
Notifications are mostly triggered by user actions in the interface, for example success or failure of Fast Remote Access connection. They are not to be confused with Events, which are triggered mostly by the system and are not shown in the Notification Center, but on Diagnostics > Events page. In other words Notifications are caused by the user, Events are caused by changing status of the unit.

Every new notification is displayed in the Notification Center drawer. User can either dismiss the notification by clicking the cross in the notification body, close all displayed notifications in the drawer or expand full Notification Center using buttons ("Close all" and "Show all") on the right side of the Notification Center drawer.



Notification Center collects all notifications that have not been dismissed and allows users to browse them.

## 6.4. User menu



It is strongly recommended to change the default password.

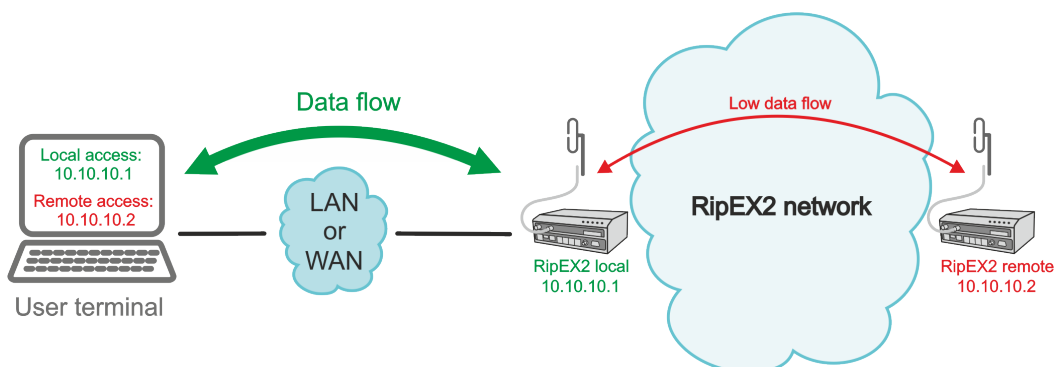
## 6.5. Remote access

M!DGE3 unit management is designed to work smoothly even when the unit under configuration is connected via relatively slow channel. In case of locally connected unit - direct configuration of the unit (accessing the unit IP address directly from the web browser) works fine. If the unit should be connected remotely via the network, the so-called "Remote access" needs to be used to configure and manage remote unit using bandwidth friendly volumes of transmitted data. Open the web browser, enter the IP address of a locally connected unit and connect to a remote unit (which needs to be accessible from the locally connected unit via the network).



### Note

To access Remote access it is possible to use shortcut "Ctrl+Alt+R".



**M!DGE3 local** unit must have the newest firmware version in the whole network to ensure proper Remote access functionality. Nevertheless it is recommended to keep the same version of firmware in the whole network. See details in chapter *Section 7.6.5, "Firmware"*

Remote access can be activated by clicking on the Connect access button.

Once the Remote access is successful, the IP address line changes its color to black together with the web page identification.

The IP address of the currently connected M!DGE3 unit is displayed as a part of the Remote access button. All the configuration settings are remotely available using standard web interface. Some of the Diagnostic features are available via local connection only.

Remote access connection can be established directly by entering the IP address of the Remote unit as an additional parameter into the URL. The required format is:

`https://LOCAL_UNIT_IP_ADDRESS?remoteAccessTarget=REMOTE_UNIT_IP_ADDRESS`

for example: `https://192.168.141.210?remoteAccessTarget=10.10.10.212`

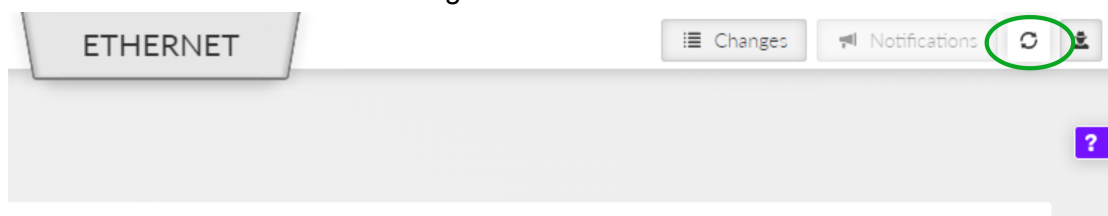


#### Note

It is possible to use this URL format to make a web browser's bookmark. Such bookmarks can be used for faster access to remote units.

## 6.6. Refresh settings

Refresh settings button (placed in the right corner of the web page header) triggers a feature which assures the user that he is working with current data.



Triggering the Refresh will upload current data from the unit to the web client.



Are you sure you want to refresh settings?

Latest settings data will be fetched from the device.

You have unsaved changes in your configuration. These will be lost.

Refresh Close



**Note**

Refresh deletes all non-saved changes which were done in the client.

### 6.7. Status overview

This feature provides a general overview about MIDGE3's individual SETTINGS (or DIAGNOSTICS) section by displaying diagnostic data relevant to the section. To update the data it is necessary to click the Refresh button. It is also possible to use auto refresh feature (Start auto refresh button), which automatically triggers Refresh after defined time period (3, 4, 5... 300 seconds).

**Status** Last refresh: 2022-10-13 09:14:16 Refresh

3 seconds Start auto refresh

Network interfaces

| Index | Interface name | MAC               | MTU [B] |
|-------|----------------|-------------------|---------|
| 10    | if_bridge      | 00:02:a9:20:09:e2 | 1500    |
| 11    | if_internet    | 00:02:a9:20:09:e6 | 1500    |
| 12    | if_rescue_net  | 00:02:a9:20:09:e3 | 1500    |

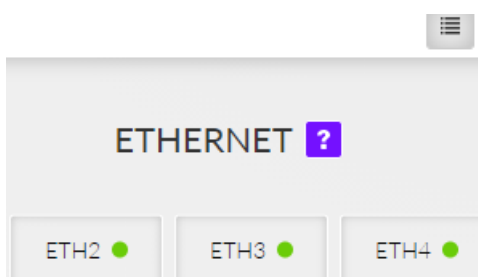
### 6.8. Help

This feature is available on individual web pages of the graphical user interface by clicking on the purple box with the question mark on the right upper corner (or in the middle) of the screen (according to the width of the screen).

ETHERNET Changes Notifications

ETH4 ETH5 ?





The content of the help is identical with the respective sub-chapter of the User manual.

## 6.9. Shortcuts

**Tab. 6.1: Table of shortcuts**

| Shortcut   | Access to           |
|------------|---------------------|
| Ctrl+Alt+C | Changes to commit   |
| Ctrl+Alt+N | Notification center |
| Ctrl+Alt+R | Remote access       |

## 7. Settings

Information provided in this chapter is identical with the content of Helps for individual menu. which will be gradually added on all screens.

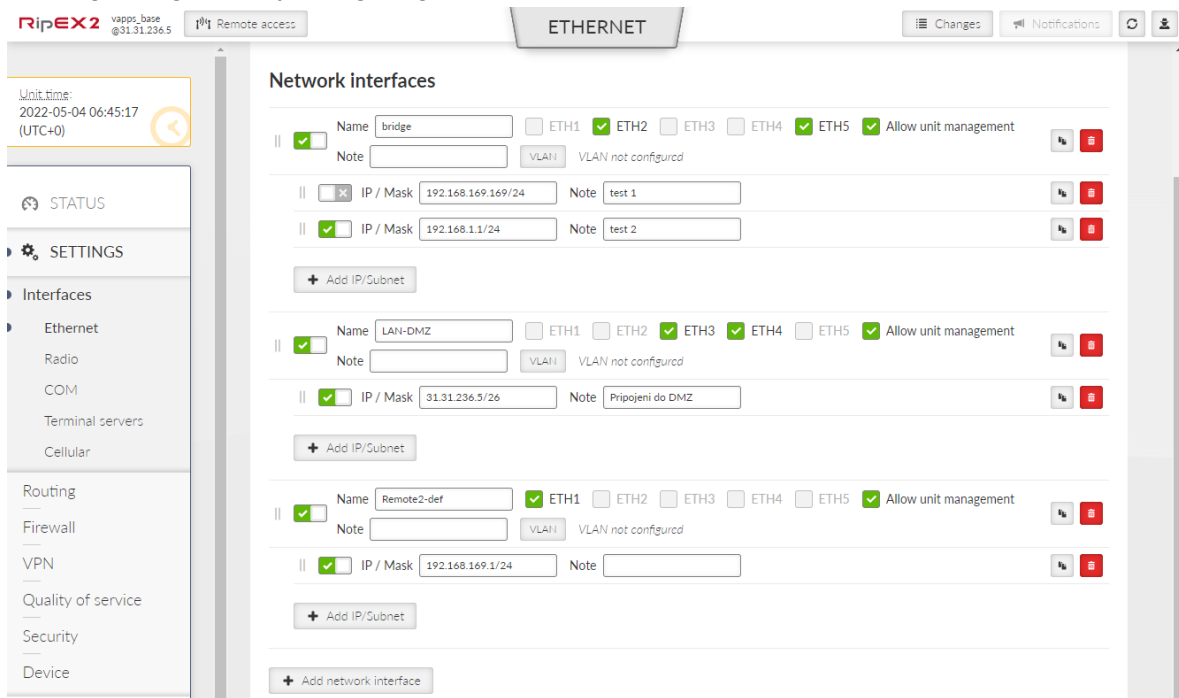
### 7.1. Interfaces

#### 7.1.1. Ethernet

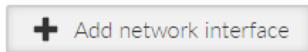
M!DGE3 provides 5 physical Ethernet ports ETH1, ETH2, ETH3, ETH4 and ETH5. ETH1 - ETH4 ports are metallic. ETH5 port is an SFP port. There is a possibility to define an Ethernet bridge - a logical Network interface - by bridging (joining) together multiple physical Ethernet interfaces. All interfaces bridged together share the same traffic.

##### 7.1.1.1. Network interfaces

The Network interface (technically - an Ethernet bridge) is identified by a name. The name always begins with a "LAN-" prefix. Multiple Network interfaces can be defined. Multiple physical Ethernet interfaces can be bridged together by using single Network interface.



The M!DGE3 cellular unit default setting bridges all Ethernet ports together. New Network interfaces can be defined to split the Ethernet traffic of the individual ports. Any single Ethernet port can be detached from an existing Network interface and added to another Network interface.



Single or multiple Ethernet subnets can be defined within one Network interface. Each subnet is identified by its IP / mask. Use the optional parameter Note to keep your network configuration in human readable manner.

**Enable / Disable**

Enables / disables the Network interface.

**Name**

Mandatory name of the Network interface.

**ETH1 - ETH5**

Range on Ethernet ports selected within the specific Network interface.

**Note**

If the Network interface has set up either a Radio interface or GRE L2 tunnel, it does not require any ETH ports.

**Allow unit management**

Enables / disables unit management for the specific Network interface.

**Add IP/Subnet**

Adds defined subnet to the Network interface.

**IP / Mask**

IP / mask of the specific Ethernet subnet (in CIDR notation). IP address represents the Network interface in the Layer 3 Ethernet network.

**Note**

Optional comment.

**VLAN**

Each Network interface can have one or more attached VLANs with one or more Subnets.

VLAN configuration - bridge ×

---

||

VLAN ID   Allow unit management  VLAN priority mapping

Note

---

---

**Enable / Disable**

Enables / disables VLAN.

**VLAN ID**

Number {0 – 4094}, default = 1  
Specifies the VLAN ID according to IEEE 802.1Q

**Allow unit management**

Allows / denies unit management for the specific VLAN. This switch is not connected with the Network interface switch with the same name, so only this VLAN can be used for diagnostics.

### VLAN priority mapping

Relates to QoS

### Attach VLAN to Network interface

Attaches VLAN to the defined network interface

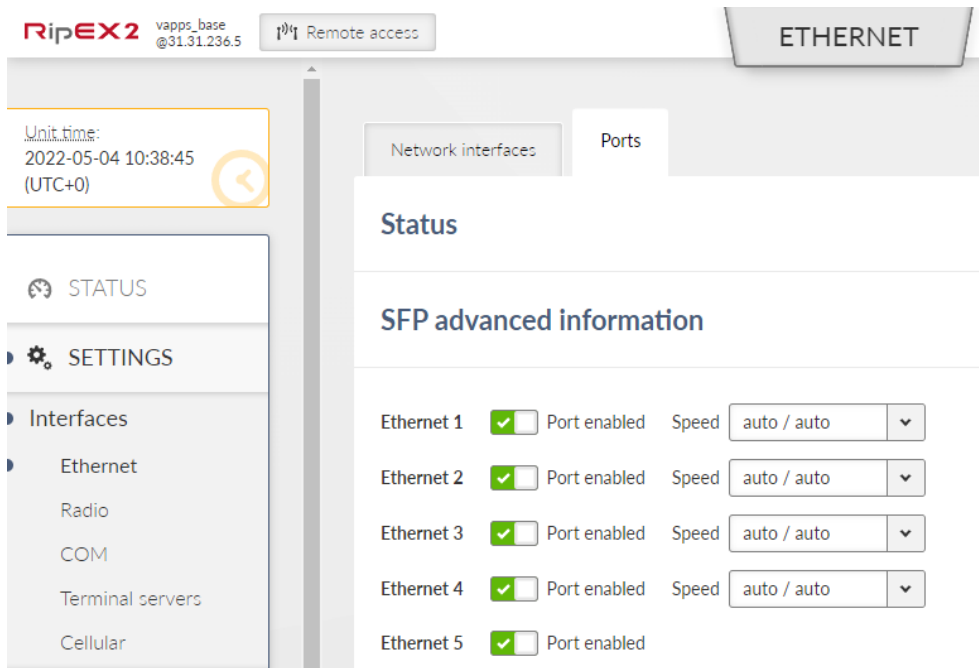
### Note

Optional comment.

### Add IP/Subnet

Adds defined subnet to the VLAN.

## 7.1.1.2. Ports



### Enable / Disable

Enables / Disables ETH ports (1 - 5) SW control.

### ETH1 - ETH4 speed

List box {auto / auto; auto / full; auto / half; 1000 Mbps / auto; 1000 Mbps / full; 1000 Mbps / half; 100 Mbps / auto; 100 Mbps / full; 100 Mbps / half; 10 Mbps / auto; 10 Mbps / full; 100 Mbps / half}, default = "auto / auto"

Defines the speed and half / full duplex traffic.



### Note

When several bridges are interconnected in the network, it is appropriate to switch on Spanning Tree Protocol (ADVANCED > Interfaces > Ethernet > STP) to prevent bridge loops and build a loop-free logical topology.

## 7.1.2. COM

Data incoming to the MIDGE3 unit from the COM port are received by the Protocol module. The Protocol module behavior depends on the Protocol selected. The incoming frame from the COM port is processed by the Protocol module, translated into UDP frame, forwarded to the MIDGE3 router module and further processed according to router rules. Such UDP frames received by the MIDGE3 unit from the MIDGE3 network (based on the unit IP address and UDP port of the Protocol module) are translated into original frame format (by the Protocol module) and send out through the COM port.

When extension module "C" is installed, two additional COM ports (RS232) are available. Their setting is similar to the COM1 port.

Unit time: 2021-06-17 10:52:50 (UTC+0)

COM1 ● COM2 ● COM3 ●

COM1 Enabled | UDP port: 8881

| COM port parameters    | Protocol parameters              |
|------------------------|----------------------------------|
| Type: RS232            | Protocol: Modbus RTU             |
| Baud rate [b/s]: 19200 | Mode of Connected device: Master |
| Data bits: 8           | Broadcast: On                    |
| Parity: None           | Broadcast address: 0             |
| Stop bits: 1           | Address translation: Mask        |
| Idle [ms]: 20          | Base IP / Mask: 10.0.0.1/24      |
| MRU [B]: 1500          | Destination (UDP port): COM1     |
| Flow control: None     |                                  |

The menu is divided to two parts:

### 7.1.2.1. COM port parameters

This settings of Baud rate, Data bits, Parity and Stop bits of COM port and setting of connected device must match.

**COM port parameters**

Type: RS232

Baud rate [b/s]: 19200

Data bits: 8

Parity: None

Stop bits: 1

Idle [ms]: 20

MRU [B]: 1500

Flow control: None

### Type

List box {possible values}, default = "RS232"  
COM port can be configured to either RS232 or RS485.

### Baud rate [b/s]

List box {standard series of rates from 600 to 1152000 b/s}, default = "19200"  
Select Baud rate from the list box: 600 to 1152000 b/s rates are available.  
Serial ports use two-level (binary) signaling, so the data rate in bits per second is equal to the symbol rate in bauds.

### Data bits

List box {5; 6; 7; 8}, default = 8, for COM3 (optional) only 8  
The number of data bits in each character.

### Parity

List box: {None; Odd; Even}, default = "None"  
Wikipedia: Parity is a method of detecting errors in transmission. When parity is used with a serial port, an extra data bit is sent with each data character, arranged so that the number of 1-bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1-bits, then it must have been corrupted. However, an even number of errors can pass the parity check.

### Stop bits

List box {1; 2 (1.5)}, default = 1, for COM3 (optional) only 1, for 5 data bits the 1.5 length of stop bits is used instead of 2  
Wikipedia: Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronize with the character stream.

### Idle [ms]

Number {10 – 16383}, default = 20  
This parameter defines the maximum gap (in milliseconds) in the received data stream. If the gap exceeds the value set, the link is considered idle, the received frame is closed and forwarded to the network.

### MRU [B]

Number {1 – 2047}, default = 1500  
MRU (Maximum Reception Unit) — an incoming frame is closed at this size even if the stream of bytes continues. Consequently, a permanent data stream coming to a COM results in a sequence of MRU-sized frames sent over the network.



#### Note

2. This MRU and the MTU in Cellular settings are independent, however MTU should be greater or equal to MRU.

### Flow control

List box {None; RTS/CTS}, default = "None"  
RTS/CTS (Request To Send / Clear To Send) hardware flow control (handshake) between the DTE (Data Terminal Equipment) and M!DGE3 (DCE - Data Communications Equipment) can be enabled in order to pause and resume the transmission of data. If RX buffer of M!DGE3 is full, the CTS goes down.



#### Note

RTS/CTS Flow control requires a 5-wire connection to the COM port.

**Buffer flush time [ms]**

Number {0 – 65535}, default = 0

This parameter can be used to prevent unwanted deadlock of the serial communication. The timer is reset by every received or transmitted packet over the COM port. When the timer expires, the protocol status is reset and the packet buffer is cleared. Setting parameter to 0 disables the feature. This parameter is available only via ADVANCED menu.

**7.1.2.2. Common Protocol parameters**

Each SCADA protocol used on serial interface is more or less unique. The COM port protocol module performs conversion to standard UDP datagrams to travel across MIDGE3 Cellular network. The same settings are valid for Terminal servers as well (for more details about TS see *Section 7.1.3, "Terminal servers"*).

**Protocol parameters**

Protocol \*  ▼

Broadcast \*  ▼

Address translation \*  ▼

Base IP / Mask \*

Destination (UDP port) \*  ▼

**Protocol**

List box {None; Async Link; COMLI; DNP3; DF1; IEC101; Mars-A; Modbus RTU; PR2000; RDS; S3964R; SAIA S-BUS; UNI}, default = "None"

**Address translation**

List box {Mask; Table}, default = "Mask"

SCADA protocol address is translated to the IP address using either Mask (common rule for all addresses) or Table (specific rule per address) type of conversion

Address translation \*  ▼

Base IP / Mask \*

Destination (UDP port) \*  ▼

**Base IP / Mask**

A part of Base IP address defined by this Mask is replaced by 'Protocol address'. The SCADA protocol address is typically 1 byte long, so Mask 24 (255.255.255.0) is most frequently used. This IP address is used as a destination IP address of the UDP datagram into which the serial SCADA packet received from COM is encapsulated.

**Destination UDP port**

List box {Manual; COM1 – COM3; TS1 – TS5}, default = "COM1"

The same UDP port will be used for all destination. This UDP port is used as the destination UDP port in UDP datagram in which serial SCADA packet received from COM is encapsulated. Default UDP ports for COM or Terminal servers can be used or UDP port can be set manually. If the des-

destination IP address belongs to a M!DGE3 and the UDP port is not assigned to COM or to a Terminal server or to any other special SW module running in the destination M!DGE3, the packet is discarded.



**Note**

Default UDP port for serial interface in M!DGE2 is 8882. Keep this in mind if combining M!DGE2 with M!DGE3/RipEX2.

**Protocol address (from)**

This is the address which is used by SCADA protocol.

The typical Protocol address length is 1 Byte. Some protocols, e.g. DNP3 are using 2 Bytes long addresses.

**Protocol address (to)**

Several consecutive SCADA addresses shall be translated using one rule.

**IP address (base)**

IP address to which Protocol address will be translated. This IP address is used as a destination IP address of the UDP datagram into which the serial SCADA packet received from COM is encapsulated. When several addresses are used, this will be the first IP address, the following one will have +1 etc.

**Destination (UDP port)**

List box {MANUAL; COM1 – COM3; TS1 – TS5}, default = "COM1"

This is UDP port number which is used as destination UDP port into UDP datagram in which the serial SCADA message, received from COM, is encapsulated. Different Destination UDP ports can be used in different rules.

**Address translation: Mask**



**Note**

All IP addresses used have to be within the same subnet, which is defined by this Mask  
The same UDP port is used for all the SCADA units, which results in the following limitations:

SCADA devices on all sites have to be connected to the same interface

Only one SCADA device to one COM port can be connected, even if the RS485 interface is used.

**Address translation: 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 connected via the RS485 interface, their multiple "Protocol addresses" are translated to the same IP address and UDP port pair.



Address translation \*  

## Protocol address translation



|   |  |
|---|--|
| <p><b>● First unit</b> <input type="button" value="edit"/></p> <p>Protocol address: 1 <input type="button" value="delete"/></p> <p>IP address: 10.11.12.1</p> | <p><b>● Second unit</b> <input type="button" value="edit"/></p> <p>Protocol address: 2 <input type="button" value="delete"/></p> <p>IP address: 10.11.15.1</p> |
| <p><b>● Third unit</b> <input type="button" value="edit"/></p> <p>Protocol address: 3 <input type="button" value="delete"/></p> <p>IP address: 10.12.17.6</p> |  |

### COM port parameters

Type \*

Baud rate [b/s] \*

Data bits \*

Parity \*

Stop bits \*

Idle [B] \*

MRU [B] \*

Flow control \*

### Protocol parameters

Protocol \*

Broadcast \*

### Protocol address translation

|   |  |   |
|---|--|---|
| <p><b>● First unit</b> <input type="button" value="edit"/></p> <p>Protocol address: 1 <input type="button" value="delete"/></p> <p>IP address: 10.11.12.1</p> | <p><b>● Second unit</b> <input type="button" value="edit"/></p> <p>Protocol address: 2 <input type="button" value="delete"/></p> <p>IP address: 10.11.15.1</p> | <p><b>● Third unit</b> <input type="button" value="edit"/></p> <p>Protocol address: 3 <input type="button" value="delete"/></p> <p>IP address: 10.12.17.6</p> |
|---|--|---|

### Edit protocol address translation

Enabled

Note

Protocol address (from) \*

Protocol address (to) \*

IP address (base) \*

Destination (UDP port) \*

**Note**

You may add a note to each address with your comments (UTF8 is supported) for your convenience.

**7.1.2.3. Individual protocol parameters**

Some of the SCADA protocols are able to setup additional Slave device response behavior.

### Response target mode

List box {LASTRCV; TARGET}, default = "LASTRCV"

Response for the incoming frame shall be directed to the IP address of the Master which sent the frame (LASTRCV) or to a specified IP address (TARGET).

### Response target IP

IP address to which the response is sent when TARGET is chosen in the Response target mode.

#### 7.1.2.3.1. None

The None protocol switches the COM port off. All incoming data will be thrown away, no data will be sent into the COM interface.

#### 7.1.2.3.2. Async link

Async link creates an asynchronous link between two COM ports on different RipEX2 (or MIDGE3) units. Received frames from COM port or from a Terminal server are sent without any processing transparently via router to the set IP destination and UDP port. Received frames from the network are sent to COM or Terminal server according to Destination (UDP port) parameter.

**Protocol parameters**

Protocol \* Async Link ▼

Destination IP \* 192.168.0.0

Destination (UDP port) \* COM1 ▼

Transmit as broadcasts \* Off ▼

Accept broadcasts \* Off ▼

### Destination IP

Defines destination IP address of RipEX2 (or MIDGE3).

#### 7.1.2.3.3. COMLI

COMLI is a serial polling-type communication protocol used by Master-Slave application. Within one MIDGE3 network more COMLI Masters can be employed and one Slave can be polled by more Masters. Broadcast packets are not used.

The frame of COMLI protocol is sent transparently, but without STX, ETX and BCC. STX (start of data), ETX (end of data) and BCC (8-bit XOR) are added on the receiving participant. While transfer, data integrity is properly secured by individual protocol checksums.



### Note

The COMLI protocol in the RipEX2 (or MIDGE3) is not fully compatible on COM port with RipEX and MR modems. MIDGE3 implementation is not supporting "Intercharacter tx delay".

**Mode of Connected device: MASTER**

| Protocol parameters      |  |
|--------------------------|--|
| Protocol                 | COMLI <input type="button" value="v"/>     |
| Mode of Connected device | Master <input type="button" value="v"/>    |
| Congestion timeout [ms]  | <input type="text" value="3000"/>          |
| Address translation      | Mask <input type="button" value="v"/>      |
| Base IP / Mask           | <input type="text" value="10.10.10.1/24"/> |
| Destination (UDP port)   | COM1 <input type="button" value="v"/>      |

**Congestion timeout [ms]**

Number {0 – 65535}, default = 3000, 0 switches this functionality off

Timeout for checking of the duplicity of two following frames. Used when the very same frame is incoming via COM port within the timeout measured from the moment of dispatch of the previous frame.

**Mode of Connected device: SLAVE**

| Protocol parameters      |         |
|--------------------------|---------|
| Protocol                 | COMLI   |
| Mode of Connected device | Slave   |
| Response timeout [ms]    | 1000    |
| Response target mode     | LASTRCV |

**Response timeout [ms]**

Number {0 – 16383}, default = 1000

COMLI protocol response timeout is used for waiting on COM port for the response of connected device.

**Response target mode**

List box {LASTRCV; TARGET}, default = "LASTRCV"

Slave response will be sent to the address of the last received request (LASTRCV) or to the specified **Response target IP** address (TARGET).

**7.1.2.3.4. 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!DGE3 configuration. The DNP3 allows both Master-Slave polling as well as report-by-exception communication from the remote units.

| Protocol parameters      |             |
|--------------------------|-------------|
| Protocol *               | DNP3        |
| Broadcast *              | On          |
| Address translation *    | Mask        |
| Base IP / Mask *         | 10.0.0.1/24 |
| Destination (UDP port) * | COM1        |

The common parameters (e.g. address translation) shall be set.

**7.1.2.3.5. DF1**

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 M!DGE3 configuration.

| Protocol parameters      |               |
|--------------------------|---------------|
| Protocol *               | DF1 ▼         |
| Duplex mode *            | Full duplex ▼ |
| Block control mode *     | BCC ▼         |
| Broadcast *              | On ▼          |
| Address translation *    | Mask ▼        |
| Base IP / Mask *         | 10.0.0.1/24   |
| Destination (UDP port) * | COM1 ▼        |

### Duplex mode

List box {Full duplex; Half duplex}, default = "Full duplex"

Mode of DF1 protocol operation: Only Full duplex mode is implemented now.

### DF1 advanced parameters

Protocol DF1 supports protocol local acknowledgment. Typically the default setting shall be used. In case a need it is possible to change ACK parameters in ADVANCED > Generic > com\_x\_prot/Protocol\_DF1 menu.

|                  |      |
|------------------|------|
| ACK Locally      | On ▼ |
| Repeats          | 2    |
| ACK timeout [ms] | 1000 |

### ACK locally

List box {On; Off}, default = "On"

Allows to switch On / Of the local ACK

### Repeats

Number {0 – 31}, default = 2

Sets number of repeats when local ACK is not received.

### ACK timeout [ms]

Number {0 – 1683}, default = 1000

Timeout of waiting for ACK.

### 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.



### Note

According to the DF1 specification, packets for the destination address 0xFF are considered broadcasts. Hence when Broadcast is On, packets with this destination are handled as broadcasts.

### 7.1.2.3.6. IEC101

| Protocol parameters      |             |
|--------------------------|-------------|
| Protocol                 | IEC101      |
| Mode of Connected device | Master      |
| Address mode             | IEC101      |
| Broadcast                | On          |
| Address translation      | Mask        |
| Base IP / Mask           | 10.0.0.1/24 |
| Destination (UDP port)   | COM1        |

#### Mode of Connected device

List box {Master; Slave; Combined}, default = "Master"



#### Note

For connected SCADA Master set Master, for connected SCADA Slave set Slave.

#### Address mode

List box {IEC101; 2B ADDR; TELEGYR; SINAUT; No addr}, default = "IEC101"

### 7.1.2.3.7. Mars-A

MARS-A is a full duplex protocol featuring:

- 32bit long addresses
- error detection (based on 16 bit checksum (XOR) or 16 bit CRC)
- error correction

MARS-A was widely used by legacy RACOM radio modems in the MORSE system from the year 1999.

The new implementation of this protocol in RipEX2 or MIDGE3 is limited to the parts of the complex protocol which can be used together with modern packet type of these routers:

USER DATA (0x09) from router to the serial interface (e.g. to RTU),

USER DATA (0x09) and PROT DATA (0x0A) from serial interface (e.g. from RTU) to the router.

Mars-A headers are removed from the packet prior to transmitting to the network - only data are transmitted.

### Protocol parameters

|                        |  |   |
|------------------------|--|---|
| Protocol               | <input type="text" value="Mars-A"/>      | ▼ |
| Broadcast              | <input type="text" value="On"/>          | ▼ |
| Repeats                | <input type="text" value="3"/>           |   |
| ACK timeout [ms]       | <input type="text" value="1000"/>        |   |
| CRC                    | <input type="text" value="Off"/>         | ▼ |
| Address translation    | <input type="text" value="Mask"/>        | ▼ |
| Base IP / Mask         | <input type="text" value="10.0.0.1/24"/> |   |
| Destination (UDP port) | <input type="text" value="COM1"/>        | ▼ |

#### ACK timeout [ms]

Number {0 – 16383}, default = 1000  
Serial interface acknowledge timeout.

#### Repeats

Number {0 – 31}, default = 3  
Number of repeats. Repetition is triggered when NAK frame is received or if ACK frame was not received within ACK timeout.

#### Security bit

List box {On; Off}, default = "Off"  
Needed for compatibility with legacy MORSE network implementations. This parameter does not change protocol behavior.

#### CRC

List box {On; Off}, default = "Off"  
Error detection algorithm:

- On - CRC algorithm is used
- Off - XOR algorithm is used

#### 7.1.2.3.8. Modbus RTU

Modbus RTU is a serial polling-type communication protocol used by Master-Slave application.

**Protocol parameters**

|                          |             |        |
|--------------------------|-------------|--------|
| Protocol                 | Modbus RTU  | ▼      |
| Mode of Connected device | Master      | ▼      |
| Broadcast                | On          | ▼      |
| Broadcast address        | 0           | ⬆️⬇️⬆️ |
| Address translation      | Mask        | ▼      |
| Base IP / Mask           | 10.0.0.1/24 |        |
| Destination (UDP port)   | COM1        | ▼      |

**Mode of Connected device**

List box {Master; Slave}, default = "Master"

**Mode of connected device: MASTER**

**Mode of connected device: SLAVE**

**Protocol parameters**

|                          |            |        |
|--------------------------|------------|--------|
| Protocol                 | Modbus RTU | ▼      |
| Mode of Connected device | Slave      | ▼      |
| Broadcast                | On         | ▼      |
| Response timeout [ms]    | 300        | ⬆️⬇️⬆️ |
| Response target mode     | TARGET     | ▼      |
| Response target IP       | 0.0.0.0    |        |

**Response timeout**

Number { 0 – 8190}, default = 300

The Response timeout parameter controls how long the unit waits for an acknowledgement frame. The timeout is started when the original frame received from the Cellular channel is transmitted to the connected device (over the serial channel). Transmission of any other frame to the connected device is temporarily blocked, whilst Response timeout is active. Response timeout = 0 disables this feature.

**7.1.2.3.9. PR2000**

PR2000 is an abbreviation for the PROTEUS 2000 SCADA protocol. This protocol is used in Master-Slave applications.

The PR2000 protocol is implemented in a fully transparent manner. The original protocol frames are transported over the RipEX network in their entirety.



| Protocol parameters      |             |
|--------------------------|-------------|
| Protocol                 | PR2000      |
| Mode of Connected device | Master      |
| Broadcast                | On          |
| Address translation      | Mask        |
| Base IP / Mask           | 10.0.0.1/24 |
| Destination (UDP port)   | COM1        |

### 7.1.2.3.10. Siemens 3964(R)

The 3964 protocol is utilized by the Siemens Company as a Point-to-Point connection between two controllers. Meanwhile it has developed into 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) handles only the link layer (L2 in OSI model), hence RipEX uses a similar way to read "SCADA address" as in UNI protocol.

There is a handshake STX(0x02) – DLE(0x10) on the start of communication and DLE+ETX – DLE on the end. This handshake is performed by RipEX locally, it is not transferred over the RipEX 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.

**Master**

| Protocol parameters      |             |
|--------------------------|-------------|
| Protocol                 | S3964R      |
| Mode of Connected device | Master      |
| Address mode             | Binary (1B) |
| Address position         | 1           |
| Broadcast                | On          |
| Broadcast address        | 255         |
| DLE timeout [ms]         | 1000        |
| Repeats                  | 3           |
| Priority                 | High        |
| BCC                      | On          |
| Address translation      | Mask        |
| Base IP / Mask           | 10.0.0.1/24 |
| Destination (UDP port)   | COM1        |

**Address mode**

List box {Binary (1 B); Binary (2B LSB first); Binary (2B MSB first)}, default = "Binary (1 B)"  
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**

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



**Note**

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

**Slave**

**Protocol parameters**

Protocol  ▼

Mode of Connected device  ▼

Broadcast  ▼

DLE timeout [ms]  ▼

Repeats  ▼

Priority  ▼

BCC  ▼

Response target mode  ▼

Response target IP

**DLE timeout [ms]**

Number {300 – 8190}, default = 1000

RipEX expects a response (DLE) from the connected device (RTU) within the set timeout. If it is not received, RipEX repeats the frame according to the “Retries” setting.

**Retries [No]**

Number {0 – 7}, default = 3

When DLE packet is not received from the connected device (RTU) within the set DLE timeout, RipEX 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 equipments want to start communication. In such a case, one unit has to have a priority. If the Priority is High, RipEX waits for DLE. When it is Low, RipEX sends DLE.

**Note**

Obviously, two pieces of equipment 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.

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

**7.1.2.3.11. SAIA S-Bus**

SAIA S-Bus protocol was widely used by legacy RACOM radio modems in the MORSE system. The S-Bus protocol is implemented as an access module for communication with the SAIA PCD device. The protocol is a MASTER/SLAVE type; the MASTER does not have its own address. There can be at most 254 SLAVES, the address 255 is reserved for broadcast transmitting which is not acknowledged.

The physical layer of the S-Bus protocol uses the RS232 or RS485 interface. The broadcast address 255 is not supported for M!DGE3.

Protocol frame has to be as whole received in the one buffer, so the IDLE parameter should be set properly. The S-bus protocol header does not always contain the length of the data, so it is not possible to work with fragmented and defragmented frames.

### Protocol parameters

|                                   |             |   |
|-----------------------------------|-------------|---|
| Protocol                          | SAIA S-BUS  | ▼ |
| Mode of Connected device          | Master      | ▼ |
| Broadcast                         | On          | ▼ |
| Address translation               | Mask        | ▼ |
| Base IP / Mask                    | 10.0.0.1/24 |   |
| Destination (UDP port)            | COM1        | ▼ |
| Transmission control timeout [ms] | 11500       |   |
| Protocol mode                     | Break       | ▼ |
| Break validity time [ms]          | 1000        |   |

### Mode of connected device

List box {Master; Slave; Slave Plus}, default= "Master"

**Master** and **Slave** behaves like standard Master or Slave Saia PCD. The **Slave Plus** mode allows to behave in limited way as a Master and sends to other Slave/Slave Plus write command (read command is not allowed).

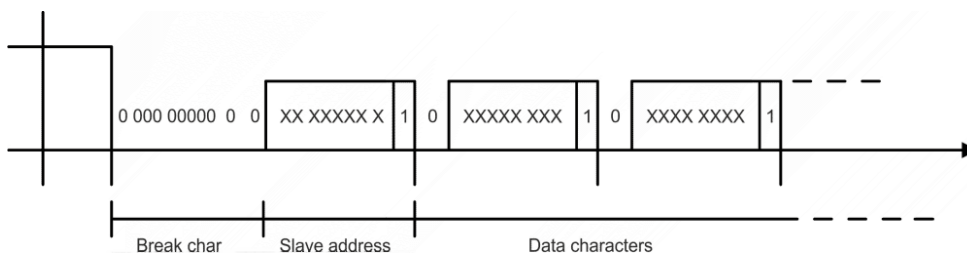
### Protocol mode

List box {Break; Data}, default ="Break"

Break or Data protocol modes can be used.

### Break mode (SM0)

The frames are synchronised by the break characters of a configured length which are sent before the addressed command.

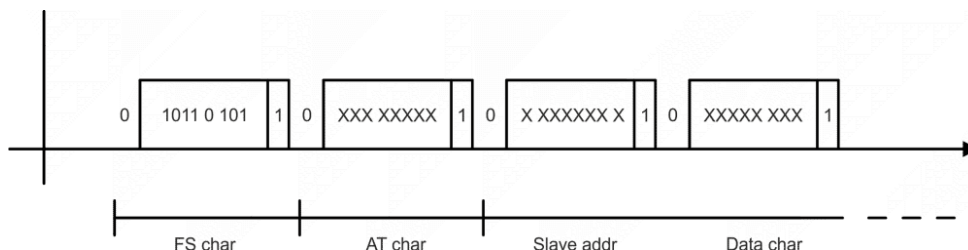


Break mode is available only with COM port, it is not implemented on TS (the break signal is not available there). The Break signal check is very rough (with step of 100 ms) due to Linux kernel limitations.

### Data mode (SM2)

Frame synchronization is accomplished by inserting the character 0xB5 in the beginning of frame. If another character 0xB5 should appear in the frame, then it is replaced by the following DLE sequence:

| Character | DLE sequence |
|-----------|--------------|
| 0x85      | 0xC500       |
| 0xC5      | 0xC501       |

**Note**

See details of the RACOM's implementation on <https://www.racom.eu/eng/support/prot/sbus/index.html><sup>1</sup>

**Mode of Connected device: MASTER****Transmission control timeout [ms]**

Number {0 – 65535}, default = 11500

Master timeout. This timeout is reset after receiving of an answer from Slave or a frame incoming from the connected master.

**Mode of Connected device: SLAVE**

**Response timeout [ms]** Number {0 – 16383}, default = 300

Slave's response timeout - waiting for response, otherwise the reply to master is resent.

**Repeats**

Number {0 – 7}, default = 3

Number of repeats when the response from master is not received.

**Break mode**

(additional parameter)

**Master, Slave Plus****Break validity time [ms]**

Number {0 – 5000}, default = 1000

**Slave, Slave Plus****Break length [ms]**

Number {0 – 128}, default = 2

Length of break in ms.

**7.1.2.3.12. RDS**

RDS protocol is a protocol used in MRxx networks. It supports network communication; any node in the network can talk to any other (unlike Master-Slave type of protocols). The RDS protocol is typically used when combining RipEX and MRxx networks or SCADA networks adapted to MRxx networks. Frames are received from the Cellular channel and sent to COM1-3 or Terminal server 1-5 according to UDP port settings and vice versa - from wire to Cellular channel.

<sup>1</sup> <https://www.racom.eu/eng/support/prot/sbus/index.html>

### Protocol parameters

|                        |  |   |
|------------------------|--|---|
| Protocol               | <input type="text" value="RDS"/>         | ▼ |
| ACK                    | <input type="text" value="On"/>          | ▼ |
| ACK timeout [ms]       | <input type="text" value="1000"/>        |   |
| Repeats                | <input type="text" value="3"/>           |   |
| Local response address | <input type="text" value="0"/>           |   |
| Address translation    | <input type="text" value="Mask"/>        | ▼ |
| Base IP / Mask         | <input type="text" value="10.0.0.1/24"/> |   |
| Destination (UDP port) | <input type="text" value="MANUAL"/>      | ▼ |
| UDP port               | <input type="text" value="50000"/>       |   |

#### ACK

List box {On; Off}, default = "On"

Frame acknowledgement when transmitted over wire (COM or Ethernet) interface. ACK (0x06) frames are transmitted on successful reception and NAK (0x15) on unsuccessful frame reception.

#### ACK timeout [ms]

Number {0 – 16383}, default = 1000



#### Note

ACK timeout is measured from the beginning of the packet transmission.

When "ACK" is enabled, RipEX is waiting "ACK timeout [ms]" after transmitting frame to receive acknowledgement. If the ACK frame isn't received, the frame is re-transmitted. Frame re-transmission happens up to "Repeats" number of times.

#### Repeats

Number {0 – 31}, default = 3

Number of frame re-transmissions.

#### Local response address

Number {0 – 255}, default = 0

This address is used only with status query (0x51). Response of M!DGE3 is "0x54 <Local response address> 0x00".

#### 7.1.2.3.13. UNI

UNI is the 'Universal' protocol utility designed for RipEX. It is supposed to be used when the required application protocol is not available in RipEX and the network communication is using addressed mode (which is a typical scenario). The key prerequisite is: messages generated by the Master application device must always contain the respective Slave address and the address position, relative to the beginning of the message (packet, frame), is always the same (**Address position**). Generally, two communication modes are typical for UNI protocol: In the first one, communication is always 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 packets generation on remote sites are possible.

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

**Protocol parameters**

Protocol

Mode of Connected device

Address mode

Address position

Poll response control

Broadcast

Broadcast address

Address translation

Base IP / Mask

Destination (UDP port)

#### Mode of Connected device

List box: {Master, Slave}, default = Master

#### Address mode

List box {Binary (1B); ASCII (2B); Binary (2B LSB first); Binary (2B MSB first)}, default = "Binary (1B)"

Protocol address format and length (in Bytes). 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 (the ASCII-2-Byte format function will be available in a future FW release).

#### Address position

Number {1 – 255}, default = 1

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.

#### Poll response control

List box {On; Off}, default = "On"

"On" – The Master accepts only one response per a request and it must come from the specific remote to which the request has been 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 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 RF channel - all packets are passed to the application, including broadcasts. That allows e.g. spontaneous packets to be generated at remote sites. This mode is suitable for Master-Master communication scheme or a combination of the UNI and ASYNC LINK protocols.

**Mode of Connected device: SLAVE**

|                          |       |   |
|--------------------------|-------|---|
| Mode of Connected device | Slave | ▼ |
| Broadcast                | On    | ▼ |

**7.1.3. Terminal servers**

Generally, a Terminal Server (also referred to as a Serial Server) enables connection of devices with serial interface to a M!DGE3 over the local area network (LAN). It is a virtual substitute for devices used as serial-to-TCP (UDP) converters.

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!DGE3, user data extracted from TCP messages and processed like it comes from a COM port. When data reaches the destination M!DGE3, it can be transferred to the RTU either via a serial interface or via TCP (UDP), using the Terminal server again.

The screenshot shows the 'SETTINGS' menu with 'Terminal servers' selected. At the top, there are five terminal server status indicators: TS1 (green), TS2 (grey), TS3 (grey), TS4 (grey), and TS5 (grey). Below this, a checkbox for 'TS1' is checked, with the text 'Enabled | UDP port: 8892'. The 'Terminal server parameters' section includes: 'Type' set to 'UDP', 'TCP inactivity [s]' set to '120', 'Source (my) port' set to '50001', 'Destination (peer) IP' set to '0.0.0.0', and 'Destination (peer) port' set to '0'. The 'Protocol parameters' section includes: 'Protocol' set to 'Async Link', 'Destination IP' set to '192.168.0.0', 'Destination (UDP port)' set to 'TS1', 'Transmit as broadcasts' set to 'Off', and 'Accept broadcasts' set to 'Off'. The left sidebar contains navigation options: STATUS, SETTINGS, Interfaces (Ethernet, Radio, COM), Terminal servers, Routing, Firewall, VPN, Security, Device, DIAGNOSTICS, and ADVANCED.



Up to 5 independent Terminal servers can be set up. Each one can be either TCP or UDP Type, **TCP Inactivity** is the timeout in seconds for which the TCP socket in M!DGE3 is kept active after the last data reception or transmission. As source IP address of a Terminal server will be used the IP address of the M!DGE3 ETH interface (**Local preferred source address** if exists see *Section 7.2.1, “Static”*), **Source (my) port** can be set as required. **Destination (peer) IP** and **Destination (peer) port** values belong to the locally connected application (e.g. a virtual serial interface). In some cases, applications dynamically change the IP port with each datagram. In such a case set Destination port=0. M!DGE3 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!DGE3 and locally connected application to any value up to 10 on each Terminal server. **Protocol** follows the same principles as a protocol on COM interface.

For details of settings see *Section 7.1.2.2, “Common Protocol parameters”*.



### Note

Max. user data length in a single datagram processed by the Terminal server is 8192 bytes.

## 7.1.4. Cellular

M!DGE3 can have up to two Cellular modules (MAIN and optional EXT). All features are identical for both. If both modules are used, each SIM card has to be assigned to a specific module.

APN must always be set up, all other parameters can keep their default values.

### 7.1.4.1. MAIN/EXT

The screenshot displays the M!DGE3 web interface for configuring Cellular settings. The top navigation bar includes 'Remote access', 'CELLULAR', 'Changes', 'Notifications', and user icons. The left sidebar lists various system settings. The main content area is titled 'CELLULAR' and shows the 'MAIN' module configuration. Under 'Status', 'Cellular MAIN' is 'Enabled'. The 'Parameters' section includes dropdown menus for 'Masquerade' (On), 'Allow unit management' (On), 'Link testing' (Off), and 'Profile switching' (Off). The 'Cellular profiles' section shows a table with one profile: '0' with 'Preferred service: 4G (LTE) first'. An '+ Add' button is visible at the bottom.

#### Enable / Disable cellular MAIN/EXT:

Enables / Disables the cellular MAIN/EXT. When disabled (default), the module power is off.



**Note**

Routing **Mode** “WWAN MAIN/EXT” is added to the Static routing rules definition. When this mode is selected, the routing Gateway parameter is ignored. The packet is forwarded to the Cellular (WWAN) interface instead.

Routing rules are enabled / disabled automatically when the Cellular (WWAN) interface is opened / closed.

No routing rules are added automatically after configuring a new cellular profile. Add all appropriate routing manually (e.g., default route 0.0.0.0/0 via WWAN interface).



**Note**

This section closely cooperates with *Section 7.7.2, “SMS”*.

**7.1.4.1.1. Parameters**

**Parameters**

|                       |                                  |   |
|-----------------------|----------------------------------|---|
| Masquerade            | <input type="text" value="On"/>  | ▼ |
| Allow unit management | <input type="text" value="On"/>  | ▼ |
| Link testing          | <input type="text" value="Off"/> | ▼ |
| Profile switching     | <input type="text" value="Off"/> | ▼ |

**Masquerade**

List box {On; Off}, default = "On"

Enables / Disables SNAT (MASQUERADE) for the packets outgoing from the WWAN interface.

When on, the source address of packets outgoing via the Cellular WWAN interface will be changed to the address assigned to this interface (WWAN IP address is used instead of internal/LAN IP addresses). Returning packets will be correctly routed back to its original source (internal device).

**Allow unit management**

List box {On; Off}, default = "On"

Allows to manage the unit over WWAN interface.

**Link testing**

List box {On; Off}, default = "Off"

Enables / Disables Link testing.

**Profile Switching**

List box {On; Off}, default = "Off"




Enables / Disables automatic Profile switching.

**7.1.4.1.2. Cellular profiles**

Set of defined profiles (at least one profile is required), which are setting parameters of requested service of the network (e.g APN).

## Cellular profiles

Minimum number of 1 rows of table Cellular profiles has been reached.

|                                      |   |
|--------------------------------------|---|
| ● 0                                  |  |
| Preferred service:<br>4G (LTE) first |  |
|                                      |  |

+ Add

Edit

×

|                         |                                     |
|-------------------------|-------------------------------------|
| Enable profile          | <input checked="" type="checkbox"/> |
| SIM                     | SIM1 ▼                              |
| Access point name (APN) | internet                            |
| Authentication          | None ▼                              |
| Preferred service       | 4G (LTE) first ▼                    |
| Header compression      | Off ▼                               |
| Data compression        | Off ▼                               |
| Network selection       | Automatic ▼                         |
| MTU [B]                 | 1500                                |
| Note                    |                                     |

Confirm and close

Close

### Enable profile

Enables / Disables specific profile.

### Access point name (APN)

String {up to 99 char}, default = <empty>

The APN for access into the cellular network. Valid APN is provided by customers Cellular provider.

### Authentication

List box {None; PAP (legacy); CHAP}, default = "None"

Selects the method of authentication into the APN.

#### None

No authentication is used for the APN access.

#### PAP (legacy)

PAP (Password Authentication Protocol) authentication. We do not recommend to use this option because of security issues (the option is provided to offer legacy systems compatibility). Username and Password are required.

### CHAP

CHAP (Challenge-Handshake Authentication Protocol) authentication. Username and Password are required.

### Preferred service

List box {2G (GSM) first; 2G (GSM) only; 3G (UMTS) first; 3G (UMTS) only; 2G/3G (GSM/UMTS) only; 4G (LTE) first; 4G (LTE) only; 3G/4G (UMTS/LTE) only}, default = "4G (LTE) first"  
Sets preferences and/or permission of the individual cellular network services.

### Header compression

List box {On; Off}, default = "Off"  
Enables / Disables the user data traffic IP headers compression. Not used with 4G service.

### Data compression

List box {On; Off}, default = "Off"  
Enables / Disables the user data traffic data compression. Not used with 4G service.

### Network selection

List box {Automatic; Prefer manual; Lock to manual; Lock to home}, default = "Automatic"  
Defines the network selection preferences:

#### Automatic

Network is selected automatically.

#### Prefer manual

The network according to the **Location area identity (LAI)** is preferred. Another network will be selected when the preferred network is not available.

#### Lock to manual

Only the LAI filled in the **Location area identity (LAI)** parameter will be used.

#### Lock to home

Only the home network will be used (if the SIM supports PLMN reading). This option can also be used as a "switch-off" for the roaming.

### Location area identity (LAI)

String {00000 – 999999}, default = 00000

The Public Land Mobile Network (PLMN) identification number of the cellular network.

This parameter occurs only, if parameter **Network selection** is set to "Prefer manual" or "Lock to manual".

### MTU [B]

Number {70 – 1500}, default = 1430

Outgoing packets MTU. Default value matches to the value of the mPLS83W module and it is the most common value within cellular networks.

Minimum MTU value for IPv6 (Babel) = 1280 B.

### Note

Optional comment.

### 7.1.4.1.3. Link testing

Testing not only the connection to the cellular network (Connection check), but the connection with the destination address(es) as well (Link testing). Tests are in form of sending ICMP ping to defined address(es) and waiting for response. This section occurs only, if parameter **Link testing** is set to "On".

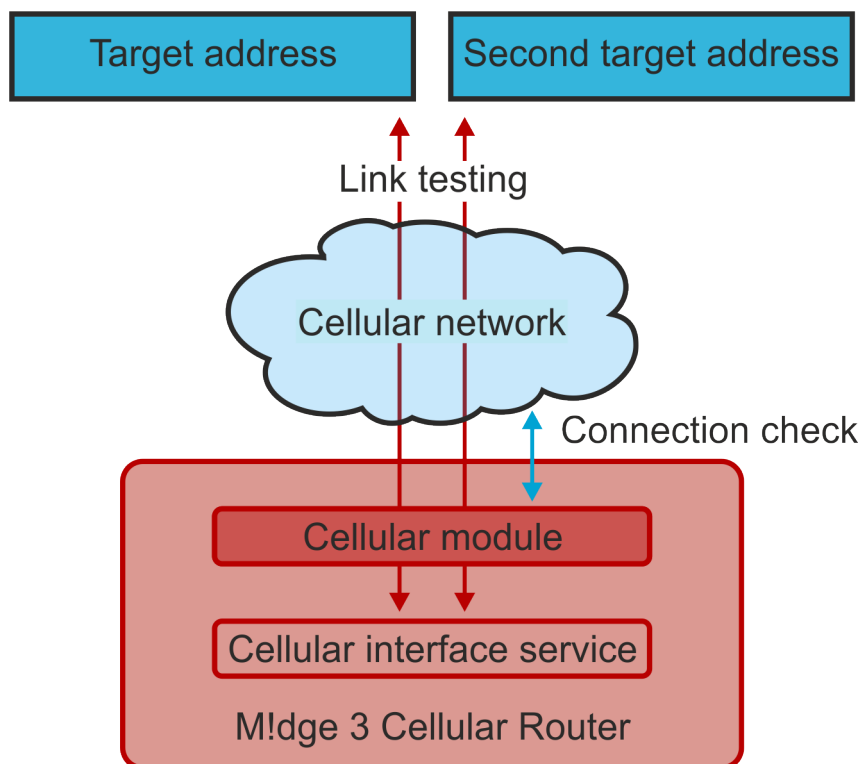


Fig. 7.1: Link testing scheme

Settings of Link testing for MAIN (EXT):

#### Link testing

|                              |   |
|------------------------------|---|
| Test period [s]              | <input type="text" value="60"/>                 |
| Repeat period [s]            | <input type="text" value="10"/>                 |
| Repeat period [s]            | <input type="text" value="10"/>                 |
| Retries [No]                 | <input type="text" value="3"/>                  |
| Target address               | <input type="text" value="0.0.0.0"/>            |
| Enable second target address | <input type="text" value="On"/> ▼               |
| Second target address        | <input type="text" value="0.0.0.0"/>            |
| Test mode                    | <input type="text" value="One address succ"/> ▼ |

#### Test period [s]

Number {3 – 3600}, default = 60

Time period, during which is the connection being tested.

**Repeat period [s]**

Number {3 – 3600}, default = 10

If the test results as failed, the connection is tested again after defined time period.

**Retries [No]**

Number {1 – 20}, default = 3

Amount of failed tests, after which is the link declared to be non-functional.

**Target address**

IP address, default = 0.0.0.0

Primary tested IP address.

**Enable second target address**

List box {On; Off}, default = "On"

Enables / Disables testing of the second IP address.

**Second target address**

IP address, default = 0.0.0.0

Secondary tested IP address.

**Test mode**

List box {One address succeeds; Both addresses succeeds}, default = "One address succeeds"

Defines the success of the test:

- One address succeeds - only one address is enough to pass the test.
- Both addresses succeeds - both addresses must pass the test.



**Note**

If the connection to SIM card fails (missing SIM, wrong PIN), all profiles using that SIM will be blocked. If all profiles are blocked, the whole Cellular interface service will be blocked.

**7.1.4.1.4. Profile switching**

In case of a malfunction of the current running profile, the module switches automatically to another (if it is defined). If the module has no more defined profiles to switch to, it switches back to the first one. After defined time period, the module can try to reconnect via the first profile again (independently on the profile queue). This section occurs only, if parameter **Profile switching** is set to "On".

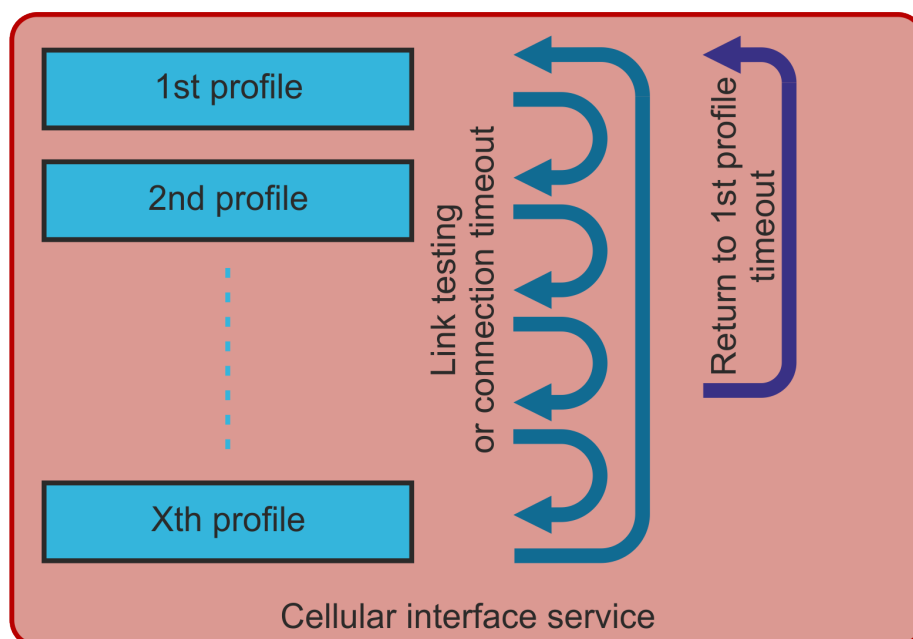


Fig. 7.2: Link testing scheme

## Profile switching

|                                       |                    |   |
|---------------------------------------|--------------------|---|
| Switching method                      | On failure to recc | ▼ |
| Connection timeout [min]              | 15                 |   |
| Return to first profile               | On                 | ▼ |
| Time to return to first profile [min] | 480                |   |

### Switching method

List box {On first failure; On failure to reconnect, On timeout}, default = "On first failure"  
 Defines the way of switching to the next profile, when the connection fails.

- On first failure - after first failure, the module switches to another profile.
- On failure to reconnect - after failure, the module tries to reconnect. If the reconnection is unsuccessful, the module switches to another profile.
- On timeout - the module keeps reconnecting to its current profile for the time period of its timeout (parameter **Connection timeout [min]**).

### Connection timeout [min]

Number {3 – 60}, default = 15

Time period, during which is the module waiting for connection (after initial opening of the interface).

### Return to first profile

List box {On; Off}, default = "On"

When enabled, the module will switch back to its first profile after defined time period.

### Time to return to first profile [min]

Number {5 – 10080}, default = 480

Time period, after which is the current profile switched back to the first one.

### 7.1.4.2. SIM1 and SIM2

SIM1 and SIM2 tabs contain the same setting for SIM1 and SIM2 respectively.

#### **PIN protection**

List box {On; Off}, default = "Off"

Enables / Disables the SIM module PIN protection. It has to be switched on if the PIN is required.

The parameter is ignored if the SIM does not require a PIN.

#### **PIN code**

String {0000 – 9999}, default = "0000"

The PIN is used only when PIN protection is On and the module requires the PIN.

### 7.1.4.3. Cooperation with other services

#### **Firewall L3**

Parameters **Input interface** and **Output interface** can filter the traffic either coming to WWAN or leaving to WWAN (List box WWAN or EXT).

#### **NAT**

- SNAT - parameter **Output interface** can filter the traffic (List box WWAN or EXT). Rules of SNAT (user settings) have higher priority than rules of MASQUERADE in this section (parameter **Masquerade**).
- DNAT - parameter **Input interface** can filter the traffic (List box WWAN or EXT).

#### **IPsec**

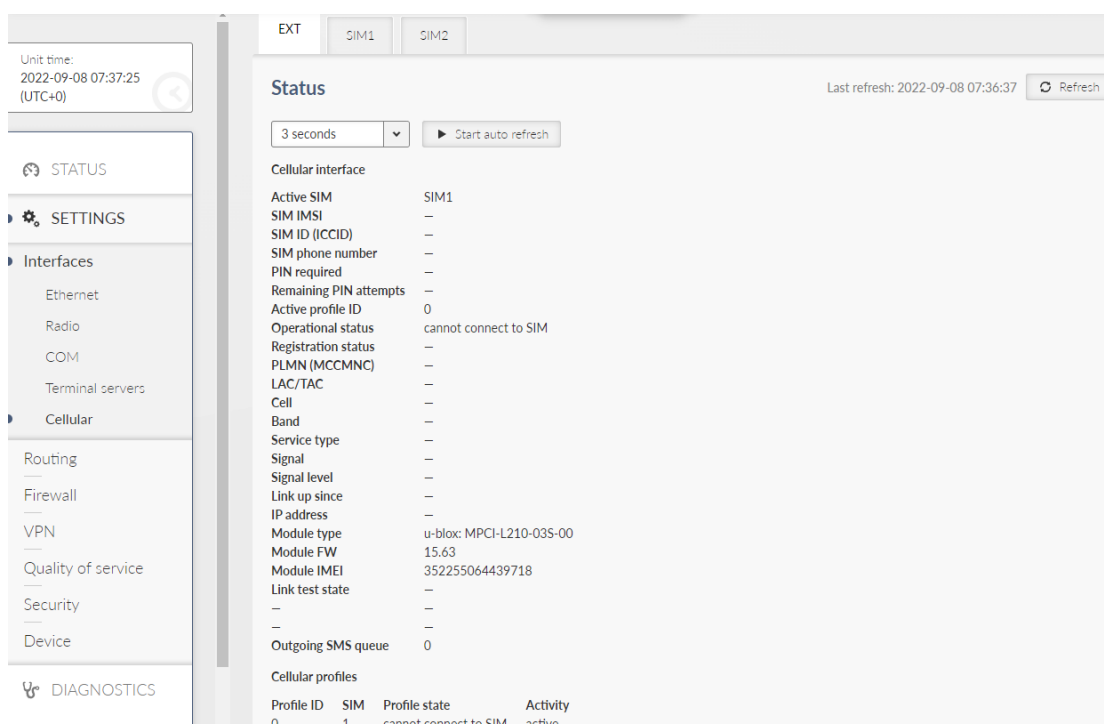
Automatic rules of MASQUERADE do not overwrite the source address of packets, which are encapsulated into IPsec.

It is recommended for IPsec to enable MOBIKE, if guided through Cellular.

### 7.1.5. Status

Values are displayed from the moment of opening the SETTINGS menu. The values can be updated by using Refresh button.





Common status information and SIMs information are available.

**Tab. 7.1: Signal levels for individual services**

| Signal level     | LED color | 2G: RSSI       | 3G: RSCP        | 4G: RSRP        |
|------------------|-----------|----------------|-----------------|-----------------|
| Weak / No signal | Red       | <= -95 dBm     | <= -100 dBm     | <= -100 dBm     |
| Medium           | Orange    | -95 to -84 dBm | -100 to -89 dBm | -100 to -80 dBm |
| Good             | Green     | -84 dBm <=     | -89 dBm <=      | -80 dBm <=      |

## 7.2. Routing

RipEX router supports both static and dynamic IP routing.

Static routing is based on fixed – static – definition of routing tables. Dynamic routing is based on automatic creating and updating of routing tables. Various methods and protocols are used for this purpose. Babel, OSPF and BGP standard routing protocols are available in RipEX networks.

Link management option was added allowing to set the switchover of the main link (in the event of its failure) to an existing backup link by automatic changes of routing rules.

### 7.2.1. Static

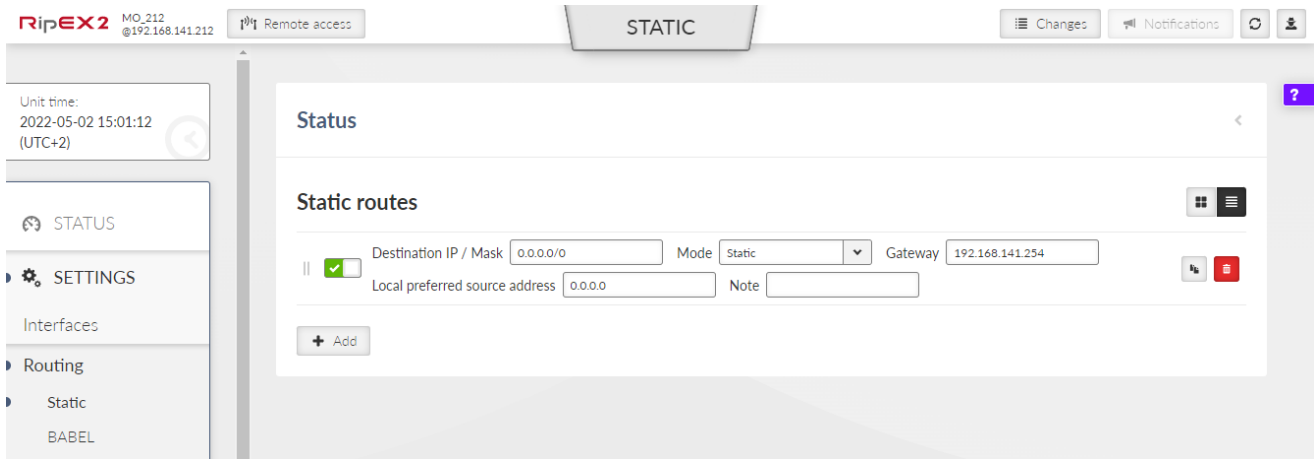
MIDGE3 works as a standard IP router with multiple independent interfaces: Network interfaces (bridging physical Ethernet interfaces), COM ports, Terminal servers, Cellular interface etc. Each of the interfaces has its own IP addresses and Masks. All IP packets are processed according to the Routing table.

Unlimited number of subnets can be defined on the Network interface. They are routed independently.

The COM ports are treated in the standard way as router devices, messages can be delivered to them as UDP datagrams to selected UDP port numbers. Destination IP address of COM port is IP of a Network

interface (bridging Ethernet interfaces). The IP address source of outgoing packets from COM ports is equal to IP address of interface (Network interface) through which packet has been sent. The source address can also be assigned to **Local preferred source address** value - see description below. Outgoing interface is determined in Routing table according to the destination IP.

The IP addressing scheme can be chosen arbitrarily, only 127.0.0.0/8 and 192.0.2.233/30 and 192.0.2.228/30 restriction applies. It may happen that also the subsequent addresses from the 192.0.2.0/24 subnet according to RFC5737 may be reserved for internal usage in the future.



**Active**

{On / Off}

Switches the rule on / off.

**Destination IP / mask**

IP address, default = 0.0.0.0/0

Each IP packet, received by M!DGE3 through any interface (ETH, COM, ...), has got a destination IP address. M!DGE3 (router) forwards the received packet either directly to the destination IP address or to the respective Gateway, according to the Routing table. Any Gateway has to be within the network defined by IP and Mask of one of the interfaces, otherwise the packet is discarded.

Each item in the routing table defines a Gateway (the route, the next hop) for the network (group of addresses) defined by Destination IP and Mask. When the Gateway for the respective destination IP address is not found in the Routing table, the packet is forwarded to the Default gateway, when Default gateway (0.0.0.0/0) is not defined, the packet is discarded.

The network (Destination IP and Mask) is written in CIDR format, e.g. 10.11.12.0/24.



**Note**

Network defined by the same combination of Destination IP and Mask cannot be used for two different rules.

**Mode**

List box {Static; WWAN}, default = Static

{Static} Used for static IP routing rules.

**Local preferred source address**

IP address, default = 0.0.0.0

Local IP address used as a source address for packets originating in the local M!DGE3 unit being routed by this routing rule. It might be for example packets originating from the COM port or from the Terminal Server. If the address is set to 0.0.0.0 it is not considered active. The IP address has to belong to the Network interfaces.

**Metric**

Number {0 – 4294967294}, default = 0

Routing rule metric value.

**Note**

You may add a name to each route with your comments up to 16 characters (UTF8 is supported) for your convenience.

**Persistent route**

List box {On; Off}, default = Off

Sets the persistence (time of presence) of dynamic routing rule.

This parameter is available only if parameter **Mode** is set to "WWAN (MAIN)" or "WWAN (EXT)".

- On - Routing rule is always present. When the WWAN interface is closed, it reports "unreachable" messages (via ICMP) and the traffic cannot be caught by a different rule.
- Off - Routing rule exists only if the WWAN interface is open. If it is closed, the traffic can be caught by a different rule.

**7.2.1.1. Loopback addresses**

Table of loopback addresses contains IP addresses of M!DGE3, which are set on the loopback interface as "support" addresses independent on specific interface. Maximum number of addresses is 256. Loopback addresses can be useful e.g. for specific routing purposes or specific user data traffic. For example using different routing rules for different traffic.

The screenshot shows the 'Loopback' configuration page in the RipEX2 web interface. The page is titled 'Loopback' and 'Loopback addresses'. It features a table with columns for '#0', 'Enable address', 'Note', and 'IP'. The 'Enable address' column has a dropdown menu set to 'On'. Below the table are buttons for '+ Add' and 'Reset form'. The interface also shows a navigation menu on the left with options like STATUS, SETTINGS, DIAGNOSTICS, and ADVANCED. The top right corner has an 'ADVANCED' tab.

**Enable address**

List box {On; Off}, default = "On"

**Note**

Optional comment.

**IP**

IP address, default = 0.0.0.0

Defines the IP address which will be set on the loop-back interface. The mask is automatically /32.

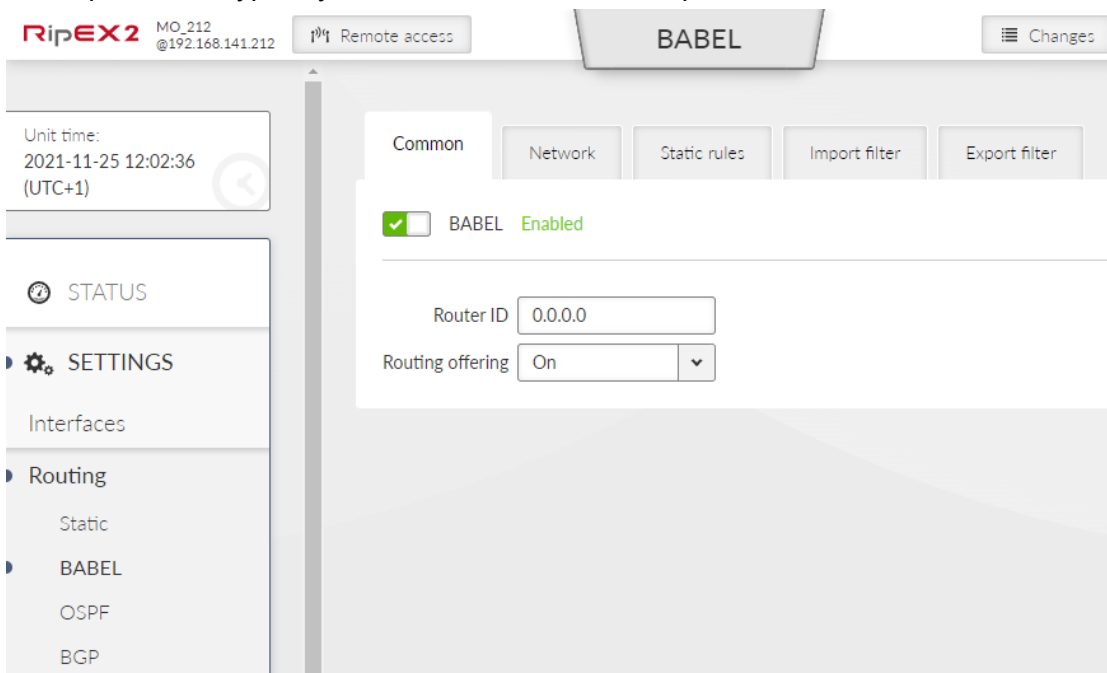
### 7.2.2. Babel

Babel is a loop-avoiding distance-vector routing protocol that is designed to be robust and efficient both in networks using prefix-based routing and in networks using flat routing ("mesh networks"), and both in relatively stable wired networks and in highly dynamic wireless networks (for more information see [RFC6126](https://datatracker.ietf.org/doc/html/rfc6126)<sup>2</sup>).

Babel is also a dynamic routing protocol for Internet Protocol (IP) networks. It is an Interior Gateway Protocol (IGP) working within one Autonomous system. It is based on OSPF protocol (see the next chapter for OSPF protocol description) with the following differences:

- Works within one autonomous system
- Babel provides both wired and wireless type of network interface

Babel protocol is typically used within the network hops or other networks with limited data throughput.



Configuration parameters are described in the following chapters. Several use case scenarios and configuration examples are described in the *Babel Application note*<sup>3</sup>.

#### 7.2.2.1. Description

Every router defines which interfaces are used for Babel protocol to search for available network neighbors.

Each router is periodically transmitting and receiving Hello packets to determine existence and quality of a connection to neighboring network nodes. The result information about available routes (paths) and their quality is shared across the network. Routing tables are exchanged periodically and also after their update.

Routing path decision is based on a "metric":

<sup>2</sup> <https://datatracker.ietf.org/doc/html/rfc6126.html#section-1.1>

<sup>3</sup> [https://www.racom.eu/download/hw/ripex/free/eng/1\\_application/ripex2-app-bab-en.pdf](https://www.racom.eu/download/hw/ripex/free/eng/1_application/ripex2-app-bab-en.pdf)

- Metric is set on each interface. It reflects a “price” for the packet reception. The higher the metric value, the more disadvantageous is usage of such a path.
- Maximum value is 65535.

There are two types of interfaces:

- Wired: assumes a reliable link. The quality is evaluated according to the number of received Hello packets. If configured limit of lost packets is exceeded, the line is considered down.
- Wireless: assumes a variable connection quality. The price of the interface increases gradually with each lost Hello packet until the line is declared down.

Routing decision:

- SETTINGS > Routing > Static routes are valid even if the Dynamic routing is enabled. Dynamic routing protocols “export” resulting routing rules into Linux and they are added to the existing (static) routing rules.
- Particular routing decision takes IP mask as a primary decision rule (narrower mask has a higher priority) and metric as a secondary decision rule. Rules received from dynamic protocols have higher metric compared to Static routes (they always have the highest possible metric).
- Internal metrics of dynamic protocols are processed only inside them. Only the final set of routing rules is exported to the Linux router.

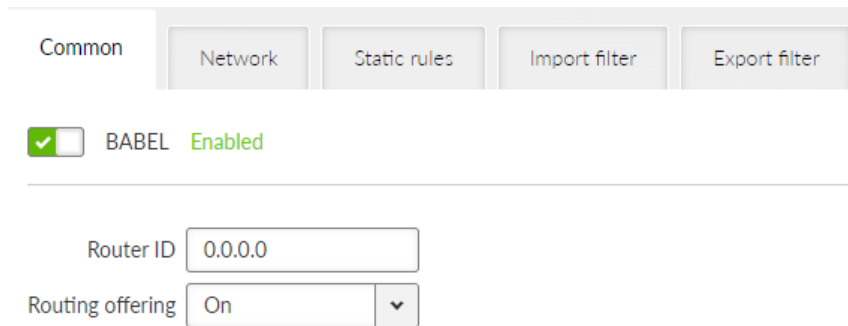
Example 1:

- SETTINGS > Routing > Static routes rule: 0.0.0.0/0 → 10.10.1.11
- Dynamic rule: 192.168.1.0/24 → 192.168.11.1 metric 32
- Packet with DST 192.168.1.42 will be routed to 192.168.11.1 because the dynamic rule has a narrower mask.

Example 2 – similar situation with additional static rule:

- SETTINGS > Routing > Static routes rule: 0.0.0.0/0 → 10.10.1.11
- SETTINGS > Routing > Static routes rule: 192.168.1.0/24 → 192.168.22.1
- Dynamic rule: 192.168.1.0/24 → 192.168.11.1 metric 32
- Packet with DST 192.168.1.42 will be routed to 192.168.22.1 because the static rule has the same mask, but better metric.

### 7.2.2.2. Common - Common settings



Common   Network   Static rules   Import filter   Export filter

BABEL Enabled

Router ID

Routing offering  ▼

#### Router ID

IP address, default = 0.0.0.0

M!DGE3 unit acts in the Babel network as a dynamic router. Every router is identified by an ID having the format of IP address. This IP address does not have to be 'real'.

Router ID is shared across all dynamic protocols.

#### Randomize ID

List box {On; Off}, default = "Off"

Advanced feature: Enables randomization of the upper 4 Bytes of the router identification. The lower 4 Bytes are set by a **Router ID** parameter. This feature might be used in a case the Babel node is often restarted resulting in refusing its messages by its neighbors.

#### Routing offering

List box {On; Off}, default = "On"

Enables propagation of routing rules acquired from the neighbors. When disabled, the incoming rules are not propagated to other routers and this router behaves as an end point terminal – network paths are started or terminated in such a point, but do not travel through.

### 7.2.2.3. Network - Interfaces

Edit interface
×

Enable interface

Interface

Type Wireless ▼

Rx cost

Hello interval [s]

Update interval multiplier

Advertised next hop

Authentication Full ▼

Authentication algorithm HMAC SHA256 ▼

Password

Note

Confirm and close
Close

#### Active

List box {On; Off}, default = "Off"  
Enables / disables the interface.

#### Interface

String {a..z A..Z 0..9}, max 16 char, default = <empty> Interfaces which will be used by Babel for searching the available connections. Name of an existing unit interface has to be used. Following interfaces can be used:

LAN – “if\_” prefix must be used followed by Network interface name, e.g. “if\_LAN-141”

VLAN – “if\_” prefix must be used followed by Network interface name, ‘.’ dot and VLAN number, e.g. “if\_LAN-141.29”

GRE L3 – “gre\_tunX” where ‘X’ is the tunnel number, starting from zero

Cellular – “wwan”, “ext”

Interface MTU must be 1280 Bytes or bigger in order to operate Babel protocol correctly.

#### Type

List box {Wired; Wireless}, default = "Wireless"

Type of network interface and also the type of link status evaluation. “Wired” link status is evaluated by checking the limit of received Hello packets – if not met, the link is considered down. “Wireless” link status is evaluated using ETX criteria – each lost Hello packet gradually decreases the link metric.

### Rx cost

Number {1 – 65534}, default = 128

The cost of using this interface to receive packet from a neighbor. It is added to Babel path metric.

### Hello limit

Number {1 – 16}, default = 12

For “Wired” interface only: limit of received Hello packets from the 16 expected; if not met, the link is considered down.

### Hello interval

Number {0.1 – 327.0}, default = 4.0

Interval (in seconds) of sending Hello packets.

### Update interval multiplier

Number {2 – 30}, default = 4

Interval of sending the routing table update packets – to share the network topology information across the Babel network. The update interval is calculated as a multiplication of this parameter and **Hello interval**. The maximum length of the update interval (after the multiplication) is 655 seconds.

### Advertised next hop

IP address, default = 0.0.0.0

This is the Next hop address which is announced to neighbors to be routed over this interface. Should this interface serve more IP addresses, this parameter enables selection of which of the addresses should be used for this station in the network neighbors routing tables.

### Authentication

List box {None; Full; Only sign}, default = "None"

Enables packets authentication of Babel protocol.

- Full - packets are signed during transfer and the signature is validated when receiving incoming packets. Packets with invalid signature are reported to the log and thrown away.
- Only sign - Packets are signed during transfer and the signature is validated when receiving incoming packets. Packets with invalid signature are reported to the log and accepted. This settings is intended for gradual network switch to safe mode.

### Authentication algorithm

List box {HMAC SHA256; HMAC SHA384; HMAC SHA512; BLAKE2s-128; BLAKE2s-256; BLAKE2b-256; BLAKE2b-512}, default = "HMAC SHA256"

Selects the authentication algorithm. This parameter occurs only, if parameter **Authentication** is set either to "Full" or "Only sign".

Each algorithm has its own password length limit.

HMAC SHA256 - string length up to 128 char

HMAC SHA384 - string length up to 128 char

HMAC SHA512 - string length up to 128 char

BLAKE2s-128 - string length up to 32 char

BLAKE2s-256 - string length up to 32 char

BLAKE2b-256 - string length up to 64 char



BLAKE2b-512 - string length up to 64 char

### Password

String {up to 128 char}

Defines the password for packets authentication.

### Note

Optional comment.

## 7.2.2.4. Static rules

The screenshot shows a configuration page for 'Static rules'. At the top, there are tabs for 'Common', 'Network', 'Static rules', 'Import filter', and 'Export filter'. The 'Static rules' tab is active. Below the tabs, the title 'Static rules' is displayed. A list of rules is shown, with the first rule being active (checkbox checked). The rule details are: Destination IP / Destination mask: 0.0.0.0/0, Metric: 0, and a Note field. At the bottom, there is a '+ Add rule' button.

Pre-defined static routing rules to be exported over the Babel protocol. Maximum number of rules is 256.

### Active

List box {On; Off}, default = "On"

Enables / disables the static routing rule.

### Destination IP / Destination mask

IP address, default = 0.0.0.0/0

IP address and mask defining the exported routing rule address range.

### Metric

Number {0 – 65534}, default = 0

Routing rule metric value. The higher the value, the more "expensive" the path is.

### Note

Optional comment.

**7.2.2.5. Import filter**

Common Network Static rules **Import filter** Export filter

Filter policy  ▼

### Import filter rules

Off ✎

Interfaces:  
Off: 0.0.0.0/0 {0,32}

Accept 🗑

+ Add rule

Babel import filter rules. The order of rules matters. Each incoming routing rule is processed by those Import filters. Maximum number of filter rules is 256.

**Active**

List box {On; Off}, default = "On"  
Enables / disables the filter rule.

**Filter network**

List box {Off; Match; Not match}, default = "Off"  
Method of the routing rule target range comparison.

**IP address / mask**

IP address / mask, default = 0.0.0.0/0  
IP address and mask defining the network range to be compared.

**Mask from**

Number {0 – 32}, default = 0

**Mask to**

Number {0 – 32}, default = 32  
Definition of the enabled range of the mask length of the processed routing rule.  
Examples:

Rule 0.0.0.0/0 {0,32} captures all IP ranges

Rule 192.168.1.0/24 {24,32} captures 192.168.1.0/24 and all subnets (for example 192.168.1.1/32)

Rule 10.9.8.7/32 {8,32} captures all ranges having the mask longer than 8 covering the address 10.9.8.7 (e.g. 10.9.0.0/16)

**Action**

List box {Accept; Reject; Pass}, default = "Accept"  
Type of action to be performed when the filter rules above matches the incoming routing rule. When "Pass" is selected, the packet processing continues.

**Set preference**

List box {On; Off}, default = "Off"

When enabled, the Preference (see next parameter) will be set to this rule.

**Preference**

Number {0 – 65535}, default = 210

Routing rule preference in the routing table (to be used when Set preference is enabled). The higher the number the better the preference.

**Local preferred source address**

IP address, default = 0.0.0.0

Preferred source IP address for the locally generated packets. When disabled (default value 0.0.0.0 is used), the source IP address is set according to the outgoing interface.

**Note**

Optional comment.

**7.2.2.6. Export filter**

Common Network Static rules Import filter Export filter

Filter policy Reject

Export filter rules

Off

Interfaces: Off

Protocol: Off

Accept

+ Add rule

Babel export filter rules define set of routing rules to be exported from the unit to other Babel routers. The order of rules matters. Maximum number of filter rules is 256.

**Active**

List box {On; Off}, default = "On"

Enables / disables the filter rule.

**Filter network**

List box {Off; Match; Not match}, default = "Off"

Method of the routing rule target range comparison.

**IP address / mask**

IP address / mask, default = 0.0.0.0/0

IP address and mask defining the network range to be compared.

**Mask from**

Number {0 – 32}, default = 0

**Mask to**

Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

#### Filter protocol

List box {Off; Match; Not match}, default = "Off"

Selects the way how the routing rule source protocol is compared.

#### Protocol

List box {System; BGP; BGP external; BGP internal; OSPF}, default = "System"

Selection of the protocol origin. "System" – stands for rules from the ordinary routing table.

#### Filter BGP path

List box {Off; Is empty; Not empty}, default = "Off"

Compares BGP routing rule path if it is empty (i.e. the rule originates in this AS).

#### Filter OSPF source

List box {Off; Match; Not match}, default = "Off"

Selects the way how the routing rule from the OSPF protocol is compared.

#### OSPF source

List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 2"

OSPF sources. "Internal" – stands for internally generated rule (e.g. interface range). "Inter-area" – stands for rule generated on the area borders.

#### Filter OSPF tag

List box {Off; Match; Not match}, default = "Off"

OSPF tag based filtering method.

#### OSPF tag

Number {0 – (2<sup>32</sup>-1)}, default = 0

OSPF tag to be compared.

#### Action

List box {Accept; Reject; Pass}, default = "Accept"

Defines what action is taken on the routing rule. When "Pass" is selected, the packet processing continues.

#### Metric from other protocol

List box {Off; BGP MED; OSPF Metric 1; OSPF Metric 2; OSPF Metric Sum}, default = "Off"

Defines source of metric.

Off: The static **Metric** value (see the following parameter) is used.

BGP MED: MED (Multi-Exit Discriminator) rules from the BGP protocol. If the rule does not have a MED value filled in, the static Metric value is used.

OSPF metric 1: Metric of OSPF type 1. If the rule does not have a metric value filled in, the static Metric value is used.

OSPF metric 2: Metric of OSPF type 2. If the rule does not have a metric value filled in, the static Metric value is used.

OSPF metric sum: Sum of OSPF type 1 a type 2 metrics. If the rule does not have both metric values filled in, the static Metric value is used.

**Metric**

Number {0 – 65534}, default = 0

Routing rule metric value. The higher the value, the more “expensive” the path is.

**Note**

Optional comment.

**7.2.3. OSPF**

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). OSPF Version 2 defined in RFC 2328 (1998) for IPv4 is implemented in the RipEX router. OSPF provides Layer 2 dynamic routing. In the context of RipEX networks it is typically used for the backhaul network routing.

OSPF splits the network into “areas” to simplify the network topology. There is a primary “backbone” (0.0.0.0) area and the other areas are connected to this backbone area via border routers.

The route decision process is affected by the path “metric”. There are two types of metrics:

- Metric Type 1 – path length; individual interfaces pass-over costs are added.
- Metric Type 2 – is setup on the rules which are exported to the OSPF from outside. Rules having metric ‘Type 2’ are always treated as worse (i.e. longer path) comparing to metric ‘Type 1’.

Routers in a specific area are always connected via interfaces.

- An address range can be defined for an interface where is the OSPF working. Multiple address ranges can be defined (behaving as another interface).
- Router to router interconnection can be protected by encryption with the password.
- Specific “Cost” is defined for each interface which is added to metric ‘Type 1.’
- There are multiple types of interfaces:
  - Stub – interface only announces to OSPF: its presence and its address ranges to be propagated further to the network.
  - Broadcast – to be used in the network where all the participants always hear each other (Ethernet). Designated Router (DR) and Backup DR (BDR) are setup between the neighbors. They are responsible for the update propagation (broadcast).
  - NBMA (Non-Broadcast Multiple Access) – to be used in the network where only specific participants can communicate between each other; all the participants hear each other but multicast is not available. DR and BDR is setup.
  - Point2Point – network having only two participants. They discover each other using multicast.
  - Point2Multipoint – network where only predefined pairs of participants can hear each other (e.g. star topology); multicast is not available.
- Static rules can be defined. Such a routing rules are propagated to the network from this router.
- It is possible to define exported routing rules aggregation or specific routing rule hiding.

- It is possible to control the routing rules which are imported into the RipEX unit from the OSPF protocol and those that are exported into the OSPF protocol from the unit by using 'filters'.
  - Export filters – to control rules exported from the unit to the OSPF protocol which is propagating them further.
  - Import filters – to control rules imported from the OSPF into the unit.

### 7.2.3.1. OSPF Common - Common settings

#### Active

List box {On; Off}, default = "Off"

Enables the dynamic routing and the OSPF protocol.

#### Router ID

IP address, default = 0.0.0.0

M!DGE3 unit acts in the OSPF network as a dynamic router. Every router is identified by an ID having the format of IP address. This IP address does not have to be 'real'. Router ID is shared across all dynamic protocols.

#### Instance ID

Number {0 – 255}, default = 0

OSPF protocol instance number. This number is needed in case of running multiple OSPF protocols (for example on the border of 2 independent OSPF networks).

### 7.2.3.2. OSPF Network - Areas and interfaces

#### 7.2.3.2.1. Areas and interfaces

OSPF areas RipEX unit belongs to are described here. Maximum number of areas is 32.

#### Enable / Disable

Enables / disables the specific area.

#### Area ID

IP address, default = 0.0.0.0

OSPF area identifier. The ID has a format of an IP address. This IP address does not have to be 'real'. The 'Router ID' value is used typically. The default value of 0.0.0.0 is called 'backbone' and it has to be present somewhere in the OSPF network.

#### Stub area

Click box {On; Off}, default = "Off"

Defines if the area is of a 'stub' type – which means, the traffic is not routed through such an area. Every traffic is originated or terminated in the 'stub' area.

#### Stub default GW (ADVANCED parameter)

List box {On; Off}, default = "On"

If 'On' – only default GW is routed to the 'stub' area. If 'Off' – individual routes are routing the traffic into the area. It may be effective to disable this parameter when multiple border routers are present.

**Note**

Optional comment. It is a good practice to enter some descriptive area name since this value is displayed (when filled) instead of the **Area ID** as an **Area** name in other configuration dialogs (e.g. Networks configuration).

OSPF interfaces of the respective OSPF area are defined here. Maximum number of interfaces is 128.

**Active**

List box {On; Off}, default = "Off"  
Enables / disables the interface.

**Interface**

String {a..z A..Z 0..9}, max 16 char, default = <empty>

OSPF interface name. Name of an existing unit interface has to be used. Following interfaces can be used:

- LAN – “if\_” prefix must be used followed by Network interface name, e.g. “if\_LAN-141”
- VLAN – “if\_” prefix must be used followed by Network interface name, ‘.’ dot and VLAN number, e.g. “if\_LAN-141.29”
- GRE L3 – “gre\_tunX” where ‘X’ is the tunnel number, starting from zero
- Cellular – “wwan”, “ext”

**IP address / mask**

IP address / mask, default = 0.0.0.0/0

IP address and mask of the address range above which the OSPF protocol will be working on this interface. The default value is 0.0.0.0/0, which means the whole address range on this interface is available for the OSPF protocol.

**Network type**

List box {Broadcast; Point2Point; Point2Multipoint; NBMA; Stub}, default = "Broadcast"  
Defines the type of the network behind the interface.

**Cost**

Number {1 – 65535}, default = 10

The cost of traffic over this interface. The higher the Cost, the worse the path. It is added to OSPF metric ‘Type 1’.

**Hello interval**

Number {1 – 3600}, default = 10

Interval (in seconds) of sending Hello packets. The interval must be the same for the all participants of the given interface.

**Poll interval**

Number {1 – 3600}, default = 20

Interval (in seconds) of sending Hello packets to inactive neighbors in the NBMA type of interface.

**Retransmit interval**

Number {1 – 3600}, default = 5

Interval (in seconds) of repeating unacknowledged packets.

**Dead count**

Number {2 – 64}, default = 4

Number of lost Hello packets from the neighbor to treat the connection as interrupted.

#### **TTL security**

List box {On; Off}, default = "On"

Protection against OSPF packets spoofing.

#### **Authentication, Password**

List box {None; Keyed MD5 (OSPFv2); HMAC SHA256; HMAC SHA384; HMAC SHA512}, default = "None"

Selection of a method to authenticate the OSPF messages. Password is used as a secret key for the selected hash function. Maximum length of the password is 128 characters.

#### **Priority**

Number {0 – 255}, default = 1

Priority is used to select primary or backup router responsible for the routing updates propagation.

The higher the number, the higher the priority. '0' states the router cannot be used as a primary or backup router.

#### **Use broadcast**

List box {On; Off}, default = "Off"

Defines if OSPF packets distribution is provided using multicasts (default behavior) or broadcasts (nonstandard behavior).

#### **Note**

Optional comment. It is possible to enter some descriptive OSPF interface name. This value is used (when filled) instead of the original **Interface** identification as an **Interface** name in other configuration dialogs (e.g. Neighbors configuration).

### **7.2.3.2.2. Neighbors**

Network neighbors of Point2Multipoint and NBMA types of OSPF interfaces are defined here. Maximum number of neighbors is 512.

#### **Active**

List box {On; Off}, default = "Off"

Enables / disables the interface.

#### **Interface**

List box {list of existing OSPF interfaces}

OSPF interface the neighbor belongs to. The interface – **Note** value is used when defined. The interface – **Interface** value is used otherwise.

#### **IP**

IP address, default = 0.0.0.0

IP address of the neighbor.

#### **Note**

Optional comment.

### **7.2.3.2.3. Networks**

The Networks table modifies networks announced out of the area. It enables partial networks aggregation into the common prefixes or specific network hiding. Maximum number of rules is 256.



**Active**

List box {On; Off}, default = "Off"  
Enables / disables the interface.

**Area**

List box {list of existing OSPF areas}  
OSPF area the record belongs to.

**IP address / mask**

IP address / mask, default = 0.0.0.0/0  
IP address and mask of the range (i.e. network) which will be aggregated or hidden.

**Action**

List box {Aggregate; Hide}, default = "Aggregate"

- Aggregate – small network prefixes will be exported from this area aggregated into this range (defined by **IP / mask**)
- Hide – this network prefix will be hidden and will not be exported

Example:

Area 0.0.0.1 exports two subnets: 192.168.1.0/24 and 192.168.2.0/24. Area border router between Area 0.0.0.1 and 0.0.0.0 defines a rule for network aggregation: 192.168.0.0/16. As a result of this, the area border router announces to the area 0.0.0.0 only one route 192.168.0.0/16 instead of the two individual routes.

**Note**

Optional comment.

**7.2.3.3. OSPF Static rules**

Pre-defined static routing rules to be exported over the OSPF protocol. Maximum number of rules is 256.

**Active**

List box {On; Off}, default = "Off"  
Enables / disables the static routing rule.

**Destination IP / Destination mask**

IP address, default = 0.0.0.0/0  
IP address and mask defining the exported routing rule address range.

**Metric type**

List box {Type 1; Type 2}, default = "Type 1"  
Metric type of the routing rule. Metric 1 is added to the path cost. Metric 2 stays apart and compared to metric 1 is always bigger.

**Metric**

Number {1 – 65535}, default = 1000  
Routing rule metric value.

**OSPF tag**

Number {0 –  $(2^{32}-1)$ }, default = 0  
OSPF tag is added to a rule at the moment of its insertion to the network. The tag travels through the OSPF without any modification so it can be used to distinguish the rule in the filters.

### Note

Optional comment.

### 7.2.3.4. OSPF Import filter

OSPF import filter rules. The order of rules matters. Each incoming routing rule is processed by those Import filters. Maximum number of filter rules is 256.

#### Active

List box {On; Off}, default = "Off"  
Enables / disables the filter rule.

#### Filter network

List box {Off; Match; Not match}, default = "Off"  
Method of the routing rule target range comparison.

#### IP address / mask

IP address / mask, default = 0.0.0.0/0  
IP address and mask defining the network range to be compared.

#### Mask from

Number {0 – 32}, default = 0

#### Mask to

Number {0 – 32}, default = 32  
Definition of the enabled range of the mask length of the processed routing rule.  
Examples:

- Rule 0.0.0.0/0{0,32} captures all IP ranges
- Rule 192.168.1.0/24{24,32} captures 192.168.1.0/24 and all subnets (for example 192.168.1.1/32)
- Rule 10.9.8.7/32{8,32} captures all ranges having the mask longer than 8 covering the address 10.9.8.7 (e.g. 10.9.0.0/16)

#### Filter source

List box {Off; Match; Not match}, default = "Off"  
Method of the OSPF routing rule source comparison.

#### Source

List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 1"  
Source types comments:

- Internal – internally generated rule, for example interface range
- Inter-area – rule generated on the area border

#### Filter OSPF tag

List box {Off; Match; Not match}, default = "Off"  
Method of the OSPF routing rule OSPF tag comparison

#### OSPF tag

Number {0 – (2<sup>32</sup>-1)}, default = 0  
OSPF tag to be compared.

**Action**

List box {Accept; Reject; Pass}, default = "Accept"

Type of action to be performed when the filter rules above matches the incoming routing rule.

**Set preference**

List box {On; Off}, default = "Off"

When enabled, the **Preference** (see next parameter) will be set to this rule.

**Preference**

Number {0 – 65535}, default = 200

Routing rule preference in the routing table (to be used when **Set preference** is enabled). The higher the number the better the preference.

**Local preferred source address**

IP address, default = 0.0.0.0

Preferred source IP address for the locally generated packets. When disabled (default value 0.0.0.0 is used), the source IP address is set according to the outgoing interface.

**Note**

Optional comment.

**7.2.3.5. OSPF Export filter**

OSPF export filter rules define set of routing rules to be exported from the unit into the OSPF area. The order of rules matters. Maximum number of filter rules is 256.

**Active**

List box {On; Off}, default = "Off"

Enables / disables the filter rule.

**Note**

Optional comment.

**Filter network**

List box {Off; Match; Not match}, default = "Off"

Selects a method of the routing rule destination range comparison.

**IP address / mask**

IP address / mask, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared.

**Mask from**

Number {0 – 32}, default = 0

**Mask to**

Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

**Filter protocol**

List box {Off; Match; Not match}, default = "Off"

Selects the way how the routing rule source protocol is compared.

**Protocol**

List box {System; BGP; BGP external; BGP internal}, default = "System"

Selection of the protocol origin. "System" – stands for rules from the ordinary routing table.

#### **Filter BGP path**

List box {Off; Is empty; Not empty}, default = "Off"

Compares BGP routing rule path if it is empty (i.e. the rule originates in this AS).

#### **Action**

List box {Accept; Reject; Pass}, default = "Accept"

Defines what action is taken on the routing rule. "Pass" continues in processing.

### **7.2.4. BGP**

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems. BGP is classified as a path-vector routing protocol, and it makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

BGP splits the network into Autonomous Systems (AS) which are identified by a specific number. Individual BGP routers are interconnected with their neighbors using TCP connections. Any connection can travel over multiple hops. Any connection can be secured using MD5 signatures.

Connections inside the AS are called 'internal' (iBGP):

- All BGP routers within given AS must be fully interconnected – every router must have connection to all other routers.
- It is possible to define 'Route reflectors' – they must be fully interconnected. The other routers behave as Route reflector clients and they need a connection to their reflector only. Route reflector and its clients form a 'cluster'. It is possible to create a cluster with multiple Route reflectors for the purpose of backup.
- The iBGP router having a higher local preference will be preferred during the internal AS path selection.

Connections to another AS are called 'external' (eBGP):

- It is possible to communicate from the router to the neighbor AS the MED (Multi-Exit Discriminator) metric designating which of the AS border routers will be used as an input point.

When the routing rules are spread across the multiple AS, those AS are added into the accumulated path (BGP path). Path length is the primary criteria during the decision which of the routing rules will be used.

It is possible to prescribe routing rules toward this router which will be spread across the network (Static rules).

It is possible to control the routing rules which are imported into the RipEX unit from the BGP protocol and those that are exported into the BGP protocol from the unit by using 'filters'.

Import IGP filter – controls which of the routing rules from the BGP are accepted to the dynamic routing table and how

Export IGP filter – controls which of the routing rules from the dynamic routing table are exported to the BGP and how

Import OUT filter – controls which of the routing rules from the other AS are accepted to the BGP and how

Export OUT filter – controls which of the routing rules are exported from the BGP to other AS and how

Routing rules passed on between iBGP and BGP tables are not filtered

#### 7.2.4.1. BGP Common - Common settings

##### Active

List box {On; Off}, default = "Off"

Enables the dynamic routing and the BGP protocol.

##### Router ID

IP address, default = 0.0.0.0

RipEX unit acts in the BGP network as a dynamic router. Every router is identified by an ID having the format of an IP address. This IP address does not have to be 'real'. Router ID is shared with the OSPF protocol.

##### Local AS

Number  $\{0 - (2^{32}-1)\}$ , default = 65000

Local Autonomous System identification number. AS numbers are assigned by IANA. Part of the range is reserved for private network usage: 64512 – 65534 and 4200000000 – 4294967294. AS numbers from this range can be safely used by anyone.

##### Preference

Number  $\{0 - (2^{32}-1)\}$ , default = 100

Router preference within the local AS. The higher the number, the higher the preference.

##### MED (Multi-Exit Discriminator)

List box {Off; Static; OSPF metric 1}, default = "Off"

Setting of MED (Multi-Exit Discriminator) on the routing rules being exported to other AS. MED makes it possible to advertise which of the routers in the local AS is the preferred input point to the AS. "Static" option sets the fixed value for all rules (**Static MED**). "OSPF metric 1" copies the OSPF metric to MED; for the rules which are not from the OSPF it enters the fixed value **Static MED**.

##### Static MED

Number  $\{0 - (2^{32}-1)\}$ , default = 0

Metric to be used for the preferred input point to the AS selection (see MED (Multi-Exit Discriminator) description). The higher the number the lower the preference.

##### Route reflector

List box {Off; On}, default = "Off"

Enables the Route reflector function on this router. iBGP requires connection in between all routers under normal circumstances. Route reflector makes it possible to avoid this requirement by distributing routing updates to all its clients. Such clients do not need any other connection except connection to this Route reflector. Route reflector and its clients form a 'cluster'. See more details at the beginning of the BGP chapter.

##### Cluster ID type

List box {Router ID; Manual}, default = "Router ID"

Controls the iBGP cluster identification. Cluster identification must be the same inside the cluster and it has to be different in another cluster. If the "Router ID" is selected, the **Router ID** value is used as a cluster id.

### Cluster ID

IP address, default = 0.0.0.0

Cluster identification in the format of an IP address. This IP address does not have to be 'real' (valid).

### 7.2.4.2. BGP Neighbors

Neighboring BGP routers. Maximum number of neighbors is 256.

#### Active

List box {On; Off}, default = "On"

Enables the specific neighbor.

#### Note

Optional comment.

#### Neighbor type

List box {Internal; External}, default = "External"

Neighbor router type selection. "Internal" neighbor belongs to the same AS (iBGP). "External" belongs to other AS (eBGP).

#### Neighbor AS

Number {0 – (2<sup>32</sup>-1)}, default = 65000

Neighbor AS number.

#### Neighbor IP

IP address, default = 0.0.0.0

Neighbor router IP address.

#### Local IP of the connection

IP address, default = 0.0.0.0

Local IP address of the connection. Default value 0.0.0.0 provides automatic set up of this address – from the routing.

#### Neighbor connection

List box {Direct; Multihop}, default = "Direct"

Network connection type between the neighbors. "Direct" means direct – one hop – connection. This is typical for eBGP routers. "Multihop" means connection over the multiple routers. This is typical for iBGP routers.

#### MD5 authentication

List box {On; Off}, default = "Off"

Enables BGP packets authentication using TCP MD5 Signature extension.

#### Password

String {up to 128 char}

Password for the **MD5 authentication**.

#### Passive

List box {On; Off}, default = "Off"

Passive BGP router does not initiate connection to a neighbor, it is waiting for the neighbor activity.

**Hold interval [s]**

Number {3 – 10800}, default = 240

Time (in seconds) to wait for the keepalive message from the neighbor. It is negotiated with the neighbor. When it expires, the connection is treated as interrupted.

**Keepalive interval [s]**

Number {1 – 3600}, default = 80

Period (in seconds) of sending keepalive messages. It should not be longer than 1/3 of the **Hold interval**.

**Connection retry interval [s]**

Number {1 – 3600}, default = 120

Time (in seconds) to wait before trying to re-connect the interrupted connection.

**TTL security**

List box {On; Off}, default = "On"

Protection against BGP packets spoofing. [PP1] The Generalized TTL Security Mechanism (GTSM – RFC 5082) is used. BGP transmits packets with known TTL value. Incoming packets having lower than expected value (expected number of hops) are discarded.

**Expected hops**

Number {2 – 32}, default = 2

Number of expected hops between the neighbors.

**Route reflector client**

List box {On; Off}, default = "Off"

Defines if this neighbor is a client of this Route reflector.

**Set cost**

List box {On; Off}, default = "Off"

Enables to set a specific **Cost** of the BGP connection.

**Cost**

Number {0 – (2<sup>32</sup>-1)}, default = 10

The cost of connection to this neighbor. The higher the number the higher the cost. It enables to make decisions inside the router between multiple paths from the same neighbor.

**Next hop self**

List box {Off; Always; Internal; External}, default = "Off"

Defines if the exported routing rules should have 'next hop' addresses overwritten to the address of this router. "Internal" overwrites only the rules from the local AS. "External" overwrites only the rules from the other AS.

**7.2.4.3. BGP Static rules**

Pre-defined static routing rules to be exported over the BGP protocol. Maximum number of rules is 256.

**Active**

List box {On; Off}, default = "Off"

Enables / disables the static routing rule.

### Destination IP / Destination mask

IP address, default = 0.0.0.0/32

IP address and mask defining the exported routing rule destination address range.

### Note

Optional comment.

### 7.2.4.4. BGP Import IGP filter

Import IGP filter [PP1] rules. The order of rules matters. Maximum number of filter rules is 256.

### Filter policy

List box {Accept; Reject}, default = "Reject"

Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Import IGP filter**.

### Active

List box {On; Off}, default = "On"

Enables / disables the filter rule.

### Note

Optional comment.

### Filter network

List box {Off; Match; Not match}, default = "Off"

Selects a method of the routing rule destination range comparison.

### IP address / mask

IP address / mask, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared

### Mask from

Number {0 – 32}, default = 0

### Mask to

Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

### Filter source

List box {Off; Internal; External}, default = "Off"

Selection based on the routing rule source. "Internal" selects rules received from the internal (iBGP) connection. "External" selects rules received from the other AS (eBGP).

### Filter BGP path

List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"

Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.

### Path position

List box {Any; Neighbor; Source}, default = "Any"

Selects position of the specific AS (**Path AS**). "Any" – anywhere on the path. "Neighbor" – the path was received from this AS (last on the path). "Source" – routing rule was originated from this AS (first on the path).



**Path AS**

Number {0 – (2<sup>32</sup>-1)}, default = 65000

The number of the AS searched for.

**Action**

List box {Accept; Reject; Pass}, default = "Accept"

Defines what action is taken on the captured [PP1] routing rule. "Pass" continues in processing.

**Set preference**

List box {Off; On}, default = "Off"

Defines if the specific **Preference** will be set up for this rule.

**Preference**

Number {0 – 65535}, default = 100

Routing rule preference in the routing table. The higher the number the higher the preference.

**Local preferred source address**

IP address, default = 0.0.0.0

Preferred source IP address for the locally generated packets. When disabled (default value 0.0.0.0 is used), the source IP address is set according to the outgoing interface.

**7.2.4.5. BGP Export IGP filter**

Export IGP filter rules. The order of rules matters. Maximum number of filter rules is 256.

**Filter policy**

List box {Accept; Reject}, default = "Reject"

Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Export IGP filter**.

**Active**

List box {On; Off}, default = "On"

Enables / disables the filter rule.

**Note**

Optional comment.

**Filter network**

List box {Off; Match; Not match}, default = "Off"

Selects a method of the routing rule destination range comparison.

**IP address / mask**

IP address / mask, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared

**Mask from**

Number {0 – 32}, default = 0

**Mask to**

Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

**Filter protocol**

List box {Off; Match; Not match}, default = "Off"

Selects the way how the routing rule source protocol is compared.

**Protocol**

List box {System; OSPF}, default = "System"

Selection of the protocol origin. "System" – stands for rules from the ordinary routing table. "OSPF" stands for rules from the OSPF protocol.

**Filter OSPF source**

List box {Off; Match; Not match}, default = "Off"

Selects the OSPF routing rule source comparison mode.

**OSPF source**

List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 2"

OSPF sources. "Internal" – stands for internally generated rule (e.g. interface range). "Inter-area" – stands for rule generated on the area borders.

**Filter OSPF tag**

List box {Off; Match; Not match}, default = "Off"

Selects the way of filtering based on OSPF tag.

**OSPF tag**

Number {0 – (2<sup>32</sup>-1)}, default = 0

OSPF tag to be compared. The tag is added to a rule when inserted to OSPF.

**Action**

List box {Accept; Reject; Pass}, default = "Accept" Defines what action is taken on the routing rule. "Pass" continues in processing.

**7.2.4.6. BGP Import OUT rules**

Import OUT filter [PP1] rules. The order of rules matters. Maximum number of filter rules is 256.

**Filter policy**

List box {Accept; Reject}, default = "Accept"

Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Import OUT filter**.

**Filter limit**

Number {1 – 65535}, default = 1024

Limit of the accepted routing rules from the neighbor. The limit applies before this Import OUT filter. Excess rules are dropped.

**Active**

List box {On; Off}, default = "On"

Enables / disables the filter rule.

**Note**

Optional comment.

**Filter network**

List box {Off; Match; Not match}, default = "Off"

Selects a method of the routing rule destination range comparison.

**IP address / mask**

IP address / mask, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared

**Mask from**

Number {0 – 32}, default = 0

**Mask to**

Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

**Filter BGP path**

List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"

Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.

**Path position**

List box {Any; Neighbor; Source}, default = "Any"

Selects position of the specific AS (**Path AS**). "Any" – anywhere on the path. "Neighbor" – the path was received from this AS (last on the path). "Source" – routing rule originates from this AS (first on the path).

**Path AS**

Number {0 – (2<sup>32</sup>-1)}, default = 65000

The number of the AS searched for.

**Action**

List box {Accept; Reject; Pass}, default = "Accept"

Defines what action is taken with the matching routing rule. "Pass" continues in processing.

**Prepend local AS**

Number {0 – 8}, default = 0

Enables to append (even multiple times) local AS number to the BGP path end – making the path virtually longer. The longer path is handicapped during the comparisons and selections.

**7.2.4.7. BGP Export OUT filter**

Export OUT filter rules. The order of rules matters. Maximum number of filter rules is 256.

**Filter policy**

List box {Accept; Reject}, default = "Accept"

Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Export OUT filter**.

**Active**

List box {On; Off}, default = "On"

Enables / disables the filter rule.

**Note**

Optional comment.

**Filter network**

List box {Off; Match; Not match}, default = "Off"

Selects a method of the routing rule destination range comparison.

### IP address / mask

List box {Off; Match; Not match}, default = "Off"

IP address and mask defines the network prefix to be compared

### Mask from

Number {0 – 32}, default = 0

### Mask to

Number {0 – 32}, default = 32

Definition of the enabled range of the mask length of the processed routing rule.

### Filter protocol

List box {Off; Match; Not match}, default = "Off"

Selects the way how the routing rule source protocol is compared.

### Protocol

List box {System; OSPF; BGP; BGP external; BGP internal}, default = "System"

Selection of the protocol origin. "System" – stands for rules from the ordinary routing table.

### Filter OSPF tag

List box {Off; Match; Not match}, default = "Off"

Selects the way of filtering based on OSPF tag.

### OSPF tag

Number {0 – (2<sup>32</sup>-1)}, default = 0

OSPF tag to be compared. The tag is added to a rule when inserted to OSPF.

### Filter BGP path

List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"

Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.

### Path position

List box {Any; Neighbor; Source}, default = "Any"

Selects position of the specific AS (**Path AS**). "Any" – anywhere on the path. "Neighbor" – the path was received from this AS (last on the path). "Source" – routing rule was originated from this AS (first on the path).

### Path AS

Number {0 – (2<sup>32</sup>-1)}, default = 65000

The number of the AS searched for.

### Action

List box {Accept; Reject; Pass}, default = "Accept"

Defines what action is taken on the routing rule. "Pass" continues in processing.

## 7.2.5. Link management

The link manager allows to set the switchover of the main link (in the event of its failure) to an existing backup link by automatic changes of routing rules.

Several links can be defined. The connection through the current link and all higher priority links are checked. Links with a lower priority can also be checked.

When the current link fails, link manager switches to the next functional link with a lower priority. If the link is not being checked, it is assumed to be operational and therefore it is also switched to such a link. All links' interfaces are being checked passively and if configured, actively by ICMP ping as well.

IPsec tunnels can be bound to particular links via Peer ID parameter so they are also swapped respectively.

It is automatically switched to higher priority links once they are restored.

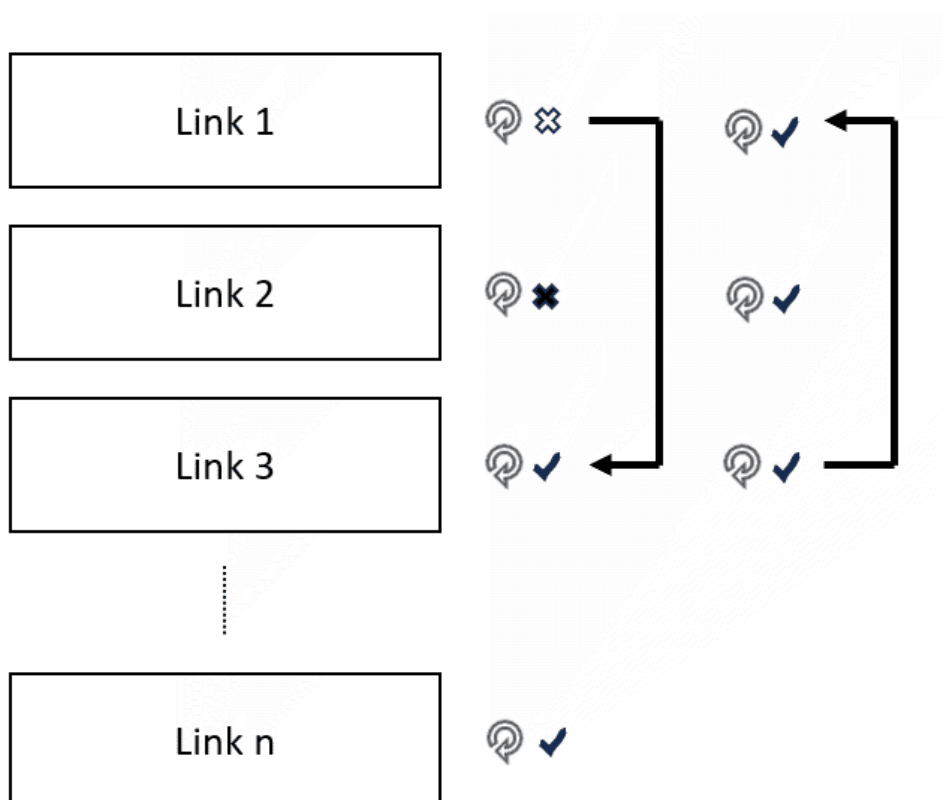
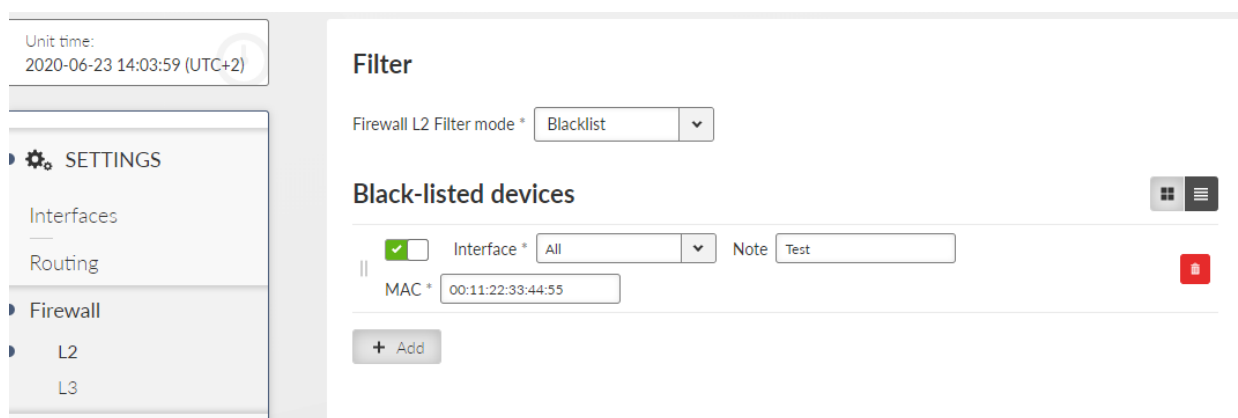


Fig. 7.3: Link management scheme

## 7.3. Firewall

### 7.3.1. Firewall L2



### Filter mode

List box {Off; Blacklist; Whitelist}, default = "Off"

#### Blacklist

The MAC addresses listed in the table are blocked, i.e. all packets to/from them are discarded. The traffic to/from other MAC addresses is allowed.

#### Whitelist

Only the MAC addresses listed in the table are allowed, i.e. only packets to/from them are allowed. The traffic to/from other MAC addresses is blocked.

### Active

List box {Off; On}, default = "On"

If "On", Layer 2 Linux firewall rule is activated.

### Interface

List box {All; ETH1..ETH5}, default = "All"

### MAC

IPv4 MAC address



#### Note

L2 firewall settings do not impact the local ETH access, i.e. settings never deny access to a locally connected M!DGE3 (web interface, ping, ...).

## 7.3.2. Firewall L3

### 7.3.2.1. Forward

Set of rules applying for the traffic coming through the cellular router.

Edit
×

Enable rule

Protocol

Source IP / Mask

Input interface

Destination IP / Mask

Output interface

Connection state New

Connection state Established

Connection state Related

Action

Note

Confirm and close
Close

**L3**

Enables / disables L3 firewall; default = "Off"

Each individual firewall rule is described by following parameters:

**Protocol**

List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"

**Source IP / Mask**

The rule with narrower mask has higher priority. The rule's order does affect priority.

**Source port (from) / Source port (to)**

Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

**Input interface**

List box {All; WWAN; All ETH; EXT; ETH1..ETH5; GRE L2; GRE L3; Other}, default = "All"

**Destination IP / Mask**

Defines the destination IP subnet.

**Destination port (from) / Destination port (to)**

Interval of destination ports.

**Output interface**

List box {All; WWAN; All ETH; EXT; GRE L3; Other}, default = "All"

**Connection state New**

List box {Off; On}, default = "Off"

Relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening a new TCP connection). Used e.g. for allowing to open TCP only from M!DGE3 network to outside.

**Connection state Established**

List box {Off; On}, default = "Off"

Relates to an already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from M!DGE3 network to outside.

**Connection state Related**

List box {Off; On} default = "Off"

A connection related to the "Established" one, e.g. FTP typically uses 2 TCP connections control and data, where data connection is created automatically by using dynamic ports.



**Note**

Management connection to a remote M!DGE3 may be lost, when another M!DGE3 acts as a router along the management packets path and TCP port 8889 (Remote Access) is disabled (DENY rule) in L3 firewall settings of that routing M!DGE3 (FORWARD chain).

**Action**

List box {Deny; Allow}, default = "Deny"

**7.3.2.2. Input**

Set of rules applying for traffic heading into the cellular router. Incoming traffic from unwanted source addresses can be blocked by setting parameter *Action* to "Deny, add to the blocklist".

Edit ×

Enable rule

Service

Protocol

Source IP / Mask

Input interface

Connection state New

Connection state Established

Connection state Related

Action

Note

**L3**

Enables / disables L3 firewall; default = "Off"

Each individual firewall rule is described by following parameters:



**Service**

Rules, that open management access through service interfaces.

List box {Other; COM1; COM2; COM3; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Remote access; SNMP; NTP}, default = "Other"

**Protocol**

List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"

**Source IP / Mask**

Source IP address and mask. The rule with narrower mask has higher priority. The rule's order does affect priority.

**Source port (from) / Source port (to)**

Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

**Input interface**

List box {All; WWAN; All ETH; EXT; ETH1..ETH5; GRE L2; GRE L3; Other}, default = "All"

**Destination port (from) / Destination port (to)**

Interval of destination ports.

**Connection state New**

List box {Off; On}, default = "Off"

Relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening a new TCP connection). Used e.g. for allowing to open TCP only from M!DGE3 network to outside.

**Connection state Established**

List box {Off; On}, default = "Off"

Relates to an already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from M!DGE3 network to outside.

**Connection state Related**

List box {Off; On} default = "Off"

A connection related to the "Established" one. e.g. FTP typically uses 2 TCP connections control and data, where data connection is created automatically by using dynamic ports.

**Note**

Management connection to a remote M!DGE3 may be lost, when another M!DGE3 acts as a router along the management packets path and TCP port 8889 (Remote Access) is disabled (DENY rule) in L3 firewall settings of that routing M!DGE3 (FORWARD chain).

**Action**

List box {Deny; Allow; Deny, Add to Blocklist}, default = "Deny"

Deny, Add to Blocklist - all traffic from the particular address will be automatically dropped. Blocklist has limited capacity of 512 addresses. Once its capacity is exceeded, the oldest address is overwritten. Addresses added to the blocklist remain in for one week (604,800s) and are deleted from it afterwards. Change of configuration including firewall, or unit reboot will delete those addresses as well.

**7.3.2.3. Output**

Set of rules applying for the traffic leaving from the cellular router.

Edit ×

Enable rule

Service  ▼

Protocol  ▼

Destination IP / Mask

Connection state New  ▼

Connection state Established  ▼

Connection state Related  ▼

Action  ▼

Note

**L3**

Enables / disables L3 firewall; default = "Off"  
Each individual firewall rule is described by following parameters:

**Service**

Rules, that allow returning management packets (replies) through service interface.  
List box {Other; COM1; COM2; COM3; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Remote access; SNMP; NTP}, default = "Other"  
The rule's order does affect priority.

**Protocol**

List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"

**Source port (from) / Source port (to)**

Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

**Destination IP / Mask**

Defines the destination IP / subnet.

**Destination port (from) / Destination port (to)**

Interval of destination ports.

**Connection state New**

List box {Off; On}, default = "Off"  
Relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening a new TCP connection). Used e.g. for allowing to open TCP only from M!DGE3 network to outside.

**Connection state Established**

List box {Off; On}, default = "Off"

Relates to an already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from M!DGE3 network to outside.

### Connection state Related

List box {Off; On} default = "Off"

A connection related to the "Established" one. e.g. FTP typically uses two TCP connections control and data, where data connection is created automatically by using dynamic ports.



#### Note

Management connection to a remote M!DGE3 may be lost, when another M!DGE3 acts as a router along the management packets path and TCP port 8889 (Remote Access) is disabled (DENY rule) in L3 firewall settings of that routing M!DGE3 (FORWARD chain).

### Action

List box {Deny; Allow}, default = "Deny"

### Note

Optional comment.

## 7.3.3. NAT - Network address translation

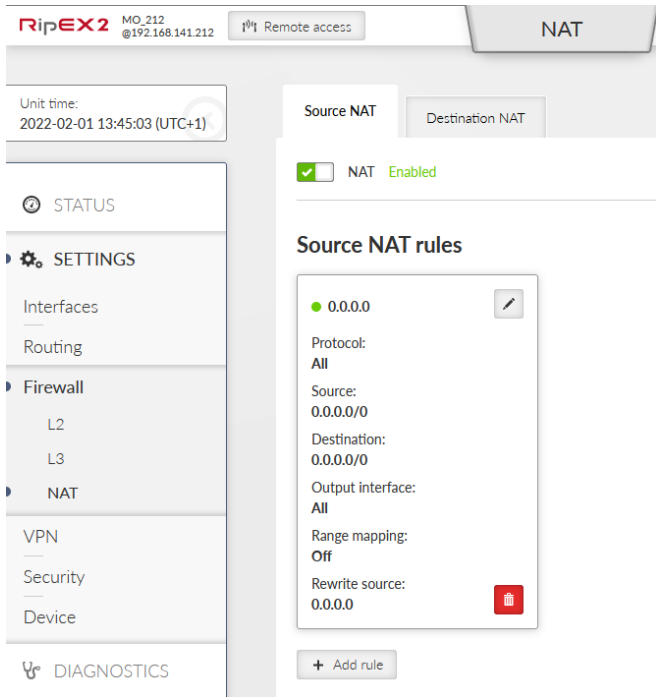
**Network address and port translation (NAPT)** is a method of mapping an IP address (or port) space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

### 7.3.3.1. Source NAT

Source Network Address Translation (SNAT) - rewrites the source address and/or port within the leaving connection and performs opposite changes for returning packets.

SNAT:

- Allows to pretend, that the packets come from a device, that performs SNAT.
- Performs during packet output from a device (after routing and filtering in firewall).



**Enable**

List box {Enable; Disable}, default = "Disable"  
Enables / disables all Source NAT rules.

Parameters "**Protocol**", "**Source IP / Mask**", "**Destination IP / Mask**", "**Output Interface**", "**Source port from**", "**Source port to**", "**Destination port from**", "**Destination port to**" and "**Protocol number**" define a filter, which is capturing specified packets. SNAT rule applies for those packets.

Parameters "**Source port from**", "**Source port to**", "**Destination port from**" and "**Destination port to**" occur only if parameter "**Protocol**" is set to "UDP" or "TCP".

Parameter "**Protocol number**" occurs only if parameter "**Protocol**" is set to "Other".

**Protocol**

List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"  
Filters selected protocol. If none of the mentioned values suits, select "Other".

**Protocol number**

Number {0 – 255}, default = 1  
This parameter occurs only, if parameter "**Protocol**" is set to "Other".

**Source IP / Mask**

IP address, default = 0.0.0.0/0  
Defines the source IP subnet.

**Source port (from) / Source port (to)**

Number {0 – 65535}, default = 0  
Defines the range of values of source port. Value 0 means, that it is not filtered according to the source port. If only one port is required, set both parameters to the same number. These parameters occur only, if parameter "**Protocol**" is set to "UDP" or "TCP".

**Destination IP / Mask**

IP address, default = 0.0.0.0/0

Defines the destination IP subnet.

**Destination port (from) / Destination port (to)**

Number {0 – 65535}, default = 0

Defines the range of values of destination port. Value 0 means, that it is not filtered according to the destination port. These parameters occur only, if parameter “**Protocol**” is set to “UDP” or “TCP”.

**Output Interface**

List box {All; ; WWANAll ETH; EXT; GRE L3; Other}, default = "All"

Filters selected interfaces.

**Output interface name**

Has to be set as one of existing interfaces (the name of LAN (or VLAN) interface, the name of GRE tunnel, etc.). This parameter occurs only, if parameter “**Output Interface**” is set to “Other”.

**Range mapping**

List box {Off; IP address to IP address}, default = "Off"

**Off** – Source address and (or) port will be replaced by values from parameters “**Rewrite source IP**” and “**Rewrite source port**”. This applies only if those parameters are set (they are not set as 0.0.0.0).

**IP address to IP address (NETMAP)** – Rewriting the Range mapping of source IP address. New source address will contain prefix from parameters “**Rewrite Source IP**” and “**Rewrite Source IP / Mask**”. Rest of the source address will be filled by the original source address.

**Rewrite source IP**

IP address, default = 0.0.0.0/0

Defines a new source address. Value 0.0.0.0/0 means, that the source address is not changed.

**Rewrite source port**

Number {0 – 65535}, default = 0

Defines a new source port (rewriting multiple defined ports into one). Value 0 means, that the source port is not changed.

**Note**

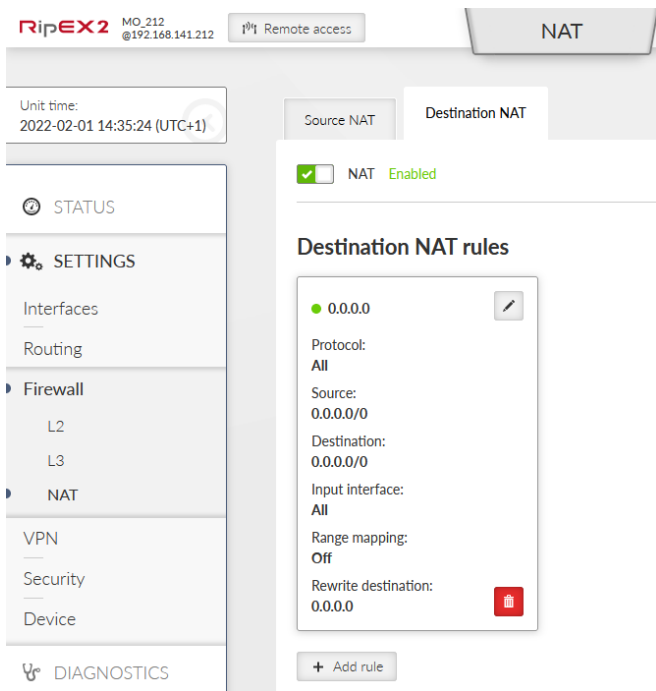
Optional comment.

### 7.3.3.2. Destination NAT

Destination Network Address Translation (DNAT) - rewrites the destination address and/or port within incoming connection and performs opposite changes for returning packets.

DNAT:

- Allows to redirect connection destination to a device, that performs DNAT.
- Performs during packet input to a device (before redirecting and filtering in firewall).



#### Enable

List box {Enable; Disable}, default = "Disable"  
Enables / disables all Destination NAT rules.

Parameters "**Protocol**", "**Source IP / Mask**", "**Destination IP / Mask**", "**Output Interface**", "**Source port from**", "**Source port to**", "**Destination port from**", "**Destination port to**" and "**Protocol number**" define a filter, which is catching specified packets. SNAT rule applies for those packets.

Parameters "**Source port from**", "**Source port to**", "**Destination port from**" and "**Destination port to**" occur only if parameter "**Protocol**" is set to "UDP" or "TCP".

Parameter "**Protocol number**" occurs only if parameter "**Protocol**" is set to "Other".

#### Protocol

Filters selected protocol. If none of the mentioned values suits, select "Other".

#### Protocol number

Number {0 – 255}, default = 1

This parameter occurs only, if parameter "**Protocol**" is set to "Other".

#### Source IP / Mask

IP address, default = 0.0.0.0/0

Defines the source IP subnet.

**Source port (from) / Source port (to)**

Number {0 – 65535}, default = 0

Defines the range of values of source port. Value 0 means, that it is not filtered according to the source port. If only one port is required, set both parameters on the same number. These parameters occur only, if parameter “**Protocol**” is set to “UDP” or “TCP”.

**Destination IP / Mask**

IP address, default = 0.0.0.0/0

Defines the destination IP subnet.

**Destination port (from) / Destination port (to)**

Defines the range of values of destination port. Value 0 means, that it is not filtered according to the destination port. These parameters occur only, if parameter “**Protocol**” is set to “UDP” or “TCP”.

**Input interface**

List box {All; WWAN; All ETH; EXT; GRE3; Other}, default = "All"

Filters selected interfaces.

**Input interface name**

Has to be set as one of existing interfaces (the name of LAN (or VLAN) interface, the name of GRE tunnel, etc.). This parameter occurs only, if parameter “**Input Interface**” is set to “Other”.

**Range mapping**

List box {Off; IP address to IP address}, default = "Off"

- Off – Destination address and (or) port will be replaced by values from parameters “**Rewrite destination IP**” and “**Rewrite destination port**”. This will apply only if those parameters are set (they are not set as 0.0.0.0).
- IP address to IP address (NETMAP) – Rewriting the Range mapping of source IP address. New source address will contain prefix from parameters “**Rewrite Source IP**” and “**Rewrite Source IP / Mask**”. Rest of the source address will be filled by the original source address.
- Port to IP address (PORTMAP): Range mapping of destination ports (parameters “**Destination port from**”, “**Destination port to**”). New range mapping of destination ports origins in parameter “**Rewrite destination IP**”. It can be additionally overwritten to parameter “**Rewrite destination port**”.

Example:

**Edit destination NAT rule** ×

Active

Protocol  ▼

Source IP / Mask

Source port (from)

Source port (to)

Destination IP / Mask

Destination port (from)

Destination port (to)

Input interface  ▼

Range mapping  ▼

Rewrite destination IP

Rewrite destination port

10.10.10.1:20000 - 10.10.10.15:20000

Note

Explanation of non-typical and interesting parameters:

**Destination port (from) and Destination port (to)**

DNAT rule applies to UDP data with destination ports within the 20001-20015 range only

**Input interface**

Data must be received on any ETH port

**Range mapping**

Set to "Port to IP address" - i.e., destination ports change the destination IP address(es) accordingly.

**Rewrite destination IP and Rewrite destination port**

Set to IP 10.10.10.1 and port 502 - resulting in a range of IPs 10.10.10.1 - 10.10.10.15 due to Destination ports of received UDP data in a range of 20001-20015 (15 ports = 15 IP addresses). A new port is always 20000 (i.e., DNP3 default port).

**Rewrite destination IP**

IP address, default = 0.0.0.0/0

Defines a new destination address. Value 0.0.0.0/0 means, that the destination address is not changed.

**Rewrite destination port**

Number {0 – 65535}, default = 0

Defines a new destination port (rewriting multiple defined ports into one). Value 0 means, that the destination port is not changed.



**Note**

Optional comment.

**7.3.3.3. Cooperation with other services**

- MASQUERADE rule for Cellular connection has lower priority than user NAT (it is tested after the NAT), thus it is possible to create exceptions in NAT settings.
- By using DNAT it is possible to intercept a passing connection and redirect it into the MIDGE3 (similar to a proxy behavior).
- For redirection
  - Local IP address will be filled into “**Rewrite destination IP**” parameter.
  - Service port, to which is the local address being redirected will be filled into “**Rewrite destination port**” parameter.

**NAT and IPsec**

- DNAT can be used before packing a packet into the IPsec. For more information see *Section 7.4.1.3, “Interaction with DNAT”*.
- SNAT works on packets unpacked from IPsec.
- SNAT can be used before packing a packet into the IPsec (parameter “**Output interface**” must be set to “All”)
- Rules of SNAT and MASQUERADE (from Cellular) change packets addresses before capturing by IPsec traffic selector.

**7.4. VPN**

VPN (Virtual Private Network) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

**7.4.1. IPsec**

Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys for use during the session. IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec is an end-to-end security scheme operating within the Internet Layer of the Internet Protocol Suite. IPsec is recognized as a secure, standardized and well-proven solution by the professional public.

Although there are 2 modes of operation, MIDGE3 only offers a Tunnel mode. In Tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet (ESP – Encapsulating Security Payloads) with a new IP header.

Symmetrical cryptography is used to encrypt the packets. The symmetric keys must be safely delivered to the peer. In order to maintain a secure connection, symmetric keys must be regularly exchanged. The protocol used for secure key exchange is IKE (Internet Key Exchange). Both IKE version 1 and the newer version 2 are available in M!DGE3.

IKE protocol communication with the peer is established using UDP frames on port 500. However, if NAT-T (NAT Traversal) or MOBIKE (MOBile IKE) are active, the UDP port 4500 is used instead.



**Note**

NAT-T is automatically recognized by IPsec implementation in M!DGE3.

The IPsec tunnel is provided by Security Association (SA). There are 2 types of SA:

- IKE SA: IKE Security Association providing SA keys exchange with the peer.
- CHILD SA: IPsec Security Association providing packet encryption.

Every IPsec tunnel contains 1 IKE SA and at least 1 CHILD SA. In M!DGE3 can be set maximum of 24 IKE\_SA and 48 CHILD\_SA (TS).

Link partner (peer) secure authentication is assured using Pre-Shared Key (PSK) authentication method: Both link partners share the same key (password).

As and when the CHILD SA expires, new keys are generated and exchanged using IKE SA.

As and when the IKE SA version IKEv1 expires - new authentication and key exchange occurs and a new IKE SA is created. Any CHILD SA belonging to this IKE SA is re-created as well.

As and when the IKE SA version IKEv2 expires one of two different scenarios might occur:

- If the re-authentication is required - the behavior is similar to IKEv1 (see above).
- If the re-authentication is not required - only new IKE SA keys are generated and exchanged.

| Assoc. | Tr. sel. | Peer ID | Protocol | Local network | Remote network | State | Uptime [s] | Rekey time [s] | Traffic in [B/pack] | Traffic out [B/pack] |
|--------|----------|---------|----------|---------------|----------------|-------|------------|----------------|---------------------|----------------------|
| A0     | -        | ripx-b  | -        | -             | -              | up    | 37         | 12955          | -                   | -                    |
| A0     | T0       | ripx-b  | gre      | 10.0.0.1/32   | 10.0.0.2/32    | up    | 37         | 3455           | 2016/8              | 2016/8               |
| A0     | T1       | ripx-b  | icmp     | 10.0.0.1/32   | 10.0.0.2/32    | up    | 37         | 3277           | 0/0                 | 0/0                  |
| A0     | T2       | ripx-b  | tcp      | 10.0.0.1/32   | 10.0.0.2/32    | up    | 35         | 3426           | 0/0                 | 0/0                  |

**IPsec**

{Enable; Disable}, default = "Disable"

IPsec system turning On/Off

There can be a maximum of 16 active CHILD SA (in total over all Active IKE SA).

Every "Active" line must have an equivalent on the peer side with reversed "Local network..." and "Remote network..." fields.

"Local network..." and "Remote network..." fields must contain different address ranges and must not interfere with the USB service connection (10.9.8.7/28) or internal connection to FPGA (192.0.2.233/30).

Each "Active" Traffic selector in the configuration table must be unique.

**7.4.1.1. IPsec settings****Make-before-break**

{On; Off}, default = "Off"

This parameter is valid for all IKE SA using IKEv2 with re-authentication. A temporary connection breaks during IKE\_SA re-authentication is suppressed by this parameter. This function may not operate correctly with some IPsec implementations (on peer side).

**7.4.1.2. IPsec associations**

To further configure IPsec VPN tunnel, click the **Add VPN configuration** button.

**Add / Edit IPsec VPN tunnel associations**

Every item in the table represents one IKE SA. There can be a maximum of 24 active IKE SA (limited by system resources).

**Edit IPsec VPN tunnel configuration**

Enable tunnel

Note

Start state  ▼

MOBIKE  ▼

Dead Peer Detection  ▼

**Start state**

List box {Passive; On demand; Start}, default = "Passive"

**MOBIKE**

List box {On; Off}, default = "On"

Enables MOBIKE for IKEv2 supporting mobility or migration of the tunnels. Please note IKE is moved from port 500 to port 4500 when MOBIKE is enabled. The peer configuration must match.

It is strongly recommended to use MOBIKE mode in case of routing the traffic over the Cellular interface.

**Dead Peer Detection**

List box {On; Off}, default = "On"

Detection of lost connection with the peer. IKE test packets are sent periodically. When packets are not acknowledged after several attempts, the connection is closed (corresponding actions

are initialized). In the case when Detection is not enabled, a connection loss is discovered when regular key exchange process is initiated.

**DPD period [s]**

Number {5 - 28800}, default = 30

Dead Peer Detection check period. This parameter is available only if parameter **Dead Peer Detection** is set to "On".

**DPD action**

List box {Clear; Hold; Restart}, default = "Hold"

One of three connection states automatically activated when connection loss is detected:

Clear – connection is closed and waiting

Hold – connection is closed. Connection is established when first packet transmission through tunnel is attempted.

Restart – connection is established immediately

This parameter is available only if parameter **Dead Peer Detection** is set to "On".

**Phase 1 IKE**

Parameters related to IKE SA (IKE Security Association) provide SA keys exchange with the peer.

**Phase 1 - IKE**

|                            |  |   |
|----------------------------|--|---|
| IKE version                | <input type="text" value="IKEv2"/>           | ▼ |
| Authentication method      | <input type="text" value="PSK"/>             | ▼ |
| Encryption algorithm       | <input type="text" value="AES128"/>          | ▼ |
| Hash Algorithm             | <input type="text" value="SHA256"/>          | ▼ |
| Diffie-Hellman group (PFS) | <input type="text" value="Group 15 (MODF)"/> | ▼ |
| Reauthentication           | <input type="text" value="Off"/>             | ▼ |
| SA lifetime [s]            | <input type="text" value="14400"/>           |   |

**Authentication method**

List box {PSK}

Peer authentication method. Peer configuration must match.

The "main mode" negotiation is the only option supported. The "aggressive mode" is not supported; it is recognized as unsafe when combined with PSK type of authentication.

**Encryption algorithm**

List box {3DES (legacy); AES128; AES192; AES256}, default = "AES128"

IKE SA encryption algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

**Hash algorithm**

List box {MD5 (legacy); SHA1 (legacy); SHA256; SHA384; SHA512}, default = "SHA256"

IKE SA integrity algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

**Diffie-Hellman group (PFS)**

List box {None (legacy); Group 2 (MODP1024, legacy); Group 5 (MODP1536, legacy); Group 14 (MODP2048); Group 15 (MODP3072); Group 25 (ECP192); Group 26 (ECP224); Group 19

(ECP256); Group 20 (ECP384); Group 21 (ECP521); Group 27 (ECP224BP); Group 28 (ECP256BP); Group 29 (ECP384BP); Group 30 (ECP512BP); Group 31 (X25519); Group 32 (X448)}, default = "Group 15 (MODP3072)"

The PFS (Perfect Forward Secrecy) feature is performed using the Diffie-Hellman group method.

PFS increases IKE SA key exchange security. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

The higher the Diffie-Hellman group, the higher the security but also the higher the network and CPU load.

### Reauthentication

List box {On; Off}, default = "Off"

This parameter is valid if IKEv2 is used. It determines the next action after IKE SA has expired.

When enabled: the new IKE SA is negotiated including new peer authentication. When disabled: only the new keys are exchanged.

### SA lifetime [s]

Number {180 – 86400}, default = 14400 s (4 hours)

Time of SA validity. The new key exchange or re-authentication is triggered immediately the key expires. The true time of expiration is randomly selected within the range of 90-110%.

Unfortunately, the more frequent the key exchange, the higher the network and CPU load.



#### Note

If low capacity channel is used, the MIDGE3's channel load can be affected during the key exchange process.

### Phase 2 – IPsec

Certain parameters are shared by all subordinate CHILD SA. IPsec Security Association provides packet encryption (user traffic encryption).

#### Phase 2 - IPsec

|                            |                 |   |
|----------------------------|-----------------|---|
| Encryption algorithm       | AES256          | ▼ |
| Hash Algorithm             | SHA512          | ▼ |
| Diffie-Hellman group (PFS) | Group 20 (ECP38 | ▼ |
| Payload compression        | On              | ▼ |
| SA lifetime [s]            | 3600            |   |

### Encryption algorithm

List box {3DES (legacy); AES128; AES192; AES256}, default = "AES128"

IKE CHILD SA encryption algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

### Hash algorithm

List box {MD5 (legacy); SHA1 (legacy); SHA256; SHA384; SHA512}, default = "SHA256"

IKE CHILD SA integrity algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

The same value as selected for the Integrity algorithm, is used for the PRF (Pseudo-Random Function).

**Diffie-Hellman group (PFS)**

List box {None (legacy); Group 2 (MODP1024, legacy); Group 5 (MODP1536, legacy); Group 14 (MODP2048); Group 15 (MODP3072); Group 25 (ECP192); Group 26 (ECP224), Group 19 (ECP256); Group 20 (ECP384); Group 21 (ECP521); Group 27 (ECP224BP); Group 28 (ECP256BP); Group 29 (ECP384BP); Group 30 (ECP512BP); Group 31 (X25519); Group 32 (X448)}, default = "Group 15 (MODP3072)"

The PFS (Perfect Forward Secrecy) feature is performed using the Diffie-Hellman group method.

PFS increases IKE CHILD SA key exchange security. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

The higher the Diffie-Hellman group, the higher the security but also the higher the network and CPU load.

**Payload compression**

This parameter enables payload compression. This takes place before encryption. Peer configuration must match.

**SA lifetime [s]**

Number {180 – 86400}, default = 3600 s (1 hour)

Time of CHILD SA validity. The new key exchange or re-authentication is triggered immediately the key expires. The true time of expiration is randomly selected within the range of 90-110%. The SA lifetime for CHILD SA is normally much shorter than SA lifetime for IKE SA because the CHILD SA normally transfers much more data than IKE SA (key exchange only). Changing the keys serves as protection against breaking the cypher by analyzing big amounts of data encrypted by the same cypher.

**Note**

If low capacity channel is used, the M!DGE3's channel load can be affected during the key exchange process.

**PSK**

PSK (Pre-shared key) authentication is used for IKE SA authentication. The relevant peer is identified using its "Peer ID". The key must be the same for both local and peer side of the IPsec.

**PSK**

Mode  ▼

Passphrase

**Mode**

List box {Passphrase; Key}, default = "Passphrase"

**Passphrase**

The PSK key is entered as a password. Empty password is not allowed (max. length is 128 characters). Passphrase must not contain any unsupported characters. Unsupported characters are: ", ` , \ , \$ , ; .

**Key**

It is possible to set 256 bits long Key instead of Passphrase. This parameter occurs only, if parameter **Mode** is set to "Key".

## IPsec associations

Edit VPN configuration
 Peer address 
 Local ID 
 Peer ID

### Peer Address

Default = 0.0.0.0  
IKE peer IP address.

### Local ID

IP address or FQDN (Fully Qualified Domain Name) is used as the Local side identification. It must be the same as "Peer ID" of the IKE peer.

### Peer ID

IP address or FQDN (Fully Qualified Domain Name) is used as the IKE peer identification. It must be the same as "Local ID" of the IKE peer. The "Peer ID" must be unique in the whole table.

#### 7.4.1.2.1. Traffic selector

Defines which traffic is forwarded to the IPsec tunnel. The rule that defines this selection matches an incoming packet to "Local network ..." and "Remote network ..." address ranges.

##### Traffic selectors

Local network address / Mask 
 Remote network address / Mask 
 Note

### Local network address / Mask

Source IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

### Remote network address / Mask

Destination IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

### Protocol

List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"  
Defines the transport protocol of packets which will be caught and encrypted.

### Protocol number

Number {1 – 255}, default = 1  
Defines the number of the transport protocol of packets which will be caught and encrypted. This parameter is available only if parameter **Protocol** is set to "Other".

#### 7.4.1.3. Interaction with DNAT

If IPsec captures packets which were modified by DNAT, routing rules automatically created by IPsec rules will not apply to them, because DNAT rewrites their destination address. Therefore a new static routing rule must be created (SETTINGS > Routing > Static) for those packets.

### 7.4.2. GRE L2

GRE L2 tunnel is interconnected to the bridge (LAN interface) as one of the bridge's port, it captures Ethernet frames of the bridge and sends them to the other end of the tunnel. It enables to build bridge via the complex network and combine the local partial networks to one network.

GRE L2 tunnel can be used to tunnel the Q-in-Q and IPv6 traffic over the RipEX IPv4 network.



#### GRE L2 Enable

Switches all L2 tunnels On or Off.

#### Individual L2 tunnels:

##### Enable

Enables particular L2 tunnel. Maximum number of configurable tunnels is 256.

##### Note

Optional comment.

##### Peer address

IP address of the equipment with the second end of the tunnel. This address is the expected source address of incoming GRE packets from the peer.

##### Network interface name

Has to be set as one of existing bridge's name in SETTING/Interfaces/Ethernet/ Network interface Name.

##### Key enabled

Enables using key identification of the tunnel from/to the same peer.

##### Key

Identification number of the tunnel Number {0 – 4,294,967,295}, default = 0

##### MTU [B]

MTU of the L2 tunnel. Number {74 – 1500}, default = 1430 B

**Overhead of the L2 tunnel is 38 B**, so it should be GRE MTU = Path MTU - 38.

Minimum MTU value to establish TCP between MIDGE3 units = 576 B.



**Note**

For traffic in bridged network (e.g. when using Transparent protocol), it is necessary to set the MTU to a proper value, otherwise there is a risk of packet fragmentation and thus compromising efficiency and reliability of the transfer.

**7.4.3. GRE L3**

GRE L3 tunnel works as an additional unit's interface with its own IP address (and mask). The routing rules are used for sending packets to this interface. It bridges part of the network, so it seems to be one hop for the user traffic.

**GRE L3 Enable**

Switches all L3 tunnels On or Off.

**Individual L3 tunnels:****Enable**

Enables particular L3 tunnel. Maximum number of configurable tunnels is 256.

**Note**

Optional comment.

**Peer address**

IP address of the equipment with the second end of the tunnel. This address is the expected source address of incoming GRE packets from the peer.

**Tunnel address / Mask**

IP address and mask of the GRE tunnel interface

**Key enabled**

Enables using key identification of the tunnel from/to the same peer.

**Key**

Identification number of the tunnel Number {0 – 4,294,967,295}, default = 0

**MTU**

MTU of the L2 tunnel. Number {70 – 1476}, default = 1476

**Overhead of the L3 tunnel is 24 B**, so it should be GRE MTU = Path MTU - 24. If the MTU is bigger than is allowed along the route, the GRE packets will be discarded and ICMP report will be send back to the source of the original packet (Path MTU discovery).

Minimum MTU value to establish TCP between M!DGE3 units = 576 B.

## 7.5. Security

User authentication is required to access RipEX unit management. There are two types of user authentication which differ in the user account location:

Local authentication – user accounts are stored directly in the RipEX unit

Remote authentication – user accounts are stored on a remote authentication server (RADIUS is implemented)

There are four different levels of user access privileges – they are bound with four different user access roles:

### **Guest (role\_guest)**

Read only access for configuration parameters (except secured part of configuration). Diagnostics tools are available.

### **Technician (role\_tech)**

All privileges of Guest role plus: write access for non-secured part of configuration; unit firmware up/down-grade.

### **Security technician (role\_sectech)**

All privileges of Technician role plus: write access for secured part of configuration (except unit authentication related parts).

### **Administrator (role\_admin)**

No access level restrictions. All privileges of Security technician role plus: user accounts management; remote authentication configuration.

Limitations:

**Tab. 7.2: Overview of roles and rights in each section**

| Section     | Features           |   | Roles / Rights |             |             |       |       |
|-------------|--------------------|---|----------------|-------------|-------------|-------|-------|
|             |                    |   | Guest          | Tech        | Sec tech    | Admin |       |
| SETTINGS    | Interfaces         | Ethernet, COM, Terminal servers, Cellular | Read-only      | Write       | Write       | Write |       |
|             | Routing            | Static                                    | Read-only      | Write       | Write       | Write |       |
|             |                    | Babel, OSPF, BGP                          | Non-visible    | Non-visible | Write       | Write |       |
|             | Firewall           | L2, L3, NAT                               | Read-only      | Write       | Write       | Write |       |
|             | VPN                | IPsec                                     | Non-visible    | Non-visible | Write       | Write |       |
|             |                    | GRE                                       | Read-only      | Write       | Write       | Write |       |
|             | Quality of service |   | Read-only      | Write       | Write       | Write |       |
|             | Security           | Local authentication                      | Non-visible    | Non-visible | Non-visible | Write |       |
|             |                    | RADIUS                                    | Non-visible    | Non-visible | Non-visible | Write |       |
|             |                    | Tamper reset                              | Non-visible    | Non-visible | Non-visible | Write |       |
|             | Device             | Unit                                      |                | Read-only   | Write       | Write | Write |
|             |                    | Configuration                             |                | Read-only   | Write       | Write | Write |
|             |                    | Events                                    |                | Read-only   | Write       | Write | Write |
|             |                    | Software keys                             |                | Read-only   | Write       | Write | Write |
|             |                    | Firmware                                  |                | Non-visible | Write       | Write | Write |
|             | Services           | Firmware distribution                     |                | Non-visible | Write       | Write | Write |
|             |                    | SNMP                                      |                | Non-visible | Non-visible | Write | Write |
|             |                    | SMS                                       |                | Non-visible | Non-visible | Write | Write |
| Hot standby |                    |   | Read-only      | Write       | Write       | Write |       |
| DIAGNOSTICS | Monitoring         |   | Non-visible    | Write       | Write       | Write |       |
|             | Tools              |   | Read-only      | Write       | Write       | Write |       |

At least one Administrator type of account must be defined in the unit.

Maximal number of concurrently active sessions is 64. One user can have multiple sessions opened in the same time. If this limit is reached and a new session is to be opened, the oldest active session is deactivated and a new one is opened.

Maximal number of Local user accounts (all roles together) is 100.

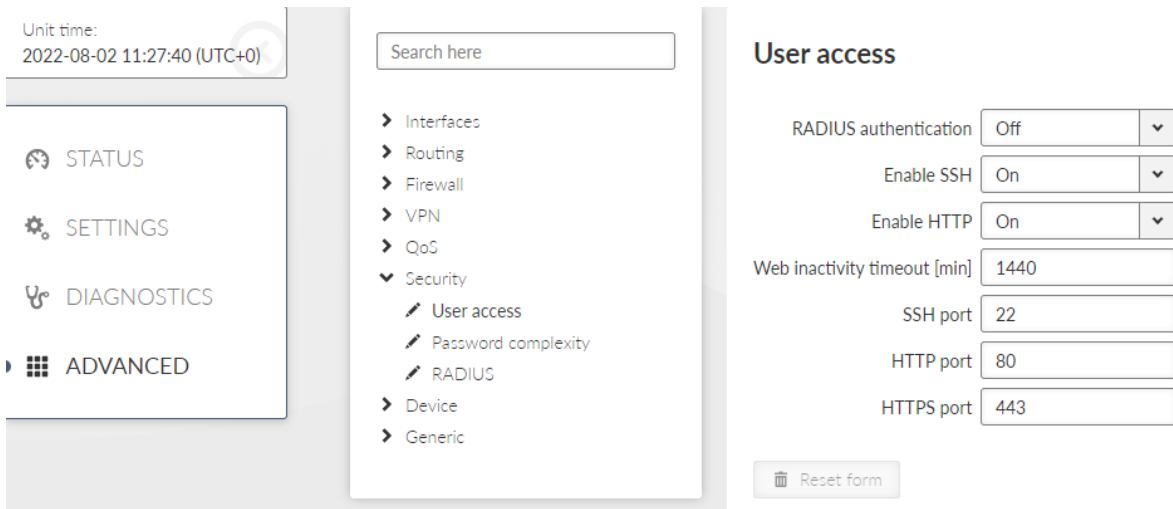


**Note**

The **Remote access** uses local identity and role of the user – there is no additional login to the remote unit (the login into local unit serves as login to the whole network).

### 7.5.1. User access

User access serves for enabling/disabling and setting of used protocol access. It can be used for setting a non-standard port for the protocol as well.



In this section you can:

- Enable/Disable HTTP or SSH access
- Set ports for HTTPS, HTTP and SSH
- Set the length of inactivity timeout on web



**Note**

HTTPS protocol is always active and cannot be turned off.



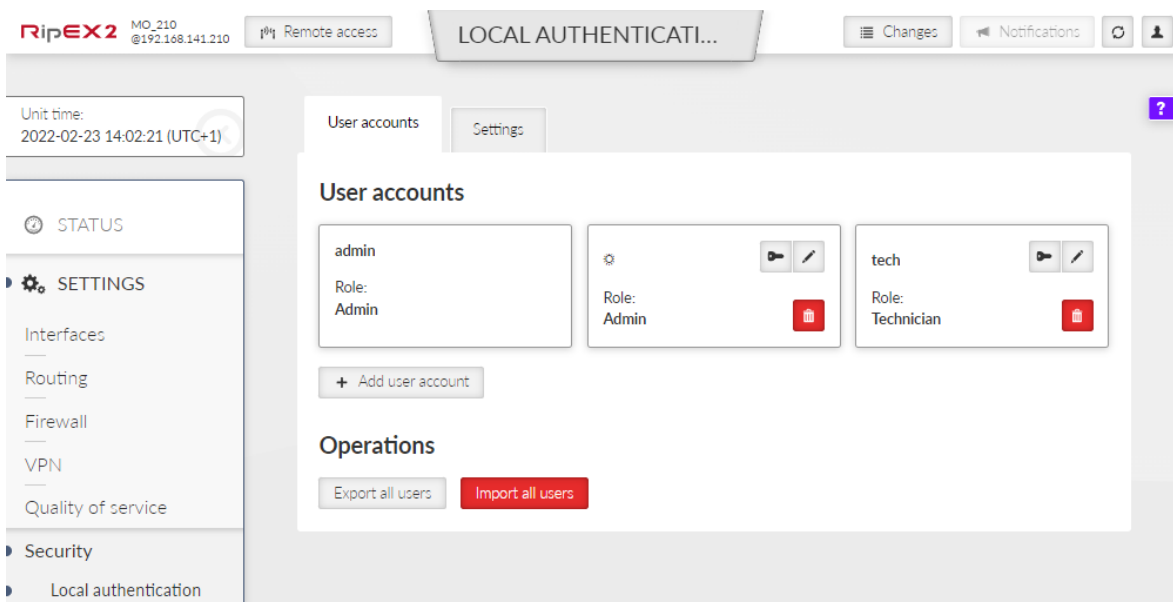
**Note**

When changing settings of HTTP or HTTPS, linux service LigHTTPd restarts. Because of that, the waiting time period for update in the web ends a returns Error: Connection to device timed out.

### 7.5.2. Local authentication

#### 7.5.2.1. User Accounts

The following settings are available only for user with the Administrator role.



Following user account parameters can be changed: password, user role. Any account (except the last one of Administrator role) can be deleted.

**Export all users** button provides backup of all Local user accounts into a file.

**Import all user** button provides restoration of all Local user accounts from a backup file. Active session is logged out automatically after this command.

+ **Add user account** button invokes new user account creation dialog:

**Add user account**
×

Username

Password

Role Admin ▼

Save and close
Close

### Username

String {1–128 char}, default = <empty>

New Username. Every username in the unit must be unique.

### Password

String {5–128 char}, default = <empty>

Password is stored in a secure way.

### Role

List box {Admin; Security Technician; Technician; Guest}, default = "Admin"

**Note**

It is highly recommended to create a new administrator type of account and delete the default “Admin” account.

**Advanced feature**

When the user account is not active for some time, the user will be automatically logged-out. The inactivity timeout of the account is set for 1 day by default. It is possible to change in the range of 5 minutes up-to 2 days (menu ADVANCED > Generic > UserAccess > **Web inactivity timeout**).

**7.5.2.2. Settings**

Allows to set password complexity rules.

The screenshot shows the 'LOCAL AUTHENTICATION' settings page. On the left is a navigation menu with 'STATUS', 'SETTINGS', 'Interfaces', 'Routing', 'Firewall', 'VPN', 'Security', and 'RADIUS'. The 'Security' section is expanded, showing 'Local authentication' and 'RADIUS'. The main content area is titled 'LOCAL AUTHENTICATION' and has two tabs: 'User accounts' and 'Settings'. The 'Settings' tab is active, showing 'Password complexity rules' with five input fields: 'Min. length [No]' (5), 'Min. lowercase letters [No]' (0), 'Min. UPPERCASE letters [No]' (0), 'Min. numbers [No]' (0), and 'Min. special characters [No]' (0).

**Min. length [No]**

Number {5 – 64}, default = 5

The minimum length of the password for all users.

**Min. lowercase letters [No]**

Number {0 – 5}, default = 0

The minimum number of lowercase letters (English letters) which are required in the user password.

**Min. UPPERCASE letters [No]**

Number {0 – 5}, default = 0

The minimum number of uppercase letters (English letters) which are required in the user password.

**Min. numbers [No]**

Number {0 – 5}, default = 0

The minimum number of number characters (0 to 9) which are required in the user password.

**Min. special characters [No]**

Number {0 – 5}, default = 0

The minimum number of special characters (not English upper or lower cases or numbers) which are required in the user password. Non-English letters (like Greek, Russian, Arabic) are counted as special characters.

**Note**

The settings are applicable for new passwords only, already existing passwords will not be affected.

### 7.5.3. Credentials

MIDGEE3 units feature a unified storage solution for keys, certificates and other credentials. This storage is secured and only accessible to users with Sectech permission and higher.

Credentials are separate from configuration to improve security and it also is protected using checksum to prevent unauthorised modification. Because of this all Repository/Key changes are executed immediately and do not go through the “Changes” workflow like the regular configuration.

Note: In this manual and in the user interface we are calling all Credential storage entries “Keys”. While this is a simplification, we believe it is understandable. Further on “Keys” are all keys, public and private certificates, DH parameters, CA chains etc.

Warning: Downgrading the Unit will always reset all Credentials to defaults.

#### 7.5.3.1. General

Credentials are stored in Repositories. Repository is a reserved space, which contains 0-1 Key and is addressable via its ID in the rest of the unit configuration. This construct, while it may seem complicated at first, brings major benefits. Mainly the user can simply update expired certificates in a repository without any need to change configuration using that Repository.

There are two types of Keys: Read-only, easily identifiable by a lock icon and “\_RO\_” prefix. These Keys are built into firmware, or generated automatically on device. The rest are user-defined keys.

Admin website allows users to perform various operations with the keys and repositories.

Using buttons on the bottom of the page we also allow users to download complete credential backup.

There are two ways to restore credentials: Replace, which replaces all Keys with ones from the file, and Update, which merges current and new Keys.

#### 7.5.3.2. Credentials

Credentials show all Repositories and Keys currently on the device. Users can filter them by type and show only valid or all Keys. The card border and bottom label indicate whether the Repository is empty, or whether the Key is valid or invalid.

Each card represents a Repository. Card title is Repository ID. All user-defined repositories can be edited using the “Edit” button and deleted using the red “Delete” button.

##### ID

Unique identifier used to reference Repository in configuration.

Validated according to regular expression: `[a-zA-Z0-9_]{1,128}`. IDs starting with underscore “\_” are reserved for Read Only keys.

##### Type

Defines the type of Key the Repository can contain.

**Note**

Optional comment.

There are several operations, that can be performed on a repository:

**Info**

Displays Key info including checksums.

**Generate**

Generates a new Key using local Certification authority (see below).

**Update**

Updates the Key with a new one. Both file and text, encrypted and unencrypted Keys are supported.

**Download**

Allows download of the Key. Both encrypted and unencrypted downloads are supported, according to Setting (see below).

**Generate CSR (Certificate Signing Request)**

Generates and downloads CSR from eligible Keys.

**Sign CSR (Certificate Signing Request)**

Signs CSR. Both file and text certificates are supported. Signed certificate is automatically downloaded. It is possible to add "extended key usage" Certificate modifier for OpenVPN client/server.

Operation "Add repository" creates an empty Repository.

Shortcut operations "Generate key" and "Upload key" allow users to create a Repository and generate/upload a key into it. These buttons cannot be used to modify existing repositories.

**7.5.3.3. Read-only keys**

**\_RO\_Ssh\_Host\_Key**

Type: SSH Key (PRI)

The SSH host key used to authenticate the server on the client. If missing, it is generated when the station boots.

**\_RO\_Rmt\_Access\_Host\_Key**

Type: RMTACCESS Key (PRI)

Host key for the Remote access server (QSSH). It is used to authenticate the server.

If missing, it is generated when the station starts.

**\_RO\_Rmt\_Access\_Client\_Key**

Type: RMTACCESS Key (PRI)

Key for Remote access (QSSH) client login to the server. Must be present on both sides.

Obtained from FW. If it differs from the version in FW, it is updated.

**\_RO\_Web\_Private\_Key**

Type: Certificate (PRI)

Web server private key (default).

Obtained from FW. If it is different from the version in FW, it is updated.

**\_RO\_Web\_Cert**

Type: Certificate Key (PUB)

Web server certificate (default).



Obtained from FW. If it is different from the version in FW, it is updated.

#### **\_RO\_Web\_CA\_Chain**

Type: CA Chain (PUB)

The certificate string of the authority that signed the Web server certificate. If self-signed, it will be empty.

Retrieved from FW. If it differs from the version in FW, it is updated.

#### **\_RO\_Web\_DH\_Param**

Type: DH Parameters (PUB)

Parameters for the Diffie-Hellman key exchange in the Web server.

Retrieved from FW. If it differs from the version in FW, it is updated.

#### **\_RO\_File\_Distribution\_Key**

Type: UFTP Key (PRI)

Key for authenticating stations in the "File distribution" (UFTP) service.

Obtained from FW. If it differs from the version in FW, it is updated.

### **7.5.3.4. Settings**

This tab displays additional settings needed for Local CA authority and Passphrase complexity rules for Key downloads.

#### **Local authority**

##### **Private key ID**

Private key used for local certification authority.

##### **Certificate ID**

Public certificate used for local certification authority.

##### **Signature algorithm**

Algorithm used for certificate signing. It depends on the Certification Authority key algorithm and may not be used in case CA uses a specific algorithm.

##### **Expiration period (days)**

Expiration period in days. Default 7300.

### **7.5.3.5. Organisation**

Contains organisation identification used for certificate generation.

- Country
- Country code (pre filled automatically, possible to manually set by using "Other" in "Country")
- Organisation
- Department
- Location
- State
- Common name

- E-mail

### 7.5.3.6. Passphrase complexity rules

Passphrase required

If set to “No” users may download keys unencrypted (without password).

#### **Passphrase - Minimal length**

Number {5 – 64}, default = 5

The minimum length of the password.

#### **Passphrase - Minimal number of lower case characters**

Number {0 – 5}, default = 0

The minimum number of lowercase letters (English letters) which are required in the password.

#### **Passphrase - Minimal number of uppercase characters**

Number {0 – 5}, default = 0

The minimum number of uppercase letters (English letters) which are required in the password.

#### **Passphrase - Minimal number of digits**

Number {0 – 5}, default = 0

The minimum number of number characters (0 to 9) which are required in the password.

#### **Passphrase - Minimal number of special characters**

Number {0 – 5}, default = 0

The minimum number of special characters (not English upper or lower cases or numbers) which are required in the password. Non-English letters (like Greek, Russian, Arabic) are counted as special characters.

### 7.5.3.7. Creating Local Certification Authority

To create local CA you need to follow these steps:

1. Generate a new private certificate “Certificate key (PRI)”
2. Generate a new “CA Chain (PUB)” using certificate created in previous step as “Certificate key”
3. Activate Local CA by going to Settings tab and activating Local CA, selecting newly created “Private key ID” (= new private certificate “Certificate key (PRI)”) and “Certificate ID” (= new “CA Chain (PUB)”) )



#### **Note**

Web server private key must use “RSA” or “EC (ECDSA)” algorithms. Other algorithms are not supported by web browsers.

### 7.5.4. Remote authentication

User accounts can be managed centrally with an authentication server. RADIUS client-server protocol is used for remote authentication. RADIUS accounts can be mapped to one of the four user roles. This is either managed by the server itself or by local M!DGE3 settings.

Local accounts are checked first and if the account does not exist, RADIUS accounts will be used. If the RADIUS server is not accessible, users may use the local username/password to “fall back” to local authentication.

Unit time:  
2021-08-06 08:00:40 (UTC+0)

RADIUS authentication

RADIUS server address

RADIUS server authentication key

Users realm

Server response timeout [s]

Server request retries

STATUS

SETTINGS

Interfaces

Routing

Firewall

VPN

Security

Local authentication

RADIUS

Menu SETTINGS > Security > RADIUS allows to set all the main parameters.

#### **RADIUS server address**

IP Address of RADIUS server used for authentication.

#### **RADIUS server authentication key**

Text {0 – 32 characters}

Password to authenticate against the RADIUS server.

#### **User realm**

Text {must contain at least one dot “.”}

Realm allows to shorten the login name - e.g. when the full login name is "tech@noname.eu" and the realm is "noname.eu" the Username filled in the login page is only "tech".

#### **Server response timeout [s]**

Number {1 – 30}, default = 10

Time measured while waiting to the server's response before sending a request retry.

#### **Server request retries**

Number {1 – 7}, default = 3

Number of request retries in case of M!DGE3 did not receive a valid reply.

Additional expert parameters shall be set in the ADVANCED menu.

Unit time:  
2021-08-06 08:09:11 (UTC+0)

Search here

- ▶ Interfaces
- ▶ Routing
- ▶ Firewall
- ▶ VPN
- ▼ Security
  - ▶ RADIUS
  - ▶ Device
  - ▶ Generic

### RADIUS

RADIUS authentication: On

Web inactivity timeout [min]: 1440

RADIUS server address: 192.168.199.7

Users realm: noname.eu

Server response timeout [s]: 10

Server request retries: 3

Access level source: From server

Static access level: guest

'Guest' role access level - from: 0

'Guest' role access level - to: 99

'Technician' role access level - from: 100

'Technician' role access level - to: 199

'Security technician' role access level - from: 200

'Security technician' role access level - to: 299

'Administrator' role access level - from: 300

'Administrator' role access level - to: 399

The level of access is realised by Management-Privilege-Level (RFC 5607, index 136, type integer). The level for each account shall be set during the server configuration. The user access level will be granted according to the integer ranges for individual role levels. When the server does not allow setting of Management-Privilege-Level the static account level option (for all users) has to be used.

### 7.5.5. Tamper reset

Tamper is a detection service, which is triggered, when the MIDGE3 chassis is physically opened. There are 2 contacts (securing top and bottom casing) and the event is triggered even if the unit is without power. When the chassis is opened an alarm is triggered and shown in Status report. Triggered Tamper stops the RTC (real time clock) which means, that every unit reboot resets the unit timer back to the time, when the Tamper was triggered.

The screenshot shows the M!DGE3 STATUS page. The top navigation bar includes 'STATUS', 'Changes', 'Notifications', and a user icon. The main content area displays the status of various components: Device (green checkmark), USB (green checkmark), Security (red shield with a star and a red 'X' icon, with a 'Tamper open' link below it), Ethernet 1 (green checkmark), Ethernet 2 (green checkmark), Ethernet 3 (green checkmark), and Ethernet 4 (green checkmark). A sidebar on the left contains links for STATUS, SETTINGS, DIAGNOSTICS, and ADVANCED. At the bottom, an 'Alarms in last 7 days' section shows a red alert box: 'Tamper open detected', Count: 1x, Active from: 2022-08-26 14:22:53.

To solve Tamper alarm, re-assemble the unit, via admin user account see SETTINGS/Security/Tamper reset in the menu and click the "Reset tamper" button.

The screenshot shows the M!DGE3 TAMPER RESET page. The top navigation bar includes 'TAMPER RESET', 'Changes', 'Notifications', and a user icon. The main content area features a blue information box: 'Tamper alarm can be reset after the unit has been assembled again. Please note it will require unit reboot.' Below this is a red 'Reset tamper' button. The left sidebar is expanded to show the 'Security' section, with 'Tamper reset' selected. The unit time is 2022-08-26 14:32:26 (UTC+2).

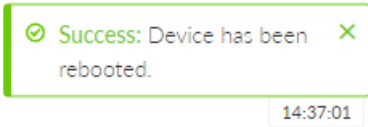


### Note

The unit must be re-assembled before clicking the "Reset tamper" button, otherwise it returns an error.

The error message box is red with a white border and contains the text: 'Error: Tamper reset blocked, lid not closed yet.' with a red 'X' icon in the top right corner. A timestamp '14:34:30' is visible at the bottom.

Whole process can take a while and ends by rebooting the unit.



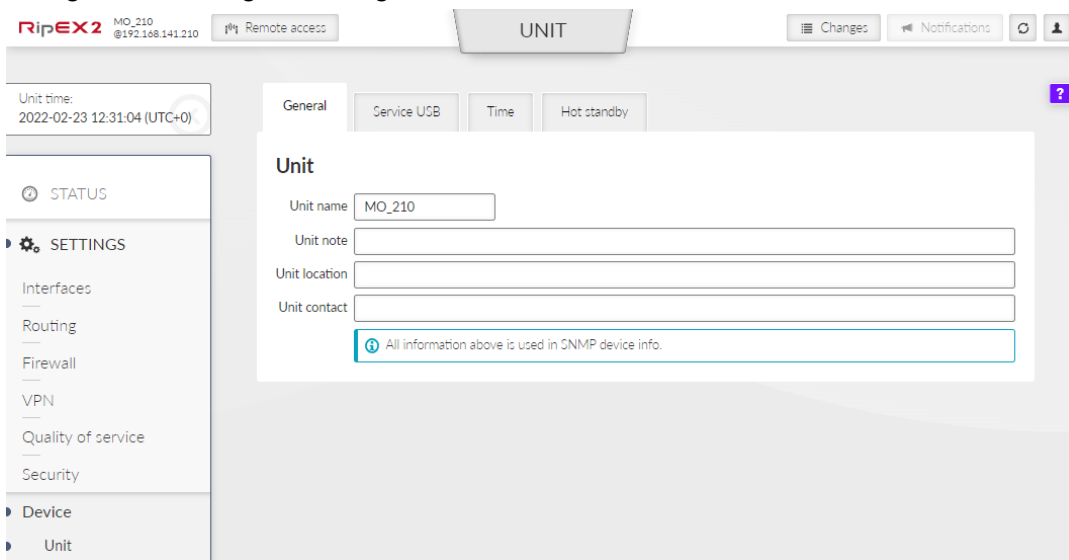
If an automatic time synchronization is not set, the time in the RTC needs to be set manually.

## 7.6. Device

### 7.6.1. Unit

#### 7.6.1.1. General

The general settings affecting the whole unit.



#### Unit name

This name is used as a real name of the Linux router, so the allowed characters are strictly limited to:

Text; default = `_a..zA..Z0..9`

#### Unit note

Text; default = `_a..zA..Z0..9`

Longer unit name without special characters restrictions.

#### Unit location, Unit contact

Text; default = `_a..zA..Z0..9`

Additional SNMP information. All the fields above are typically used in the NMS systems to identify the specific unit.

#### 7.6.1.2. Service USB

The USB service interface primary purpose is to provide unit service and management access. Ethernet or WiFi connection can be established using an external ETH/USB or WiFi adapter.

Please note that only adapters listed in

[https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories\\_ethusb](https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb) can be used.

The screenshot shows the 'Service USB' configuration page. The left sidebar has 'STATUS', 'SETTINGS', and 'Device' sections. The 'Service USB' tab is selected, showing 'Parameters' and 'WiFi' sections. Under 'Parameters', 'USB/ETH' and 'USB/WiFi' are checked. The IP/Mask is 10.9.8.7/28, DHCP pool start is 10.9.8.8, and DHCP pool end is 10.9.8.12. Under 'WiFi', 'SSID automatically' is 'On', SSID is 'RipEX2 1801619451', Mode is '802.11g', Channel is '1 - 2412 MHz', Security is 'Off', and Password is empty.

The DHCP server is running on this service interface to enable easier connection of the management device (PC, tablet or smart phone).

### Enable / Disable

Each of the ETH or WiFi service can be enabled or disabled separately. When the WiFi is enabled, the unit acts as a WiFi Access Point (AP).

### IP address / Mask

IP address, default = 0.0.0.0/0

IP address of the DHCP server. This is the IP address to be used when accessing the unit management via this serial interface.

### DHCP pool start

Default = IP address of the DHCP server + 1

DHCP Server assigns addresses to connected clients starting from this address.

### DHCP pool end

DHCP server assigns IP addresses to connected clients in the range defined by **DHCP pool start** and **DHCP pool end** (inclusive).

### WiFi

WiFi AP parameters can be customized.

### **SSID automatically**

List box {On; Off}, default = "On"

When automatic definition of SSID is enabled, the SSID contains unit Serial number.

### **SSID**

WiFi AP SSID. When entered manually, it must follow SSID naming conventions.

### **Mode**

List box {802.11g; 802.11g }, default = "802.11g "

WiFi AP mode.

### **Channel**

Selected WiFi channel.

### **Security**

List box {Off; WPA2-PSK}, default = "Off"

It is a good practice to use WPA2-PSK secured connection together with a strong password. It is highly recommended in case of permanent WiFi adapter installation.

### **7.6.1.3. Time**

Unit Event time stamps, unit Statistics records and unit internal logs are using Unit time. It is good practice to keep the Unit time synchronized to ease unit and network diagnostics.

Unit time can be setup manually or it can be synchronized with an NTP server. NTP server synchronization is recommended.

The unit itself serves as an NTP server providing the time synchronization to another IP clients. If no NTP server is defined or no one is available, the unit runs in an "orphan" mode. The unit internal NTP server Stratum is set to 8 in this case. If the unit is synchronized with an NTP server, the unit NTP server Stratum is set a 1 higher comparing to Stratum of the NTP server providing the time synchronization to the unit.

If the unit is synchronized to a time source and the unit (synchronized) time differs from the unit RTC time (by more than 8 seconds), the RTC time is updated.



#### **Note**

Each unit can serve as NTP server for further IP equipment, this functionality is always on.



**Status** Last refresh: 2023-05-26 11:18:36

3 seconds

NTP state: synced to GNSS  
 Stratum: 1  
 Delay [ms]: 0.000  
 Dispersion [ms]: 225.501

**Time**

Change device time manually: 2023-05-26 11:21:04   Use browser time

GNSS synchronization: On  
 NTP minimum polling int: 1 min.  
 Time zone: Europe/Prague

GNSS synchronisation has priority over other NTP sources

**NTP servers**

| IP              | Note |
|-----------------|------|
| 192.168.141.211 |      |

Fig. 7.4: SETTINGS > Device > Unit > Time

## Status

The Status field provides information about NTP synchronization status. Refresh button is used to update the Status information.

### 7.6.1.3.1. Time

#### Change device time manually

This field is used to setup unit time manually.

#### Update in device

Sets the given time to the unit.

#### Use browser time checkbox

Continuously updates the Change device time manually field to minimize the delay between the time input and the moment of time setup.

#### NTP client synchronization source

Synchronization source of the NTP client. The only option “NTP server” is implemented at this firmware version.

#### GNSS synchronization

List box {On; Off }, default = "Off"

Enables / disables synchronization with the GNSS (GPS) (when optional GNSS module is used). GNSS (GPS) synchronisation has priority over other NTP sources. This parameter occurs only if GNSS (GPS) is enabled in *Section 7.6.1.5, “GNSS (GPS)”*.

#### NTP server minimum polling time

Minimal period of the NTP server queries. NTP client is allowed to prolong this time in case of poor quality of the server or connection to the server.

#### Time zone

Time zone to represent unit internal time. All the unit timestamps are displayed using this time zone. Changing the time zone does not affect unit internal records – they are always recorded using UTC time zone.

NTP status information is based on standard ntpq daemon status output (ntpq -c lpeers, ntpq -c rv) - see <https://docs.ntpsec.org/latest/ntpq.html> (system, peer and clock variables) for details.

### 7.6.1.3.2. NTP servers

Multiple NTP servers can be configured to get more precise time synchronization or to have a backup solution in case of an individual NTP server unavailability. Maximum number of records in the list is 32. The unit runs in an “orphan” mode if the **NTP client synchronization source** is set to “NTP server” and there is no NTP server defined in this list.

- Enable / Disable            Enables / Disables a NTP server.
- NTP server IP             Defines the IP address of the NTP server.
- Note                        Informational comment.

### 7.6.1.4. Sleep mode

M!DGE3 offers a mode which periodically switches between the full traffic mode and low power consumption mode. This mode is suitable e.g. for power-consumption sensitive applications. When in Sleep mode, M!DGE3 has extremely low power consumption (10 mW). The time needed for a complete wake-up from the Sleep mode (booting time) is approx. 30 seconds or more - depending on the configuration. Sleeping unit indicates its state by green flashing SYS LED.

Sleep mode **Enabled**

---

#### Wake-up parameters

Wake from [h]

Wake from [min]

Waking period [min]

Wake until [h]

Wake until [min]

#### Go to sleep parameters

Go to sleep interval [min]

Reset interval  ▼

Reset on Radio/MAIN activity  ▼

Reset on EXT activity  ▼

Fig. 7.5: SETTINGS > Device > Unit > Sleep mode

### Sleep mode

Enable / disable, default = disable

Enables / disables Sleep mode. When enabled, the unit will periodically go into Sleep mode depending on conditions defined by the following configuration.

#### 7.6.1.4.1. Wake-up parameters

Waking up the M!DGE3 from Sleep mode is possible via setting the time of its awakening. It is also possible to set an interval during which the unit will be woken up regularly. Sleep mode time boundaries are counted in a set **Time zone** (SETTINGS > Device > Unit > Time).

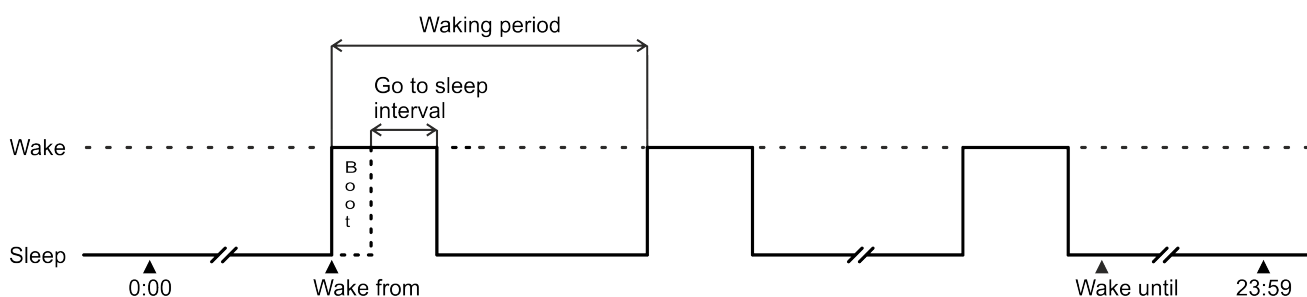


Fig. 7.6: Sleep mode scheme

#### Wake from [h]

Number {0 – 23}, default = 0

Defines the first wake-up time in a day - hour.

#### Wake from [min]

Number {0 – 59}, default = 0

Defines the first wake-up time in a day - minute.

#### Waking period [min]

Number {0 – 1439}, default = 60

Defines the length of time period (min) between individual wake-ups.

#### Wake until [h]

Number {0 – 24}, default = 23

Defines the time in a day after which the unit will not be awoken - hour.

#### Wake until [min]

Number {0 – 59}, default = 59

Defines the time in a day after which the unit will not be awoken - minute.

#### Note

Set time from parameters **Wake from [h]** and **Wake from [min]** must be smaller or equal to set time from parameters **Wake until [h]** and **Wake until [min]**.

#### 7.6.1.4.2. Go to sleep parameters

M!DGE3 will go into the Sleep mode after the set time passes. It is possible to delay the Sleep mode to assure that all data transfer is complete. Connecting USB-ETH or USB-WIFI adapters to the service port will also delay the Sleep mode. Falling into the Sleep mode will generate an event to the Event log.

#### Note

If the M!DGE3 is in the Sleep mode and a power outage occurs (for approx. 10s), the Sleep mode will be interrupted and the unit will wake up (boot).

#### Go to sleep interval [min]

Number {5 – 1439}, default = 15

Defines the length of time (min) after which the unit will go into Sleep mode. The countdown starts, when the unit is completely awake.

### Reset interval

List box {On; Off }, default = "Off"

Allows to set conditions causing the unit to delay transition into Sleep mode by resetting the count down timer back to the initial value **Go to sleep interval [min]**.

### Reset on Radio/MAIN activity

List box {On; Off }, default = "On"

If the unit shows activity on the Cellular-MAIN interface, the count down timer is reset back to the initial value **Go to sleep interval [min]**.



#### Note

ICMP ping on Cellular-MAIN interface will not trigger the **Reset on Radio/MAIN activity**.

### Reset on EXT activity

List box {On; Off }, default = "On"

If the unit shows activity on the Cellular-EXT interface, the count down timer is reset back to the initial value **Go to sleep interval [min]**.



#### Note

ICMP ping on Cellular-EXT interface will not trigger the **Reset on Radio/EXT activity**.

### Example 1:

With following settings M!DGE3 will be periodically woken up every hour for 10 minutes (all day long):

**Wake from [h] = 0**

**Wake from [min] = 0**

**Waking period [min] = 60**

**Wake until [h] = 23**

**Wake until [min] = 59**

**Go to sleep interval [min] = 10**

**Reset interval = Off**

### Example 2:

With following settings M!DGE3 will be periodically woken up from 7:00 to 16:00 every 30 minutes for 10 minutes:

**Wake from [h] = 7**

**Wake from [min] = 0**

**Waking period [min] = 30**

**Wake until [h] = 16**

**Wake until [min] = 00**

**Go to sleep interval [min] = 10**

**Reset interval = On**

**Reset on Radio/MAIN activity = On** - this parameter will ensure that M!DGE3 stays awake in case of any Cellular activity at the scheduled sleep time.

### 7.6.1.5. GNSS (GPS)

GNSS (Global navigation satellite system) allows the optional extension module to provide information about the units location and enable a precise time synchronization.

#### Enable; Disable, default = "Disable"

Enables / Disables the GNSS (GPS).

To set up GNSS (GPS) see *Section 7.7.3, “GNSS server”*.

**Tab. 7.3: LED behavior of GNSS (GPS)**

| LED | Colour | Status                              | Function   |
|-----|--------|-------------------------------------|--|
| EXT | Green  | Flashing regularly - period 1000 ms | GNSS (GPS) is active, awaiting for data about location and PPS signal. |
| EXT | Green  | Permanently lit                     | GNSS (GPS) is active, data about location and PSS signal is available. |

#### 7.6.1.5.1. Cooperation with other services

- HotStandby - GNNS (GPS) is disconnected in passive mode and activated in active.
- Events - TBD
- SNMP -TBD

#### 7.6.2. Configuration

Configuration in M!DGE3 operates on following system:

- Current configuration - displayed configuration, which is seen in the web client.
- Running configuration - actual configuration, running in the M!DGE3 unit.
- Stored configuration - configuration stored in the M!DGE3 unit. This configuration is stored in the unit, even when its turned off.
- Factory settings - default configuration.
- Changes - all changes done to the Current configuration (in the web client). For more information see *Section 6.2, “Changes to commit”*.

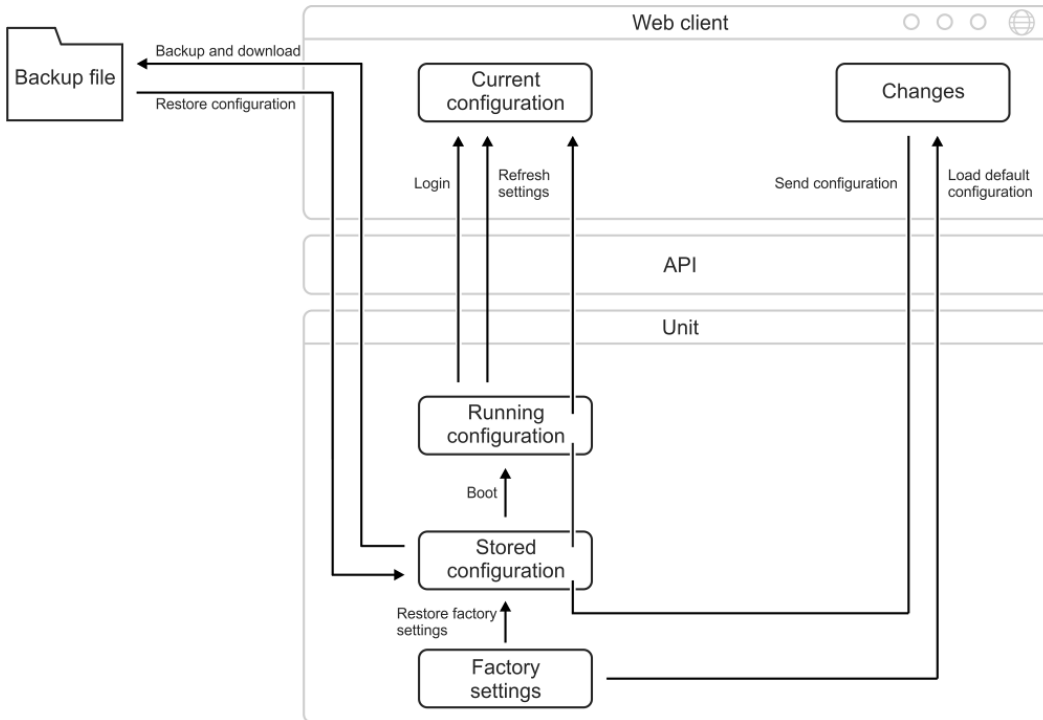
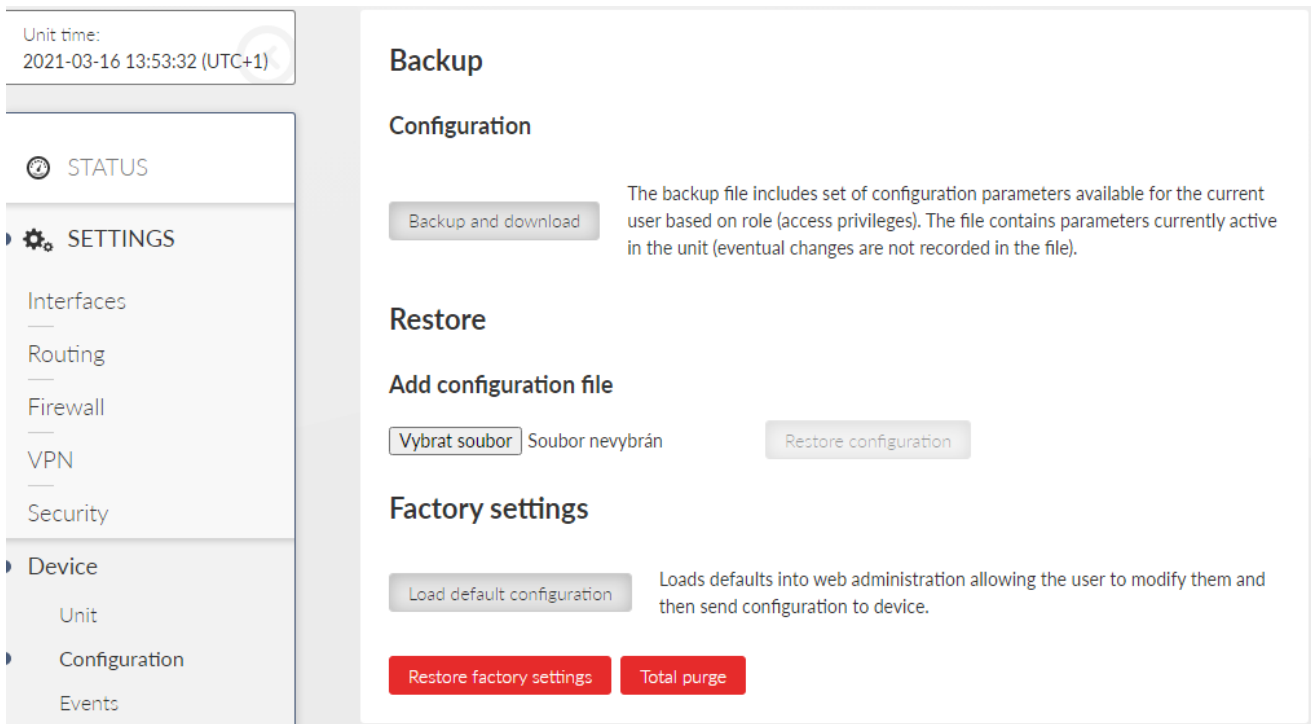


Fig. 7.7: MIDGE3 configuration scheme

There are several tools to operate full unit configuration:



**Backup**

It is a good practice to make a configuration backup into an external file every time the configuration is changed, to be able to restore the configuration into another unit in case of unit maintenance.

**Backup and download** button triggers the web browser Download action. The specific behavior depends on your web browser personal settings - whether the configuration backup file is downloaded

to a predefined download folder or the file Download dialog to select destination folder is shown. The configuration is stored in a text file (.json file type).

The backup configuration has following limitations:

- The set of configuration data is limited by a user access privileges of the user who performed the backup. The full configuration backup can only be issued by a user with the Administrator (role\_admin) access privileges. The same user access limit applies when the configuration is restored (i.e. the full configuration Restore can only be issued by a user with the Administrator (role\_admin) access privileges).

Configuration version is stored in the parameter called "CNF version" which can be checked in the menu: DIAGNOSTICS > Information > Device > Advanced information.

## Restore

The configuration can be restored from a backup file (containing the same configuration version as the configuration version currently running in the unit - see above).

### Choose File Button

Triggers the file selection dialog. Once the configuration backup file is selected, it is uploaded to the unit. The upload action can take some time - depends on the speed of your service connection to the unit.

### Factory settings

**Load default configuration** button loads default values of all configuration parameters into the web interface. All parameters whose current value differs from the default are marked as changed. They are listed in the Changes to commit dialog. They do not affect the running unit until eventually sent to the unit by the Send configuration button.

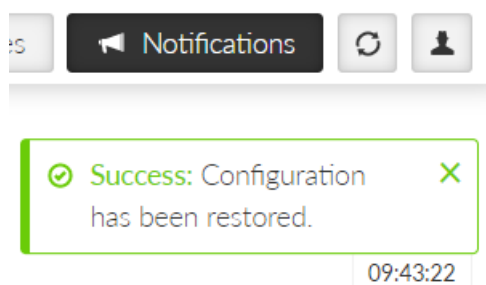


#### Note

This action can be used (for example) to check which set of parameters differs from the default value.

### Restore configuration button

Enabled after the backup configuration is uploaded. Press the button to restore the unit configuration. The configuration restore result is reported as an error message (in case of failure) or Notification center success message:



### Restore factory settings

Restores all configuration parameters to default setup (including monitoring settings). Logout from station will apply.

Deletes user database (only default user "admin" with default password will remain).

### Total purge

Restores all configuration parameters to default setup (including monitoring settings). Logout from station will apply.

Deletes user database (only default user "admin" with default password will remain).

Deletes all diagnostic logs and statistics.



**Note**

Basic data such as Code, Region, SW keys will always remain in the unit.



**Warning**

This action can take up to two minutes - do not power off the unit until finished.

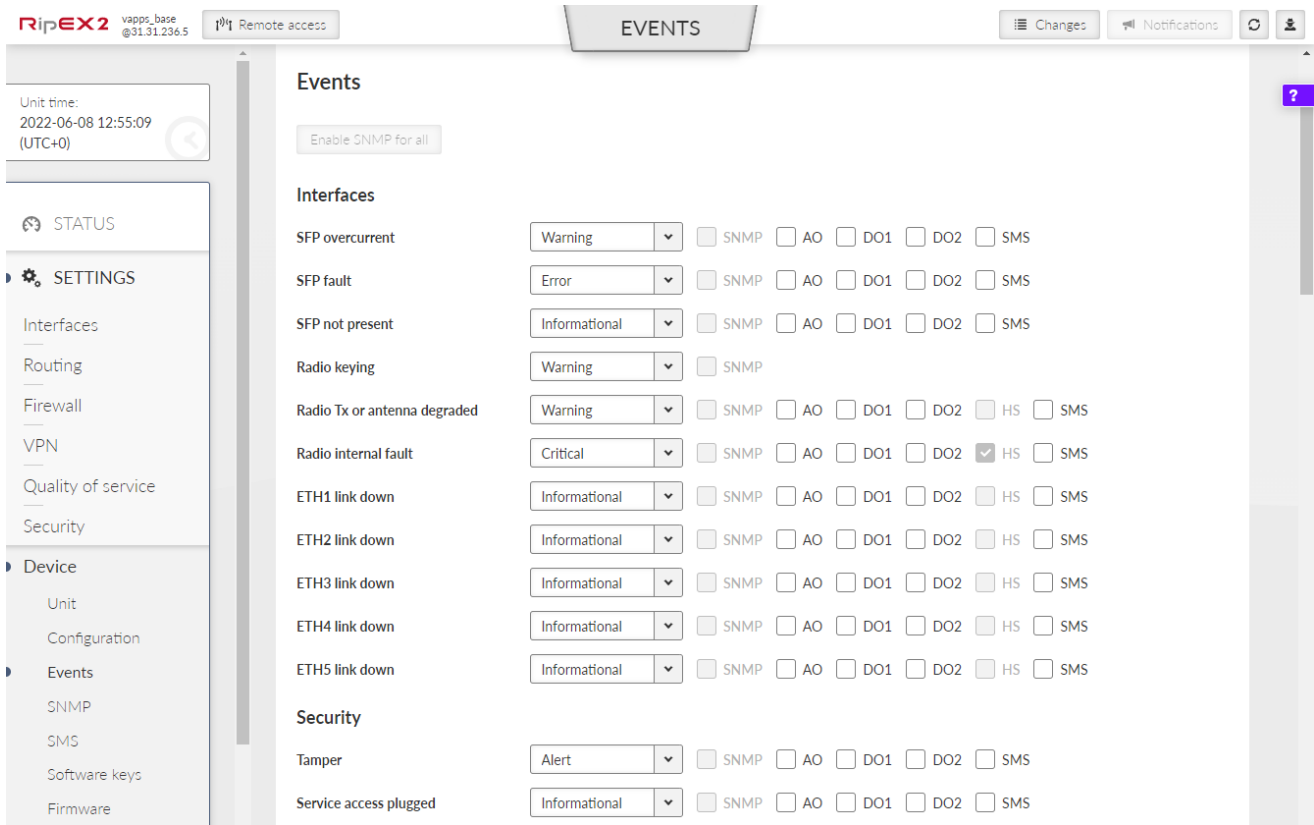


**Tab. 7.4: Configuration versions**

| <b>CNF version</b> | <b>FW version</b> |
|--------------------|-------------------|
| 18                 | 2.0.18.0          |
| 17                 | 2.0.16.0          |
| 16                 | 2.0.14.0          |
| 15                 | 2.0.13.0          |

### 7.6.3. Events

Settings of the severities of the individual events. Some events can generate SNMP notification and can change level of the HW alarm outputs (AO, DO1, DO2) see *Section 2.2.2, “Power and Control”*. Events can also generate SMS notifications, which are being sent to a defined phone number (see *Section 7.7.2, “SMS”*).



### 7.6.4. SW keys

Certain M!DGE3 features needs to be activated by a SW key to be available. When the respective SW key is not present, the feature cannot be configured. If the feature is enabled in a configuration backup file and the file is loaded to a unit which is not equipped with the respective key, the configuration is refused (no changes are made in the unit).

*Here* is the list of available SW keys and their assignment to offered SW key packages.

SW key(s) can be obtained from your supplier. It is delivered as a text file containing the key(s). Every SW key is unique for the specific unit (specific serial number). Use Choose File dialog to select the file and Install key button to install the key(s) to unit.

The screenshot displays the 'Settings' page for a RipEX device. At the top left, the 'Unit time' is shown as '2021-03-16 12:04:36 (UTC+0)'. A left-hand navigation menu includes 'STATUS', 'SETTINGS', 'Interfaces', 'Routing', 'Firewall', 'VPN', 'Security', 'Device', and 'Software keys'. The 'Software keys' section is active, showing 'Installed SW keys' with a 'Master' key listed. Below this, the 'Install new keys' section features a file selection button labeled 'Vybrat soubor', a text input field containing 'Soubor nevybrán', and an 'Install key' button. A note states 'Keys can be obtained from your supplier.'

Differences with the previous generation of RipEX:

- SW keys are always installed as a file (there is not a clipboard option)
- Single file can contain multiple SW keys
- SW keys are not time limited

**Tab. 7.5: List of atomic SW keys**

| Atomic key | Shortcut | SW key |
|------------|----------|--------|
| SFP        | SFP      | SFP    |

### 7.6.5. Firmware

#### 7.6.5.1. Local

Unit firmware defines the unit functionality. There are several principles for managing the firmware in the running network:

- Maintain the same version of firmware in the network (recommended). RipEX units are able to co-operate with different versions of firmware running, but using the same firmware version in all units is the best way to keep the network maintenance simple.
- Upgrading firmware to a newer version is not obligatory, unless there are bug/security fixes etc.
- The cyber security issues may force the firmware to be upgraded e.g. when some serious security vulnerability was fixed.

There are 3 stages of the firmware upgrade procedure:

- Choosing new firmware and loading it into the web browser.
- Uploading new firmware into the unit's internal archive.
- Activating the unit firmware.

Every operation can take up to several tens of seconds.

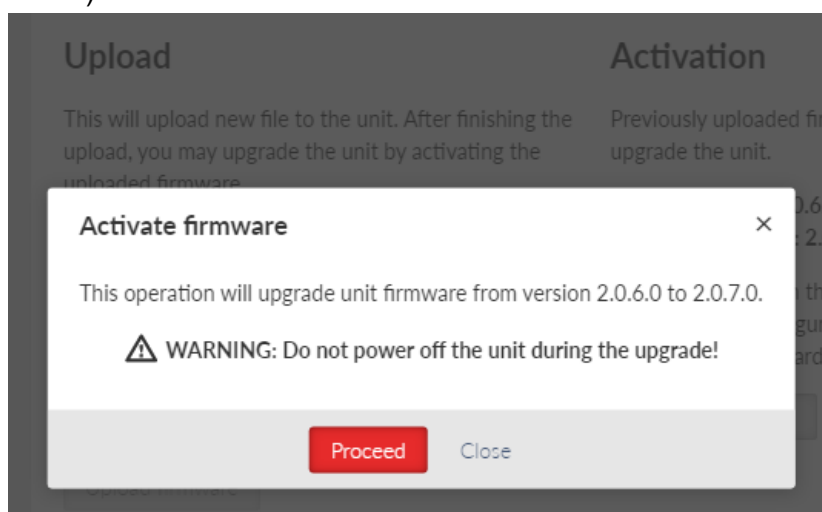


**Note**

Unit configuration backup is recommended after the firmware upgrade. See *Section 7.6.2, "Configuration"* for details.

To upgrade the firmware:

1. Optional (recommended): Backup the current unit configuration (menu SETTINGS > Device > Configuration – Backup and download).
2. Download the required firmware from the *Racom web*<sup>4</sup>: Products – MIDGE3 – Download – Firmware MIDGE3 – midge3-fw-x.x.x.0.fwp
3. Click the **Choose File** button (the button label may differ based on your web browser localization) to select the firmware file.
4. Click the **Upload firmware** button to transfer the firmware file into the unit. The upload can take a long time – depending on the connection speed between the management PC and the MIDGE3 unit. In case of slow connection and file transfer longer than 120 s, the web browser will shut down the connection and the action will not finish successfully. This action does not update the running unit firmware yet. There is no affection on the other communication running through this unit. Successful uploading of the new firmware into the archive is announced in the Notifications and the available firmware version is highlighted under the "Activation" heading as "**Uploaded firmware:**".
5. Click the **Activate firmware** button to upgrade (i.e. reinstall) the unit firmware. The upgrade process takes approx. one minute. The user data communication running through this unit is interrupted for a while. All the processes are restarted in a certain moment (e.g. VPN tunnels need to be re-established).



### Warning

Do not shut down the unit during the firmware update process. It may permanently damage the unit.

6. It is possible not only to upgrade the firmware version, but to even downgrade it, although this operation is not recommended. Be aware of eventual security issues of firmware downgrade as eventually outdated security code can be part of an old firmware. After FW downgrade, all unit parameters will be set to factory defaults.

<sup>4</sup> [https://www.racom.eu/eng/products/cellular-router-midge.html#dnl\\_fwr3](https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3)



**Note**

Direct firmware upgrade from version 2.0.3.0 (or lower) to version 2.0.13.0 (or higher) is not possible. You have to upgrade the firmware to any version from 2.0.5.0. to 2.0.10.0 prior to upgrading to 2.0.13.0 (or higher).

**7.6.5.1.1. Patch files**

In some cases, instead of uploading and activating full FW version, patch files can be used. Advantage of the patch files is that they are smaller comparing to the full version files. For successful activation a compatibility between the patch file and active firmware (or uploaded firmware) must be ensured. Patch files for M!DGE3 can be downloaded from *RACOM's web site*<sup>5</sup>. FW versions stored in M!DGE3 are displayed in SETTINGS > Device > Firmware.

---

<sup>5</sup> [https://www.racom.eu/eng/products/cellular-router-midge.html#dnl\\_fwr3](https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3)

## Upload

This will upload new file to the unit. After finishing the upload, you may upgrade the unit by activating the uploaded firmware.

Other than full firmware files, you may also upload patch files over versions:

- 2.0.10.0
- 2.0.8.0

No file selected.

Accepted file type: .fwp

**Example:** There are 2 older FW versions (2.0.8.0 and 2.0.10.0) stored in M!DGE3 (picture above). For successful activation of newer FW version (e.g. 2.0.13.0) either:



### Note

FW versions (both patch files and full versions) are stored in *M!DGE3 archive*<sup>6</sup>.

## 7.7. Services

### 7.7.1. SNMP

SNMP (Simple Network Management Protocol) implementation in M!DGE3 provides three SNMP versions: v1, v2c and v3.

<sup>6</sup> [https://www.racom.eu/eng/products/cellular-router-midge.html#dnl\\_archive](https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_archive)



## Note

Following characters are prohibited in SNMP communication:  
" (Double quote) ` (Grave accent) \ (Backslash) \$ (Dollar symbol) ; (Semicolon)

## SNMP mode

List box {Off; v1\_v2c\_v3; v3}, default = "Off"  
Enables the SNMP and defines which protocol versions are available.

## Community name

String {1–32 char}, default = "public"  
Community name used by v1 and v2c. When mode v1\_v2c\_v3 is used, this parameter is mandatory.

## Version 3 settings

### Security username

String {1–32 char}, default = <empty>  
Username for SNMPv3. When v3 protocol is selected, this parameter is mandatory.

### Security level

List box {NoAuthNoPriv; AuthNoPriv; AuthPriv}, default = "NoAuthNoPriv"  
The v3 protocol security level. Switches on/off Authentication (Auth) and the SNMP data encryption (Priv).



**Authentication**

List box {MD5\_legacy; SHA1\_legacy; SHA224; SHA256; SHA384; SHA512}, default = "SHA256"  
Authentication algorithm. Legacy algorithms are not recommended to use, they are available for compatibility reasons only.

**Authentication passphrase**

String {8–128 char}, default = <empty>  
Passphrase used for authentication with SNMP server.

**Encryption**

List box {DES\_legacy; AES128; AES192; AES256}, default = "AES128"  
Encryption algorithm.

**Encryption passphrase**

String {8–128 char}  
Passphrase used for data encryption when communicating with SNMP server.

**Engine ID mode**

List box {Default; User defined}, default = "Default"  
Engine ID serves for unique identification of the SNMP instance (i.e. the MIDGE3 unit) according to RFC3411. When the "Default" Engine ID mode is selected the MAC address of the ETH1 interface is used for the unique part of the Engine ID (the whole Engine ID example: 800083130302a92006ef).

**Engine ID**

String {1–27 char}  
When "User defined" Engine ID mode is selected the differentiated part of the Engine ID can be entered as ASCII characters or generated (e.g. U3qPrisWoDYbBVNsAWluZYGL3M5). This string is converted into HEX number (i.e. 55 33 71 50 72 69 73 57 6f 44 59 62 42 56 4e 73 41 57 6c 75 5a 59 47 4c 33 4d 35). The whole Engine ID for mentioned example: 800083130455337150726973576f44596242564e7341576c755a59474c334d35.

**Notification**

Notification is used for asynchronous notification from a MIDGE3 unit into the SNMP server.

**Notification mode**

List box {Off; Trap; Inform}, default = "Off"  
Mode of notification; Inform is not supported by SNMPv1.

**Notification version**

List box {v1; v2c; v3}, default = "v2c"  
Notification packets version.

**Inform repeats**

Number {0 – 10}, default = 3  
Number of repeats used when Inform acknowledge was not received.

**Inform timeout [s]**

Number {1 – 20}, default = 10  
Inform acknowledge timeout.

**Notification destinations****Destination IP**

IP address, default = 0.0.0.0

IP address of SNMP server receiving notification packets.

**Destination port**

Number {1 – 65535}, default = 162

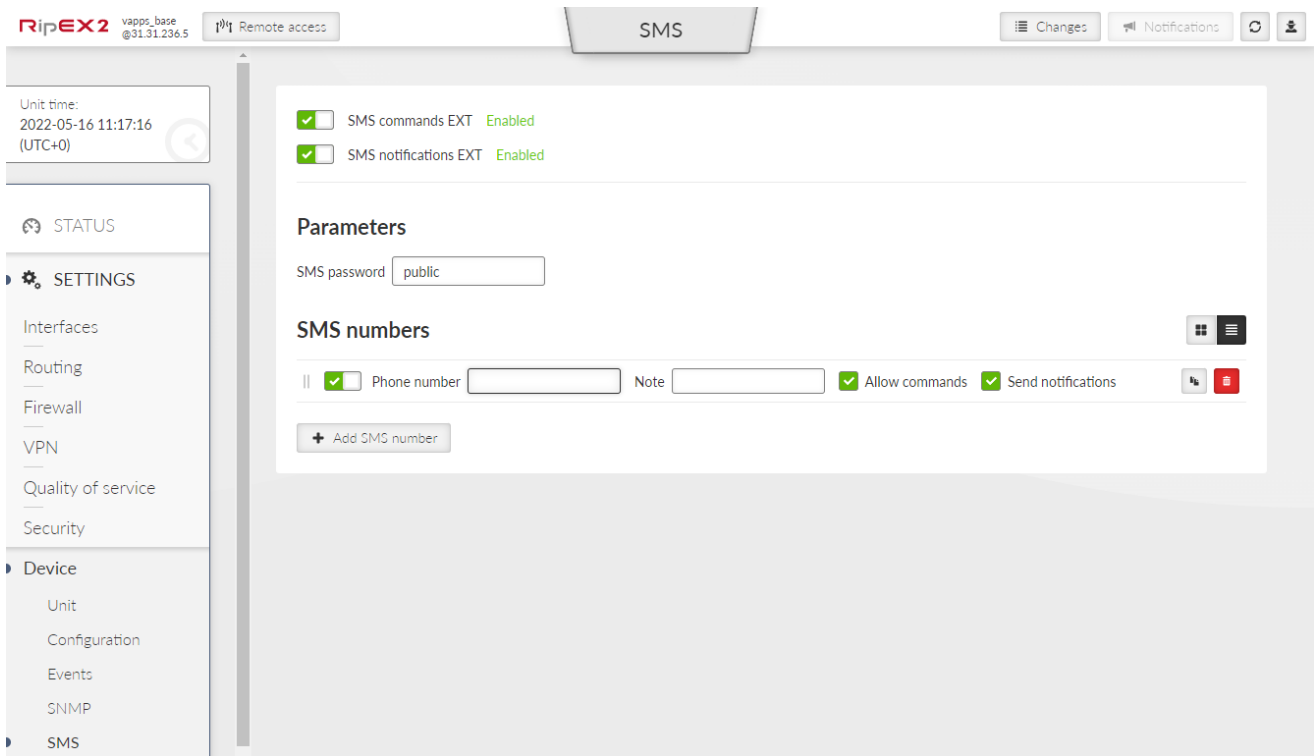
Notification packets destination port.

For more detailed information, please see *SNMP application note*<sup>7</sup>.

**7.7.2. SMS**

M!DGE3, fully connected into the cellular network (status CONNECTED), is capable of receiving and sending SMS.

- Receiving and sending SMS is provided by a linux service.
- The queue of SMS waiting for sending is controlled by appropriate diagnostic linux service.
- The length of the SMS depends on the type of module and coding. If longer SMS is required (only **SMS notifications**), it is divided into a Chained SMS.



**Note**

This section closely cooperates with *Section 7.1.4, "Cellular"*.

**SMS commands MAIN/EXT**

{Enable; Disable}, default = "Disable"

Enables / Disables SMS commands for Cellular MAIN/EXT. When enabled, the software module allows all incoming SMS and proceeds to initiate commands.

<sup>7</sup> <https://www.racom.eu/eng/products/m/ripex/app/snmp-ripex2/index.html>

- To process an SMS command from a phone number:
  - The specific phone number must be defined in parameter **SMS numbers**. If the phone number is not defined, the SMS will be not processed.
  - The SMS must contain a password to pass the authentication (parameter **SMS password**).
  - The SMS must contain a valid *format of a command*.
- Only regular SMS are supported (Chained SMS are not).
- Some commands generate an automatic reply, which is sent to a defined phone number(s), if this feature is enabled.
- If this parameter is disabled, all incoming SMS will be deleted.

### SMS notifications MAIN/EXT

{Enable; Disable}, default = "Disable"

Enables / Disables SMS commands for Cellular MAIN/EXT.

When enabled, any change (if configured in *Section 7.6.3, "Events"*) will generate a notification SMS, which will be sent to all defined phone numbers with active notification.

- To send an SMS notification to a phone number:
  - The specific phone number must be defined in parameter **SMS numbers**. If the phone number is not defined, it will not receive any notification.
- Chained SMS are supported.
- Sending SMS notifications can be activated in *Section 7.6.3, "Events"*.

#### 7.7.2.1. Parameters

##### SMS password

String {2–16 ASCII char}, default = "public"

Sets an SMS password, which serves as an authentication to send SMS from defined phone number(s). The range of length of the password is between 2–16 characters. SMS password must not contain any unsupported characters. Unsupported characters are: ", ` , \, \$, ;.

#### 7.7.2.2. SMS numbers

##### Phone number

{Enable; Disable}, default = "Enable"

Enables / Disables phone number. When enabled, defined phone number can either send or receive (or both) SMS. Amount of phone numbers, which can receive and send SMS is limited to 10.

##### Note

Optional comment.

##### Allow commands

{On; Off}, default = "On"

Allows to accept commands from defined phone number.

**Note**

This parameter will work only if parameter SMS commands MAIN/EXT is enabled.

**Send notifications**

{On; Off}, default = "On"

Allows to send notifications to defined phone number.

**Note**

This parameter will work only if parameter SMS notifications MAIN/EXT is enabled.

**7.7.2.3. SMS commands**

All commands must match following format:

<password>"space"<command>"space"[<param1>...]

SMS commands:

**cellstatus****Example: public cellstatus**

Request for SMS with extract of Cellular status of the module, which received the SMS.

**Reply of command "cellstatus":**

Station: <station\_name>

<module\_type> <SIM> Profile <profile\_id>

Status: <connection\_state>

Reg: <registration\_state>

Net: <PLMN>

Svc: <service\_type>

Band: <band>

Signal: <signal\_strength>

APN: <username\_APN>

IP: <assigned\_IP>

**Example of reply for command "cellstatus":**

Station: Alef

EXT SIM2 Profile 1

Status: CONNECTED

Reg: RegHome

Net: 23002

Svc: 2G\_EDGE

Band: ARFCN 77

Signal: RSSI: >=-48 dBm

APN: internet

IP: 100.110.103.173

**smsevent <param>****Example: public smsevent raise**

This command is used to turn on/off alarms which can be set in *Section 7.6.3, "Events"* by using its parameters ("raise", "clear").

This command does not generate an automatic reply.

### 7.7.3. GNSS server

GNSS server collects data from a GNSS (GPS) receiver and provides the data to potentially multiple client applications in a server-client application architecture. Internally is used by the NTP.

#### Enable GNSS

List box {On; Off}, default = Off

Enables / disables GNSS subsystem. This parameter occurs only, if GNSS module is available in the unit.

#### Enable GNSS server - Advanced menu

List box {On; Off}, default = Off

Enables / disables GNSS server. This parameter can be set only, if parameter **Enable GNSS server** is set to "On".

#### GNSS server port

Number {1 – 65535}, default = 2947

Sets a TCP port number of the GNSS server. This parameter can be set only, if parameters **Enable GNSS server** and **GNSS server port** are set to "On".

#### Maximal GNSS downtime [min]

Number {1 – 65535}, default = 15

Sets a timer which counts for how long the unit does not need new data about location (when GNSS active). If the time runs out, security actions are triggered (linux service restart, module restart). This parameter can be set only, if parameter **Enable GNSS server** is set to "On".

## 7.8. Advanced

M!DGE3 introduces new concept for expert settings and rapid deployment of new features called "Advanced" section. Advanced section displays all configuration set points currently present in the device automatically, without need to design a special configuration page (like the ones in "Settings"). This allows us to deploy new features rapidly with each new firmware and also allows experienced users to fine-tune their M!DGE3.

Please note, that M!DGE3 is a very powerful device and it really shows all parameters in the Advanced section.

When you visit the page for the first time, you will see a search field and below a tree of configuration pages.

Search field looks through all labels and the tree itself and is capable of showing all relevant configuration pages. It features so called "fuzzy" search capable of returning right answers even when there is a typo in search query. Try searching for "Ethernet" or "BGP" to see the feature in action. To use the whole tree again, simply delete search query.

Configuration tree has two parts. For your convenience first few items (Interfaces, Routing, ...) use similar hierarchy to "Settings", but include all advanced settings. The newest features then can be found in the last item called "General", which contains all configuration tables there are in the unit.

By selecting a configuration page (marked with pencil icon) a window is shown on the right side of the screen containing selected configuration page set points. You can change settings and then send them to the device the same way you know from "Settings".

The screenshot displays the 'ADVANCED' settings page for a M!DGE3 router. The top navigation bar includes 'M!DGE3 midge @31.31.236.8', 'Remote access', 'ADVANCED', 'Changes', 'Notifications', and user icons. The left sidebar shows navigation options: STATUS, SETTINGS, DIAGNOSTICS, and ADVANCED. The main content area is titled 'Cellular MAIN' and contains the following settings:

- Cellular MAIN: On
- Masquerade: On
- Allow unit management: On
- Link testing: Off
- Profile switching: Off
- Switching method: On failure to recv
- Connection timeout [min]: 15
- Return to first profile: On
- Time to return to first profile [min]: 480
- Test period [s]: 60
- Repeat period [s]: 10
- Retries [No]: 3
- Reply timeout [s]: 5
- Target address: 0.0.0.0
- Enable second target address: Off
- Second target address: 0.0.0.0
- Test mode: One address succ

Be careful when adjusting settings in Advanced section and review the “Changes” page in detail before sending changes to the device.

## 8. Diagnostics

### 8.1. STATUS overview

Provides information about individual sections of the unit. Each section is linked with an area of Events (see *Section 8.4, “Events”*).

**Alarms in last 7 days** View more

Showing aggregated Emergency, Alert, Critical and Error Events occurring in last 7 days.

**Radio board temperature too high**  
Count: 4x  
Active from: 2023-07-07 14:54:06

**Latest alarms** View more

Showing 25 latest Emergency, Alert, Critical and Error Events.

| Time                | Description                                | Severity | User | Remote |
|---------------------|--|----------|------|--------|
| 2023-07-07 14:54:06 | Radio board temperature too high *40.0°C ▶ | Error    |      |        |

When any non-standard parameter occurs in the unit, one of the notification icons (depends on the settings) will be displayed on the main screen together with a link leading to the parameter. STATUS also shows and describes alarms in last week which are highlighted under icons. Latest 25 Emergency, Alert, Critical and Error Events are displayed at the bottom of the section.

**Tab. 8.1: Unit section icons**

|  |              |
|--|--------------|
|  | Device       |
|  | USB          |
|  | Security     |
|  | Ethernet 1-5 |







#### Note

The number of visible Ethernet icons is depended on the units settings. (SETTINGS > Interfaces > Ethernet > Ports)

To each event an individual severity can be assigned. When multiple Events with different severities are triggered in the same section, the priority goes: Error > Warning > Notice.

**Tab. 8.2: Severity icons**

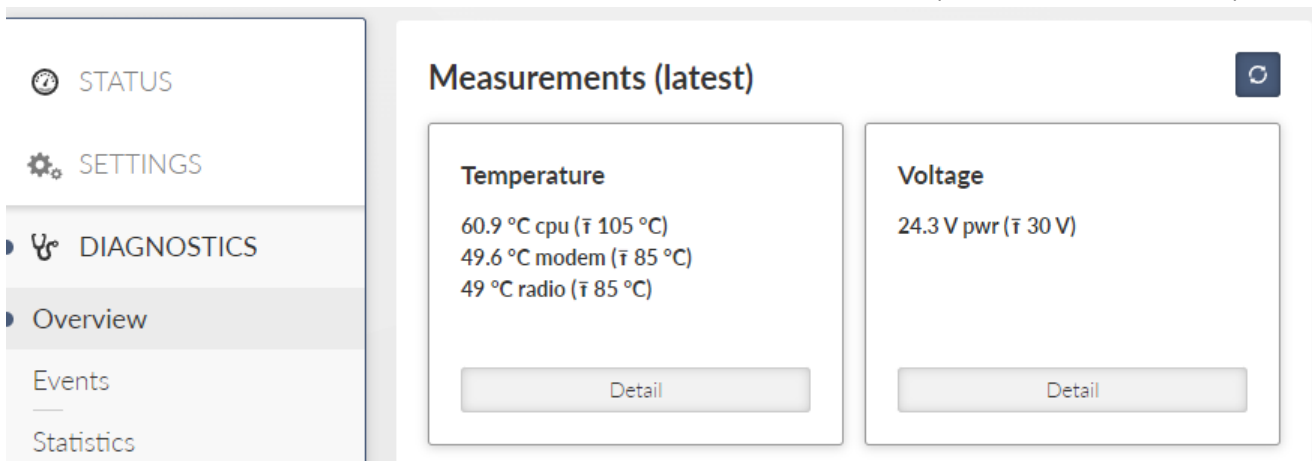
|   |                                   |
|---|-----------------------------------|
|  | Unit works flawlessly             |
|  | Informational, Notice             |
|  | Warning                           |
|  | Error, Critical, Alert, Emergency |

## 8.2. Overview

The Overview section serves to give general information about the M!DGE3.

### 8.2.1. Measurements

Section Overview - Measurements contains current data measurement (obtained from sensors).



- Card Temperature - provides data about temperature (on CPU, modem).
- Card Voltage - provides data about voltage measured on input connector.

Arrow-headed symbols (↑, ↓, →) have following meaning:

- ↑ - Maximum-limit value. An alarm is triggered, when the value (displayed in brackets) is exceeded.
- ↓ - Minimum-limit value. An alarm is triggered, when the value falls under the value, which is displayed in the brackets.
- → - Value is supposed to head to another one.



**Note**

Value measurements are collected once per 10s.

### 8.2.2. Statistics

Section Overview - Statistics shows a short view of the statistics over last 15 minutes (from the time of opening the window or pressing Refresh button).



Unit time:  
2021-03-16 14:54:50 (UTC+1)

**Statistics (15 min)**

**Radio statistics**  
rlp: rx: 0 / tx: 0  
Detail

**COM statistics**  
com1: rx: 0 / tx: 0 / rxdrop: 0  
com2: rx: --- / tx: --- / rxdrop: ---  
com3: rx: --- / tx: --- / rxdrop: ---  
Detail

**TS statistics**  
ts1: rx: 0 / tx: 0 / rxdrop: 0  
ts2: rx: --- / tx: --- / rxdrop: ---  
ts3: rx: --- / tx: --- / rxdrop: ---  
ts4: rx: --- / tx: --- / rxdrop: ---  
ts5: rx: --- / tx: --- / rxdrop: ---  
Detail

**ETH statistics**  
eth1: rx: 619 / tx: 40  
eth2: rx: 0 / tx: 0  
eth3: rx: 0 / tx: 0  
eth4: rx: 0 / tx: 0  
eth5: rx: --- / tx: ---  
Detail

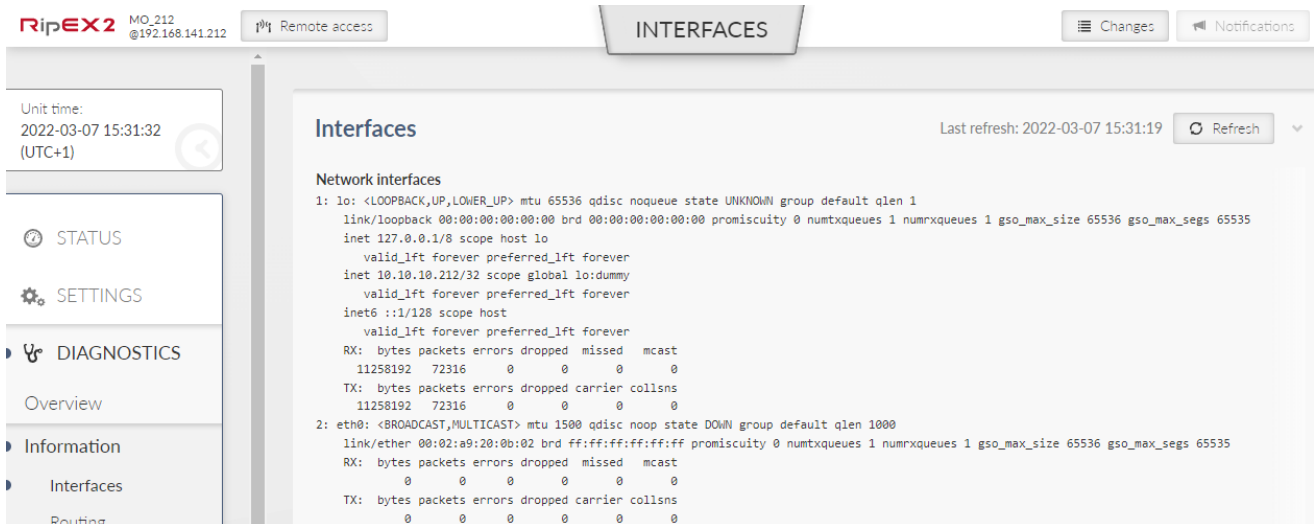
- Cards Statistics are always displayed for all interfaces.
- If the interface is off, its statistics (record) is displayed as “-“.
- Statistics collection is updated every 1 s (each second is possible to see new values).
- 15-min interval is collected by taking 14 mins from history + seconds passed from current minute.

### 8.3. Information

This section provides more detailed information (data extract) about settings of RipEX2 unit. It provides also a deeper explanation about some of set values and interfaces. Diagnostic data are provided as well.

#### 8.3.1. Network Interfaces

Provides a complete information extract about all active interfaces (addresses, details and statistics included). All interfaces used by the linux router (including all internal interfaces like np1, loop, ag, ip6tnl, etc.) are displayed in this section.



Interfaces used in M!DGE3 units are in general either Bridged ports (BP-L2) or Routed interfaces (RI-L3).

All interfaces used by the linux router (internal interfaces excluded) are displayed in the following list.

**if\_<Laniface\_Name>**

LAN bridge interface RI-L3 type  
(SETTINGS > Interfaces > Ethernet > Network interfaces)

**if\_<LanVlan\_IfName>.<LanVlan\_VlanId>**

- VLAN BP-L2 interface type (if used as a port in LAN bridge) (SETTINGS > Interfaces > Ethernet > Network interfaces>VLAN)
- VLAN RI-L3 interface type (if not used as a port in LAN bridge) (SETTINGS > Interfaces > Ethernet > Network interfaces > IP/Subnet > VLAN)

**eth1, eth2, eth3, eth4**

Interface of physical Ethernet ports ETH1 – ETH4, BP-L2 interface type

**eth0**

Interface of physical port SFP (ETH5), BP-L2 interface type

**wwan**

Bridge interface of the Main cellular module, RI-L3 interface type (SETTINGS > Interface > Cellular > MAIN)

**ext**

Bridge interface of the EXT cellular module, , RI-L3 interface type (SETTINGS > Interface > Cellular > EXT)

**gre\_tap<INDEX>**

GRE L2 tunnel interface, BP-L2 interface type (SETTINGS > VPN > GRE > L2)

**gre\_tun<INDEX >**

GRE L3 tunnel interface, RI-L3 interface type (SETTINGS > VPN > GRE > L3)

## lo

Loopback interface RI-L3 type of interface – The IP addresses of the loopback (ADVANCED > Interfaces > Loopback).

### 8.3.2. Routing

Provides information about data extract from section Routing.

The screenshot shows the RiPEX2 web interface. At the top, there's a header with 'RiPEX2' logo, user information 'MQ\_212 @192.168.141.212', and a 'Remote access' button. A 'ROUTING' tab is active. Below the header, there are buttons for 'Changes', 'Notifications', and a refresh icon. The main content area is titled 'System routing' and includes a 'Refresh' button. The 'System routing table' is displayed with the following content:

```

System routing table
default via 192.168.141.254 dev if_bridge proto static
10.10.10.0/24 dev radio proto kernel scope link src 10.10.10.212
192.0.2.232/30 dev ag10 proto kernel scope link src 192.0.2.233
192.168.44.0/24 dev if_LAN-SCADA proto kernel scope link src 192.168.44.1 linkdown
192.168.141.0/24 dev if_bridge proto kernel scope link src 192.168.141.212

```

This section is divided into following parts:

- System - complete data extract of system routing table. Displays data called by linux command “ip route show”.
- Dynamic - complete data extract of internal routing table of dynamic routing service bird master4. Displays data called by linux command “birdcl show route all table master4”.
- Babel - data extract of status of Babel protocol. Displays data called by following linux commands: “birdcl show babel interfaces”, “birdcl show babel neighbors”, “birdcl show babel routes”, “birdcl show babel entries”, “birdcl show route all table babel\_ipv4”.
- OSPF- data extract of status of OSPF protocol. Displays data called by following linux commands: “birdcl show ospf neighbors”, “birdcl show ospf state”, “birdcl show ospf interface”, “birdcl show route all table ospf\_ipv4”.
- BGP - data extract of status of all BGP protocol instances. Displays data called by following linux commands: “birdcl show protocol ""bgp\*"", “birdcl show protocol all ""bgp\*"", “birdcl show route all table bgp\_ipv4”.

### 8.3.3. Firewall

Provides general overview about data extract from sections L2, L3 and NAT.

#### 8.3.3.1. Firewall L2

Displays data called by linux command “iptables -L”.

Unit time: 2022-03-07 15:44:40 (UTC+1)

STATUS

SETTINGS

DIAGNOSTICS

Overview

Information

- Interfaces
- Routing
- Firewall

Remote access

FIREWALL

Changes

Notifications

L2 L3 NAT

L2 Last refresh: 2022-03-07 15:44:38 Refresh

Firewall L2 tables

Bridge table: filter

Bridge chain: INPUT, entries: 0, policy: ACCEPT

Bridge chain: FORWARD, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 0, policy: ACCEPT

### 8.3.3.2. Firewall L3

Displays data called by following linux commands "iptables -nvL --line-numbers".

Unit time: 2022-03-07 15:45:50 (UTC+1)

STATUS

SETTINGS

DIAGNOSTICS

Overview

Information

- Interfaces
- Routing
- Firewall

Remote access

FIREWALL

Changes

Notifications

L2 L3 NAT

L3 Last refresh: 2022-03-07 15:45:50 Refresh

Firewall L3 tables

Chain INPUT (policy ACCEPT 34002 packets, 6185583 bytes)

| num | pkts   | bytes    | target          | prot | opt | in     | out | source    | destination |
|-----|--------|----------|-----------------|------|-----|--------|-----|-----------|-------------|
| 1   | 72379  | 11268132 | ACCEPT          | all  | --  | lo     | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 2   | 173226 | 7571589  | ACCEPT          | all  | --  | ag10   | *   | 0.0.0.0/0 | 192.0.2.233 |
| 3   | 0      | 0        | DROP            | all  | --  | *      | *   | 0.0.0.0/0 | 192.0.2.233 |
| 4   | 0      | 0        | DROP            | tcp  | --  | *      | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 5   | 39003  | 6557053  | input_svcaccess | all  | --  | *      | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 6   | 38776  | 6534025  | infw_macflt     | all  | --  | if_+   | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 7   | 0      | 0        | infw_macflt     | all  | --  | hstdby | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 8   | 39003  | 6557053  | input_ipsec     | all  | --  | *      | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 9   | 0      | 0        | ACCEPT          | icmp | --  | *      | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 10  | 39003  | 6557053  | input_svc       | all  | --  | *      | *   | 0.0.0.0/0 | 0.0.0.0/0   |
| 11  | 227    | 23028    | ACCEPT          | all  | --  | *      | *   | 0.0.0.0/0 | 0.0.0.0/0   |

tcpmss match 1:500

state RELATED,ESTABLISHED

### 8.3.3.3. NAT

Displays data called by following linux commands:

- "iptables -t nat -nvL postrouting\_user" – data about SNAT
- "iptables -t nat -nvL prerouting\_user" – data about DNAT

The screenshot shows the RipEX2 Firewall configuration interface. The left sidebar contains navigation options: STATUS, SETTINGS, DIAGNOSTICS (selected), Overview, Information, Interfaces, Routing, and Firewall. The main content area is titled 'FIREWALL' and shows the 'NAT' configuration page. The page displays statistics for four NAT chains: PREROUTING, INPUT, OUTPUT, and POSTROUTING. Each chain is associated with a policy (ACCEPT) and shows the number of packets and bytes processed. Below the chain statistics, there are tables for NAT rules. The PREROUTING chain has three rules, the INPUT chain has two, the OUTPUT chain has two, and the POSTROUTING chain has four. Each rule specifies a rule number, packet count, bytes, target, protocol, options, input/output interfaces, and source/destination addresses.

### 8.3.4. Quality of service

Creates a table about object and statistics extract for each given interface. This table contains:

- Name of an interface.
- Status and statistics of front disciplines - displays data called by linux command “tc qdisc show”.
- Status and statistics of classes - displays data called by linux command “tc class show”.
- Status and statistics of filter - displays data called by linux command “tc filter show”.

The screenshot shows the RipEX2 Quality of Service configuration interface. The left sidebar contains navigation options: STATUS, SETTINGS, DIAGNOSTICS (selected), Overview, Information, Interfaces, Routing, Firewall, Quality of service (selected), and Device. The main content area is titled 'QUALITY OF SERVICE' and shows the 'Quality of service' configuration page. The page displays a table with columns for 'Interface', 'Queues', and 'Classes'. The 'if\_bridge' interface is selected, and the table shows detailed statistics for various queues and classes, including packet counts, bytes, and various limits and thresholds.

### 8.3.5. Device

Provides general information about the unit (device).

The screenshot displays the 'DEVICE' configuration page in the RipEX2 web interface. The page is organized into two main sections: 'System information' and 'Advanced information'. The 'System information' section provides basic hardware details: Product code (RipEX2-4A-G-X), Serial number (1801619751), and FW version (2.0.8.0). The 'Advanced information' section provides more detailed hardware and software details: Modem board SN (1801619751), Radio board SN (1801636251), Radio SW version (1.0.0), CNF version (13), Web client version (1.55.1), Region ID (-), and Region description (-). The interface includes a left sidebar with navigation options like 'STATUS', 'SETTINGS', 'DIAGNOSTICS', and 'Device'. The top navigation bar shows the device name 'MO\_210' and IP address '@192.168.141.210', along with 'Remote access' and 'DEVICE' tabs. Both information sections have a 'Refresh' button and a 'Last refresh' timestamp.

#### 8.3.5.1. System information

Basic unit information is provided.

- Product code - Identifies the unit hardware.
- Serial number - Unique unit identification number.
- FW version - Currently installed unit firmware.

#### 8.3.5.2. Advanced information

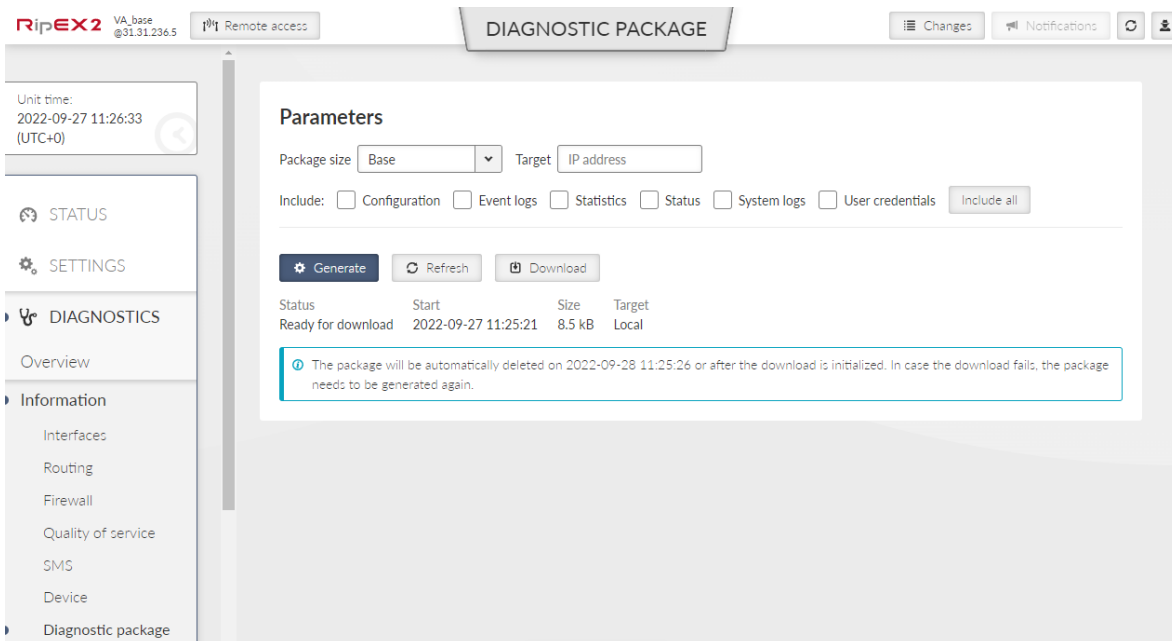
Additional unit information is provided which might be requested for advanced diagnostics. Partial description:

- Modem board SN - Modem boards system number.
- CNF version - Version of the unit configuration.
- Web client version - Version of the current web client.

### 8.3.6. Diagnostic package

This menu serves for collecting data, either from local or remote station and storing them into a package (file). Diagnostic package serves primarily as a help tool, for RACOM's technical support in case of any potential unit issues. Minimum size of a package is 5kB. Diagnostic package is downloaded already compressed, which saves approx. 1/3 of its original size.

Only one package collecting (applies for both local and remote) at a time is supported.



### Package size

List box {Base; Verbose}, default = "Base"  
 Defines the size of the generated package.

### Target

Defines the station, from which is the Diagnostic package being collected.

- Diagnostic package from a local station - this parameter stays empty.
- Diagnostic package from a remote station - destination IPv4 address of the requested station must be used.

### Include

- Configuration - configuration of the unit is added to the package (json format)
- Event logs - adds a list of events exported to csv
  - Base: Last 50 events
  - Verbose: Last 500 events
- Statistics - adds list of statistics exported to csv
  - Interval of frames statistics: 30 min
  - Base: 5 frames
  - Verbose: 10 frames
- Status - lists detailed status of networks devices and services
- System logs - adds last system logs
  - base: 100 of current lines from all logs

- verbose: whole logs content
- User credentials - adds a list of user accounts

After setting all parameters, click on "Generate" button. By clicking the "Refresh" button update the processing status of the package. Once the package is ready, it can be downloaded by clicking the "Download" button. After its download, the package is deleted from the unit. The package will be deleted even if its download is unsuccessful and if the download is not initiated, the package will be deleted automatically after 24h.

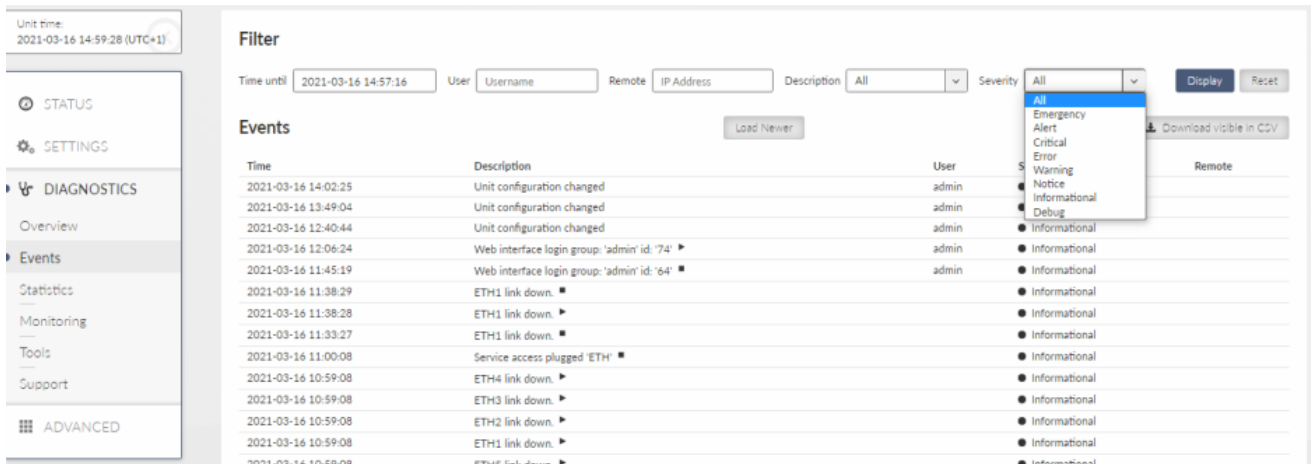
### 8.4. Events

This menu shows all events which occur within the unit history.

For filtering of events you can use the filtering tool. When no filter rules are used, the last 30 events will be displayed after Display button click.

Older events should be displayed using Load more button click, the events which occur during the viewing of this window can be loaded by using Load newer button.

Alarms are displayed in red color, warnings in orange, notices in black and debugs in gray.



It is possible to change severities of individual events in the menu SETTINGS > Device > Events.

**Tab. 8.3: Default Events level description**

| Severity group | Level | Severity  | Color code | Description   | Action                                       |
|----------------|-------|-----------|------------|---|--|
| ALARM          | 0     | Emergency | Red        | Faulty unit. HW repair is probably needed.          | Replace the unit. Contact Technical support. |
|                | 1     | Alert     | Red        | Unit does not work. HW or SW problem.               | Check the unit. Consult Technical support.   |
|                | 2     | Critical  | Red        | Serious error. Communication does not work.         | Check the unit immediately.                  |
|                | 3     | Error     | Red        | Error. Communication can work.                      | Check the unit.                              |
| WARNING        | 4     | Warning   | Orange     | Communication is OK. Self-healing action proceeded. | When often, consult with Technical support.  |



| Severity group | Level | Severity      | Color code | Description  | Action                                |
|----------------|-------|---------------|------------|--|---------------------------------------|
|                | 5     | Notice        | Blue       | Security important action proceeded or I/O action. | Security check, the I/O status check. |
| INFO           | 6     | Informational | -          | Informational item                                 | Standard behavior                     |
|                | 7     | Debug         | -          | Debug info, if set so.                             | Debug                                 |

## 8.5. Statistics

MIDGE3 unit permanently monitors various system 'channels'. There are several types of those channels: Physical interfaces (Ethernet ports, serial ports, MAIN, additional module interface (e.g. LTE module) when installed), virtual interfaces (e.g. VLAN interfaces) and HW sensors (CPU temperature, supply voltage, ...). Monitored values are stored in the internal database.

Statistics page provides aggregated statistical data from this internal database. Data can be both displayed and downloaded in CSV format. This file format is suitable to be imported to any 3rd party spreadsheet program for further analysis.

There are two different options how to display statistics data:

### Historical

Statistics counters are aggregated over the defined time interval. The interval is defined by two time stamps "From" and "To".

### Differential

Statistics counters are aggregated between the counter reset and the current time (the moment when the Display button was pressed). Reset is triggered by a unit reboot or by the Reset statistics button.

**Reset statistics button** - initiates the Differential statistic counters reset. Such a reset does not affect normal statistic counters - i.e. the Historical statistics are not affected by such a Reset at all.

### Length of statistics data

Statistics data are stored in the internal database. There is a fixed memory size allocated for the statistics data - the database is limited by number of records. As a result of this, the length of statistics history - how old records are available - depends on the actual network configuration: The more monitored values, the higher the rate of new recorded values, the shorter the available history.

Some sets of monitored values are constant (Ethernet ports and their counters) or do not rise to a high values (COM ports, Terminal servers and their counters).

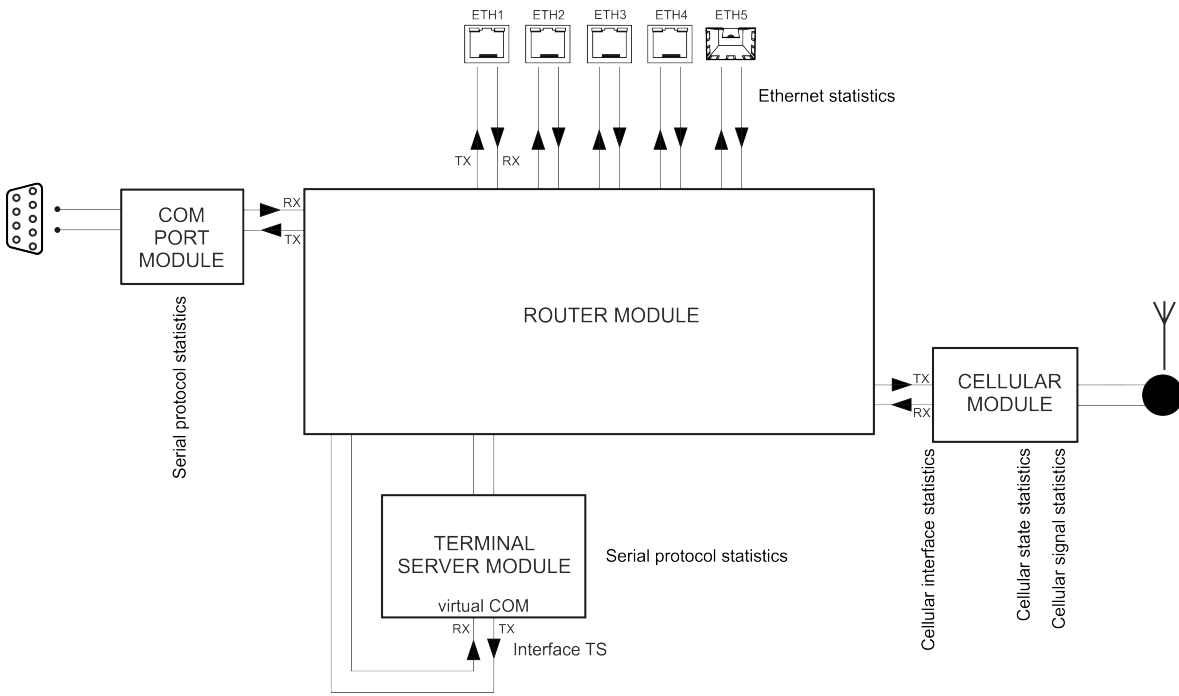


Fig. 8.1: Statistics data in the context of unit interfaces

### 8.5.1. Parameters

Statistics data are always retrieved as aggregated for a certain time Interval. This Interval can be set by putting specific date and time into "From" and "To" fields, or using buttons "Last day", "Last hour" or "More options" fast presets (from several minutes to several days). Button "Set Current Time" sets current time to both From and To fields to ease current unit status diagnostics.

There are following sets of statistical data available in the unit:

- Serial protocols statistics
- Ethernet statistics
- Cellular statistic
- Measurements

Unit time: 2022-09-14 06:40:12 (UTC+0)

Historical Differential

**Parameters**

- Serial protocols statistics
- Ethernet statistics
- Cellular interface statistics
- Cellular state statistics
- Cellular signal statistics
- Measurements

Interval: 2022-09-14 03:35 to 2022-09-14 06:35 | Now | 3 hours | Last day | Last hour | More options | Set current time

Display | Download Selected Data

**Data**

**Serial protocols statistics**

| Interface |    | Correct |     | Drop  |     |
|-----------|----|---------|-----|-------|-----|
|           |    | count   | [B] | count | [B] |
| com1      | Rx | 0       | 0   | 0     | 0   |
|           | Tx | 0       | 0   | 0     | 0   |
| ts2       | Rx | 0       | 0   | 0     | 0   |
|           | Tx | 0       | 0   | 0     | 0   |

More options dropdown menu:

- More options
- Last 5 minutes
- Last 15 minutes
- Last 30 minutes
- Last 1 hour
- Last 3 hours
- Last 6 hours
- Last 12 hours
- Last 1 day
- Last 2 days
- Last 7 days
- Today
- This week
- Yesterday
- Day before yesterday

Download Data

"Display" button then shows chosen data below. "Download Selected Data" button generates CSV (UTF-8 encoded) file of all chosen systems' data and downloads them as files without displaying them. Both "Display" and "Download ..." buttons send a request for the required set of statistics data to the unit. Retrieving and transferring of the data takes some time. Downloading the data is practical when the user needs to process them in a spreadsheet and wants to save some bandwidth. It is also recommended to use spreadsheet editor like Microsoft Excel or Apple Numbers to process statistics on mobile devices due to better user experience provided by the specialized apps.

### 8.5.2. Serial protocol statistics

Serial protocols statistics provides set of data monitoring the COM port(s) and Terminal server (s). Only enabled interfaces are displayed. The statistics counters are based on packets entering or leaving the COM port or Terminal server module. As a result of this the 'count' values correspond to the Protocol messages (the "Protocol" selected on the specific COM port or Terminal server). If the packet is 'glued' from the several frames, it is evaluated as a single packet. In case of COM port statistics, the summary of 'Correct' and 'Drop' Bytes provides the total amount of Bytes on the physical interface.

Rx direction: from the connected (at the COM or ETH port) external device to the M!DGE3 unit (i.e. from the COM port module or Terminal server module to the Router module). Tx direction: from the M!DGE3 unit to the external device.

Serial protocols statistics

Download Data

| Interface |    | Correct |     | Drop  |     |
|-----------|----|---------|-----|-------|-----|
|           |    | count   | [B] | count | [B] |
| com1      | Rx | 0       | 0   | 0     | 0   |
|           | Tx | 0       | 0   | 0     | 0   |
| ts1       | Rx | 0       | 0   | 0     | 0   |
|           | Tx | 0       | 0   | 0     | 0   |

**Interface** – Interface name

**Correct (Rx, Tx)** – Correctly received / transmitted packets count and amount of data in Bytes. Accepted by the COM port or Terminal server module - based on the selected Protocol processing. Amount of

data - for both Correct and Drop counters - is affected by COM port data only (i.e. IP headers of the UDP frames created in the COM port module are NOT counted).

**Drop (Rx, Tx)** - Dropped received / transmitted packets - reason: corrupted frame, CRC error, wrong protocol message, unsupported protocol message.


### 8.5.3. Ethernet statistics

Ethernet statistics provides set of data monitoring the physical Ethernet ports. Only enabled interfaces are displayed.

Only correctly received frames are handled. The counters correspond to the specific IP protocol types.

Rx direction: from the physical Ethernet port to the MIDGE3 unit (i.e. to the Router module). Tx direction: from the MIDGE3 unit to the physical Ethernet port.

Ethernet statistics

 Download Data

| Interface |    | UDP   |       | TCP   |         | ICMP  |     | ARP   |        | VLAN  |     | Multicast |         | IPv4 other |     | IPv6  |      | Other |     |
|-----------|----|-------|-------|-------|---------|-------|-----|-------|--------|-------|-----|-----------|---------|------------|-----|-------|------|-------|-----|
|           |    | count | [B]   | count | [B]     | count | [B] | count | [B]    | count | [B] | count     | [B]     | count      | [B] | count | [B]  | count | [B] |
| eth1      | Rx | 0     | 0     | 0     | 0       | 0     | 0   | 0     | 0      | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |
|           | Tx | 0     | 0     | 0     | 0       | 0     | 0   | 0     | 0      | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |
| eth2      | Rx | 0     | 0     | 0     | 0       | 0     | 0   | 0     | 0      | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |
|           | Tx | 0     | 0     | 0     | 0       | 0     | 0   | 0     | 0      | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |
| eth3      | Rx | 0     | 0     | 0     | 0       | 0     | 0   | 0     | 0      | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |
|           | Tx | 0     | 0     | 0     | 0       | 0     | 0   | 0     | 0      | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |
| eth4      | Rx | 321   | 70354 | 5204  | 551424  | 0     | 0   | 2425  | 111550 | 0     | 0   | 43244     | 1989224 | 2          | 92  | 42    | 5141 | 0     | 0   |
|           | Tx | 0     | 0     | 4386  | 7950627 | 0     | 0   | 22    | 616    | 0     | 0   | 0         | 0       | 0          | 0   | 0     | 0    | 0     | 0   |

**Interface** – Interface name.

**UDP, TCP, ICMP, ARP, VLAN, Multicast** - Packet count and amount of data in Bytes [B] for different protocol types - IPv4 traffic. Amount of data - for all counters - is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

**IPv4 other** - IPv4 traffic not handled by the previous counters

**IPv6** - IPv6 traffic counter

**Other** - Counter summing up the frames which were not handled by the previous counters - for example MPLS and GOOSE protocols.

### 8.5.4. Cellular statistics

Cellular statistics are available for main cellular module and eventually for optional extension module if used.

The screenshot shows the Diagnostics interface with the following sections:

- Serial protocols statistics:** Ethernet statistics, Cellular interface statistics (checked), Cellular state statistics (checked), Cellular signal statistics (checked), Measurements.
- Interval:** 2022-12-04 14:36 to 2022-12-05 14:36, 1 day.
- Data:**
  - Cellular interface statistics:**

| Interface | UDP   |     | TCP   |     | ICMP  |     | ARP   |     | IPv4 other |     | IPv6  |     | Other |     | SMS |     |
|-----------|-------|-----|-------|-----|-------|-----|-------|-----|------------|-----|-------|-----|-------|-----|-----|-----|
|           | count | [B] | count | [B] | count | [B] | count | [B] | count      | [B] | count | [B] | count | [B] | OK  | Rej |
| cell-main | Rx    | 0   | 0     | 0   | 0     | 0   | 0     | 0   | 0          | 0   | 0     | 0   | 0     | 0   | 0   | 0   |
|           | Tx    | 0   | 0     | 0   | 0     | 0   | 0     | 0   | 0          | 0   | 0     | 0   | 0     | 0   | 0   | -   |
  - Cellular state statistics:**

| Interface | SIM [%] |      | Services [%] |    |    |    | Networks [%] |      |         |       |
|-----------|---------|------|--------------|----|----|----|--------------|------|---------|-------|
|           | SIM1    | SIM2 | N/A          | 2G | 3G | 4G | NC           | Home | Roaming | Other |
| cell-main | 100     | 0    | 100          | 0  | 0  | 0  | 100          | 0    | 0       | 0     |
  - Cellular signal statistics:**

| Interface | Samples | 2G RSSI [dBm] |     |     |     | 3G RSCP [dBm] |     |     |     | 4G RSRP [dBm] |     |     |     |   |
|-----------|---------|---------------|-----|-----|-----|---------------|-----|-----|-----|---------------|-----|-----|-----|---|
|           |         | avg           | dev | min | max | avg           | dev | min | max | avg           | dev | min | max |   |
| cell-main | 0       | 0             | 0   | 0   | 0   | 0             | 0   | 0   | 0   | 0             | 0   | 0   | 0   | 0 |

### 8.5.4.1. Cellular interface statistics

Cellular interface statistics provides set of data collected from the interface between the Router module (IP routing engine in the unit) and the Cellular module. It corresponds to monitoring Cellular - Interface.

Tx direction: from the Router module to the Cellular module.

Rx direction: from the Cellular module to the Router module.

Cellular interface statistics

[Download Data](#)

| Interface | UDP   |     | TCP   |     | ICMP  |     | ARP   |     | IPv4 other |     | IPv6  |     | Other |     |
|-----------|-------|-----|-------|-----|-------|-----|-------|-----|------------|-----|-------|-----|-------|-----|
|           | count | [B] | count | [B] | count | [B] | count | [B] | count      | [B] | count | [B] | count | [B] |
| cell-aux  | Rx    | 0   | 0     | 0   | 0     | 0   | 0     | 0   | 0          | 0   | 0     | 0   | 0     | 0   |
|           | Tx    | 0   | 0     | 0   | 0     | 0   | 0     | 0   | 0          | 0   | 7     | 640 | 0     | 0   |

#### Interface

- "cell-main" interface is used for M!DGE3 MAIN cellular module.
- "cell-ext" interface is used for M!DGE3 optional extension cellular module.

#### UDP, TCP, ICMP, ARP

- Packet count and amount of data in Bytes [B] for different protocol types. Amount of data is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

#### IPv4 other

- Packets not handled by the previous counters (e.g. VLAN, services, GRE, IPsec (ESP), ...).

#### IPv6

- IPv6 packets are handled separately.

#### Other

- other packets than IPv4 or IPv6

### 8.5.4.2. Cellular state statistics

Cellular state statistics

[Download Data](#)

| Interface | SIM [%] |      | Services [%] |    |    |    | Networks [%] |      |         |       |  |
|-----------|---------|------|--------------|----|----|----|--------------|------|---------|-------|--|
|           | SIM1    | SIM2 | N/A          | 2G | 3G | 4G | NC           | Home | Roaming | Other |  |
| cell-aux  | 99      | 0    | 0            | 0  | 0  | 99 | 0            | 99   | 0       | 0     |  |

#### Interface

- "cell-main" interface is used for M!DGE3 MAIN cellular module.
- "cell-ext" interface is used for M!DGE3 optional extension cellular module.

#### SIM [%]

- information about using the individual SIM cards during the time displayed in %.

#### Services [%]

- N/A (not available), 2G (e.g. GPRS, EDGE), 3G (e.g. UMTS), 4G (e.g. LTE) services usage displayed in % of time.

#### Networks [%]

- NC (not connected), Home (home network), Roaming (roaming network), Other (not matching previous type of networks) displayed in % of time.



#### Note

Values are rounded to an integer (in %).

### 8.5.4.3. Cellular signal statistics

Cellular signal statistics

[Download Data](#)

| Interface | Samples | 2G RSSI [dBm] |     |     |     | Samples | 3G RSCP [dBm] |     |     |     | Samples | 4G RSRP [dBm] |     |      |     |
|-----------|---------|---------------|-----|-----|-----|---------|---------------|-----|-----|-----|---------|---------------|-----|------|-----|
|           |         | avg           | dev | min | max |         | avg           | dev | min | max |         | avg           | dev | min  | max |
| cell-aux  | 0       | 0             | 0   | 0   | 0   | 0       | 0             | 0   | 0   | 0   | 468     | -106          | 3   | -112 | -81 |

#### Interface

- "cell-main" interface is used for M!DGE3 MAIN cellular module.
- "cell-ext" interface is used for M!DGE3 optional extension cellular module.

#### 2G RSSI / 3G RSCP / 4G RSRP

Signal levels in dBm.

#### Samples

Number of samples used for the individual statistics.

#### avg / dev / min / max

Average / standard deviation / minimum / maximum value.

### 8.5.4.4. Measurements

#### Measurements

| Sensor           | count | avg  | min  | max  |
|------------------|-------|------|------|------|
| CPU [°C]         | 8478  | 52.9 | 52.1 | 54.3 |
| Modem board [°C] | 8478  | 38.1 | 37.6 | 39.1 |
| Radio board [°C] | 0     | 0    | 0    | 0    |
| Input [V]        | 8478  | 13.3 | 13.3 | 13.4 |

#### Sensor

Measured values on M!DGE3.

#### count

Number of times that the sensor measured given value (counter).

#### avg / min / max

Average / minimum / maximum value.

## 8.6. Monitoring

Monitoring is an advanced on-line diagnostic tool, which enables a detailed analysis of communication over any of the M!DGE3 router interfaces. In addition to all the physical interfaces (MAIN, EXT, ETHs, COMs, TSs), some internal interfaces between software modules can be monitored when such advanced diagnostics is needed.

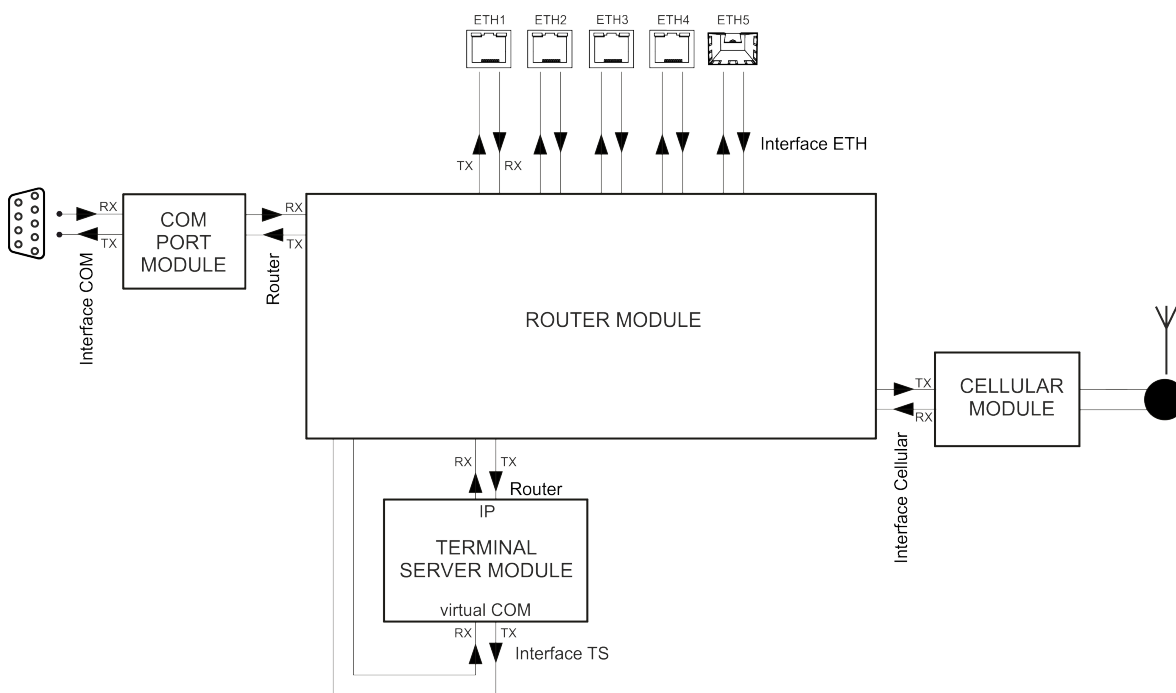
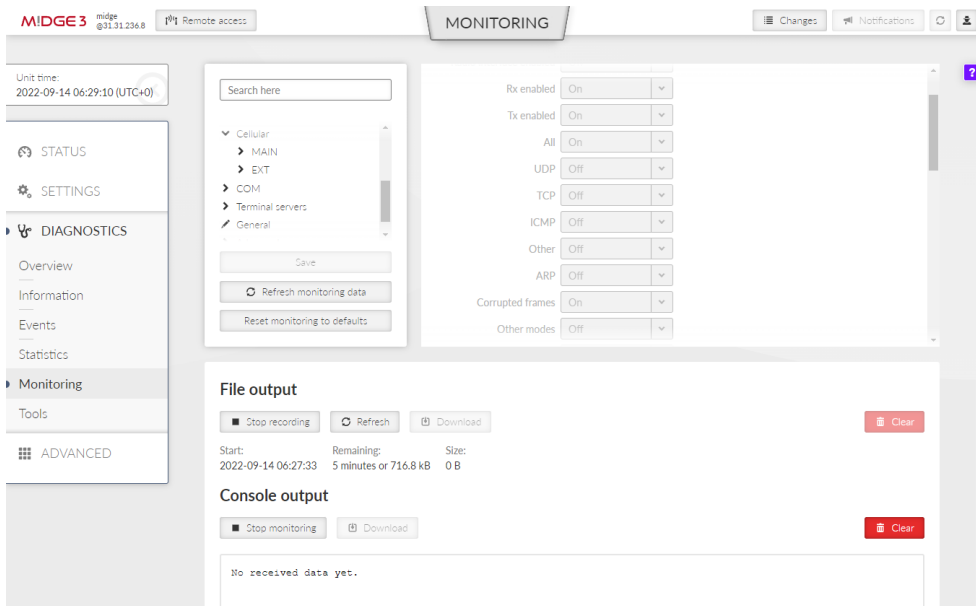


Fig. 8.2: Interfaces in the context of unit monitoring

Monitoring consists of two independent processes: settings of the monitored items and outputs. Please note that even if both of the outputs are switched off and some interfaces are set to On, the monitoring is still running in the background.

The monitoring screen has two main parts - Settings and Output



### 8.6.1. Settings

**Save** button - saves the new settings of the monitoring parameters.

**Refresh monitoring data** button - refreshes the settings menu according to the statistics status saved in the unit. The difference between the displayed and saved status can occur for example when the status is changed in different browser tab.

#### 8.6.1.1. Overview

All status (On/Off) of individual interfaces are displayed on this place for quick overview on monitoring settings.

#### 8.6.1.2. Interfaces

This section allows detailed settings of particular monitoring parameters for all interfaces.

### Common parameters for several interfaces:

#### Rx enabled, Tx enabled

List box {On; Off}, default = "On"

A packet is considered a Tx one when it comes out from the respective software module (e.g. Terminal Server) and vice versa. When an external interface (e.g. Interface COM) is monitored, the Tx also means packets being transmitted from the MIDGE3 over the respective interface (Rx means "received"). Understanding the directions over the internal interfaces may not be that straightforward, please see *Fig. 8.2, "Interfaces in the context of unit monitoring"* above for clarification.



**All**

List box {On; Off}, default = "On"

Monitoring output can also be limited by IP protocol type. Select Off to be able to enable/disable specific protocol output individually - see next parameter(s).

**UDP / TCP / ICMP / Other / ARP**

List box {On; Off}, default = "Off"

Monitoring output of specific IP protocol limitation.

**Offset [B]**

Default = 0

Number of bytes from the beginning of packet/frame, which will not be displayed - the monitoring output is truncated by 'Offset' bytes at the beginning of the message.

**Length [B]**

Default = 32

Number of bytes to be displayed from each packet/frame.

Example: Offset=2, Length=4 means, that bytes from the 3rd byte to the 6th (inclusive) will be displayed:

Data (HEX):               01AB **3798 A285** 93CD 6B96

Monitoring output:               3798 A285

**Bandwidth**

List box {LOW; NORMAL; HIGH; UNLIMITED}, default = "NORMAL"

Monitoring bandwidth limit to prevent overload of management link between client PC and the M!DGE3 unit. LOW (up to ~300 kb/s), NORMAL (up to ~800 kb/s), HIGH (up to ~2 Mb/s), UNLIMITED (up to ~8 Mb/s)

**Source port (from) / Source port (to)**

TCP/UDP source port to be enabled/disabled in the monitoring output. Use these parameters to specify the source range of ports <from - to>.

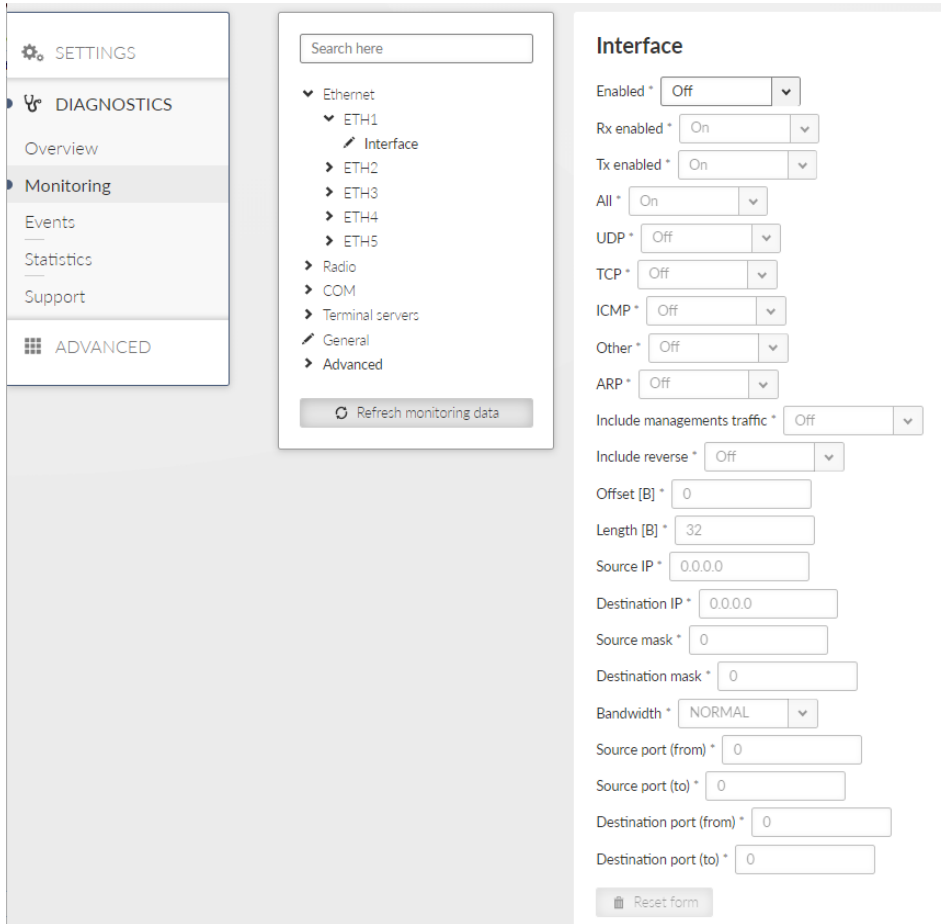
**Destination port (from) / Destination port (to)**

TCP/UDP destination port to be enabled/disabled in the monitoring output. Use these parameters to specify the destination range of ports <from - to>.

**Dropped frames**

List box {On; Off}, default = "Off"

When On, monitoring shows frames which are dropped (e.g. CRC is not valid, buffer overflow, ...).



## ETH interfaces

### Include management traffic

List box {On; Off}, default = "Off"  
 Enable/disable management packets monitoring output.

### Include ETH headers

List box {On; Off}, default = "Off"  
 Displays (enable) / omits (disable) L2 headers in the monitoring output.

### Include reverse

List box {On; Off}, default = "Off"  
 Enable/disable reverse traffic (e.g. TCP reply to a request) monitoring.

### Source IP / mask, Destination IP / mask

Monitoring output can also be limited to a specific address range - Source and Destination IP address and mask can be used to define the required range.

## Cellular interfaces

Cinterion PLS83-W cellular module is connected to L3 layer, thus captured frames do not contain L2 header(s). For consistency reasons are following values added to the frame:

- SRC mac: 0x0 0x0 0x0 0x0 0x0 0x0

- Dst mac: 0x0 0x0 0x0 0x0 0x0 0x0
- Ethertype: 0x0800

### Cellular interface MAIN enabled (MAIN)

List box {On; Off}, default = "Off"

### Cellular interface EXT enabled (EXT)

List box {On; Off}, default = "Off"

#### 8.6.1.3. General

The screenshot shows the RipEX2 web interface. At the top, there's a header with 'RipEX2' logo, unit information (MQ\_210 @192.168.141.210), and a 'Remote access' button. The main navigation bar includes 'MONITORING', 'Changes', 'Notifications', and a user icon. On the left, there's a sidebar with 'STATUS', 'SETTINGS', 'DIAGNOSTICS', and 'Monitoring'. The 'DIAGNOSTICS' section is expanded, showing a search bar and a list of categories: Overview, Ethernet, Radio, COM, Terminal servers, General (selected), and Advanced. Below this list are buttons for 'Save', 'Refresh monitoring data', and 'Reset monitoring to defaults'. The main content area shows the 'General' settings for monitoring, with three dropdown menus: 'Max. file size' (700 kB (~100 kB)), 'Time period' (5 min), and 'Show time difference' (Off). A 'Reset form' button is located below these settings.

The settings of output parameters for file output – **Max. file size** and **Time period**, the first parameter matched closes the monitoring file. File is saved in compressed way, so the uncompressed and approximate compressed size is displayed in the list box.

#### Max. file size

List box {7 kB (~1 kB); 70 kB (~10 kB); 358 kB (~50 kB); 700 kB (~100 kB); 3 MB (~500 kB); 7 MB (~1 MB); max (~2 MB)}, default = "700 kB (~100 kB)"

#### Time period

List box {1 min; 2 min; 5 min; 10 min; 20 min; 30 min; 1 hour; 3 hours; 24 hours; Off}, default = "5 min"

#### Show time difference

List box {On; Off}, default = "Off"

When On, the time difference between subsequent packets is displayed in the monitoring output.

#### 8.6.2. File output

**Record** button – starts recording to the file. Triggers a process, which is set by parameters in the chapter above (*Section 8.6.1.3, "General"*).

**Stop recording** button – stops recording to the file. The recording will be stopped immediately regardless of the size and time of recording. When the Record button is pressed for the second time the previously recorded data will be cleared.

**Refresh** button – refreshes the information about time remaining and size of the recorded data (in uncompressed way).

**Download** button – downloads file to a connected computer. The default name contains of the Unit name, date and time of the begin and day and time of the end of the monitoring. Before downloading you have to stop recording.

**Clear** button – allows to clear the monitoring data stored in the unit – both downloaded or not downloaded.

### 8.6.3. Console output

**Monitor / Stop monitoring** button

**Download** button – downloads the content of the console output as a file

**Clear** button - clears Console output screen



#### Note

If the amount of monitored data exceeds the limit (2.7 kB for remote monitoring and 32 kB for local monitoring) for one time period (approx. 1 s), some data will not be displayed in the console output. A note about the omitted data will be inserted to the console output to the position of the non-displayed data.

## 8.7. Tools

Set of diagnostic tools

### 8.7.1. ICMP ping

Unit time: 2020-06-23 10:57:38 (UTC+2)

SETTINGS

DIAGNOSTICS

- Overview
- Events
- Statistics
- Monitoring
- Tools**
- Support

ADVANCED

### ICMP Ping

**Parameters**

Length [Bytes]  Period [ms]  Timeout [ms]  Count  Source IP

Destination IP

**Controls**

**Output**

```
PING 10.10.10.11 (10.10.10.11) from 10.10.10.12 : 200(228) bytes of data.  
208 bytes from 10.10.10.11: icmp_seq=1 ttl=64 time=384 ms  
208 bytes from 10.10.10.11: icmp_seq=2 ttl=64 time=378 ms  
208 bytes from 10.10.10.11: icmp_seq=3 ttl=64 time=391 ms  
208 bytes from 10.10.10.11: icmp_seq=4 ttl=64 time=385 ms  
  
--- 10.10.10.11 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 378.059/384.800/391.316/4.760 ms
```

All parameters used by standard ICMP ping are available. Start / Stop button starts / stops pinging.

## 8.7.2. RSS ping

RSS ping can be used for monitoring of the radio channel in case of hybrid networks (M!DGE3 / RipEX2 combination). In such networks, RSS ping comes through the whole network, but information about the RSS/MSE is evaluated only for radio hops.

RSS ping is a diagnostic tool for the radio performance measurement (Radio Signal Strength and modulation Mean Squared Error) of the individual radio hops within a M!DGE3 network. Hybrid networks are supported. Output format of different type (other than radio) of hops is similar to ICMP ping.

The screenshot shows the M!DGE3 web interface with the 'RSS ping' tab selected. The interface includes a sidebar with navigation options like STATUS, SETTINGS, DIAGNOSTICS, and ADVANCED. The main content area is divided into 'Parameters', 'Controls', and 'Output' sections.

**Parameters:**

- Destination IP: 10.10.10.212
- Length [Bytes]: 1200
- Period [ms]: 100
- Timeout [ms]: 10000
- Count: 5
- Source IP: (empty)
- Go on: Off
- Traces reserved: 4

**Controls:**

- Start button
- Download button
- Clear button

**Output:**

```
1200+81 bytes from 10.10.10.212: seq=6 RTT=2038.759ms ^
10.10.10.210-->(10.10.10.212: MC:F0 RSS:68/hMSE:36/dMSE:36)-->10.10.10.212
10.10.10.212-->(10.10.10.210: MC:B0 RSS:67/hMSE:34/dMSE:32)-->10.10.10.210
---RSS Ping from 10.10.10.210 to 10.10.10.212 statistics---
5 packet(s) transmitted, 5 received, 0.00% packet loss (0 corrupted, 0 rejected), time 2.46s
RTT: min/avg/max/mdev = 324.047/1241.430/2038.759/696.078 [ms]
Load: 20948 bps
Throughput: 20948 bps
Radio hop with the lowest RSS - direction to destination:
RSS: min/avg/max/mdev = 68/68.0/68/0.0 [-dBm]
hMSE: min/avg/max/mdev = 34/35.2/36/0.7 [-dB]
dMSE: min/avg/max/mdev = 36/37.0/38/0.6 [-dB]
```

### Destination IP

Destination IP address. This address must belong to a M!DGE3 unit as the RSS ping can be initiated only between two M!DGE3 units.

### Length [B]

Number {8 – 1500}, default = 10

The length of data used by RSS ping. In case the length of RSS ping packet is longer than the length of **Radio interface MTU**, the first RSS ping packet will be lost and will cause decreasing of the packet length to the value matching to the current radio MTU. Random data are used as a payload.

### Period [ms]

Number {100 – 3 600 000}, default = 1000

Period of sending RSS ping packets

When the period is set to a shorter number than the actual RTT, collisions might appear (depends on the selected Radio protocol). In order to reach the shortest possible period enable the **Go on** mode.

### Timeout [ms]

Number {100 – 3 600 000}, default = 10000

Response timeout

### Count

Number {1 – 10000}, default = 5

Number of RSS pings to be send

**Source IP**

The local IP address of M!DGE3 unit originating RSS ping. Blank field (equal to 0.0.0.0 address) is used to assign the source address automatically - address is assigned automatically according to the routing rules.

**Go on**

List box {On; Off}, default = "Off"

Go on mode. When Enabled, RSS pings are sent immediately after receiving the RSS ping reply (Period parameter is ignored).

**Traces reserved**

The RSS ping also contains data about the route (RSS, MSE), this parameter allows to set number of radio hops within the network to be measured. Radio hop is measured in both directions, so the number has to be higher than number of hops in route multiplied by 2 (for example: link consisting of 2 radio hops needs 5 traces to be reserved).

**Output:**

- **MC** – Encodes Modulation and Coding – see transcription table:

**Tab. 8.4: Translation table for Modulation rates and FEC**

|    | <b>Modulation</b> | <b>FEC</b> |
|----|-------------------|------------|
| 00 | 2CPFSK            | FEC off    |
| 01 |                   | FEC 3/4    |
| 10 | 4CPFSK            | FEC off    |
| 11 |                   | FEC 3/4    |
| 80 | DPSK              | FEC off    |
| 81 |                   | FEC 3/4    |
| 90 | pi/4 DQPSK        | FEC off    |
| 91 |                   | FEC 3/4    |
| A0 | D8PSK             | FEC off    |
| A1 |                   | FEC 3/4    |
| B0 | 16DEQAM           | FEC off    |
| B1 |                   | FEC 3/4    |
| C0 | 64QAM             | FEC off    |
| C1 |                   | FEC 3/4    |
| D0 |                   | FEC 5/6    |
| D1 |                   | FEC 2/3    |
| E0 | 256QAM            | FEC off    |
| E1 |                   | FEC 3/4    |
| F0 |                   | FEC 5/6    |
| F1 |                   | FEC 2/3    |

- **RSS** – Radio Signal Strength [dBm] - measured within the header reception

- **hMSE** – Phy header modulation Mean Squared Error [dB] - measured within the header reception
- **dMSE** – Data modulation Mean Squared Error [dB] - measured within the frame data part reception

### 8.7.3. Routing

Routing tool provides the next hop routing information of the given IP address.

#### Destination IP

The examined IP address.

#### Output

Output section provides the following details:

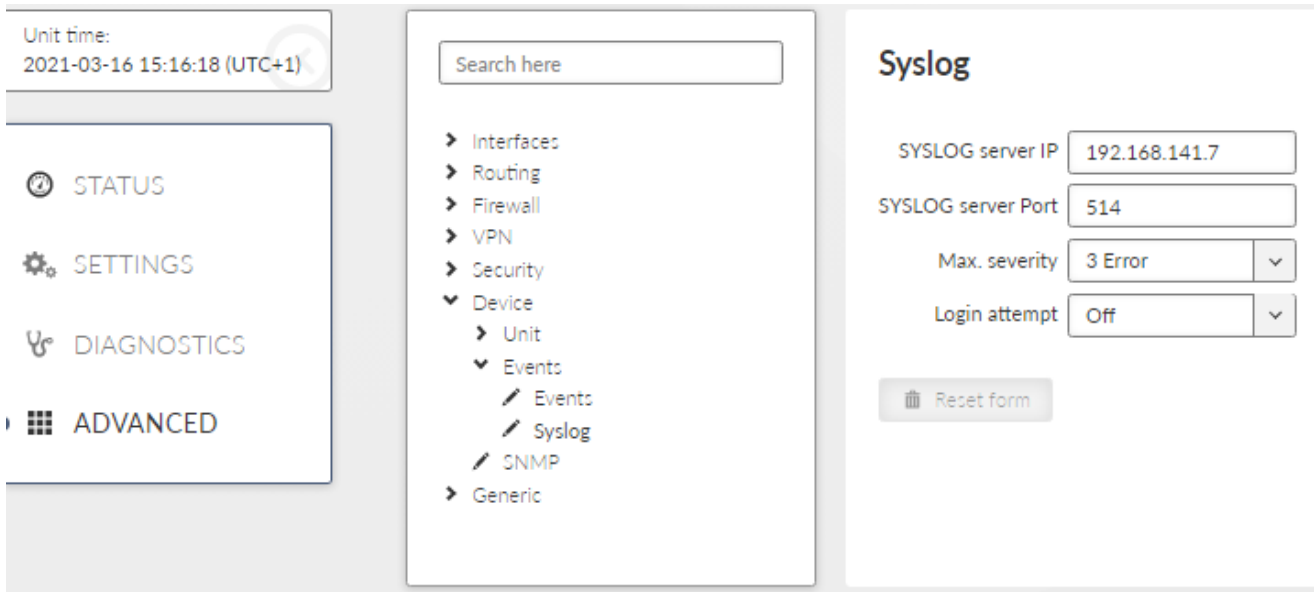
- Examined address (example: 8.8.8.8)
- Next hop (gateway) address (example: via 192.168.141.254)
- Next hop interface (example: dev if\_bridge)
- Outgoing packet Source address (example: src 192.18.141.210)

### 8.7.4. System

#### Reboot button

Performs unit cold restart (power cycle equivalent).

## 8.8. Syslog



### **SYSLOG server IP**

IP address of the remote Syslog server to which logs will be sent with severity higher than severity set in the Max. severity

### **SYSLOG server Port**

Port used by the Syslog server

### **Max. severity**

List box {Off; 0 Emergency; 1 Alert; 2 Critical; 3 Error}, default= "Off"

Off - switches off the SYSLOG functionality

Only the events with set severity (and higher) will be sent to the Syslog server. Severities for individual Events can be set in *Section 7.6.3, "Events"*.

### **Login attempt**

List box {Off; Web}, default = "Off"

Switches whether login attempts (both successful and unsuccessful) will be sent to the SYSLOG server.



## 9. Technical parameters

| <b>Electrical</b> |   |                 |
|-------------------|---|-----------------|
| Primary power     | 10 to 50 VDC, negative GND  |                 |
| Rx                | 4.8 W / 24 V, <i>see details</i>  |                 |
| Tx                | 7.8 W / 24 V, <i>see details</i>  |                 |
| Sleep mode        | 0.01 W  |                 |
| <b>Interfaces</b> |   |                 |
| Ethernet          | 10/100/1000Base-T Auto MDI/MDIX   | 4× RJ45         |
| SFP               | 10/100/1000Base-T or 1000Base-SX or 1000Base-LX<br>user exchangeable SFP with max. power consumption 1.25 W | 1× SFP          |
| COM               | RS232 / RS485 SW configurable   | Terminal block  |
|                   | 600 b/s – 1 Mb/s  |                 |
| USB               | USB 3.0   | Host A          |
| Antenna           | 50 Ω<br>2×2 MIMO  | 2×SMA female    |
| Inputs/Outputs    | 1× HW alarm input<br>1× HW alarm output<br>1× Sleep input   | Power connector |
|                   | 2× DI, 2× DO, 1× diffDI   | RJ45            |

| <b>Cellular interface</b>                         |   |
|---|---|
| Frequency bands for extension module 'W' Cellular | 4G LTE (also 5G NSA)<br>Band 1 (2100 MHz), Band 2 (1900 MHz), Band 3 (1800 MHz),<br>Band 4 (2100 MHz), Band 5 (850 MHz), Band 7 (2600 MHz),<br>Band 8 (900 MHz), Band 12 (700 MHz), Band 13 (700 MHz)*,<br>Band 18 (850 MHz), Band 19 (850 MHz), Band 20 (800 MHz),<br>Band 26 (850 MHz), Band 28 (700 MHz), Band 38 (2600 MHz),<br>Band 40 (2300 MHz), Band 41 (2500 MHz), Band 66 (2100 MHz)<br>* a sensitivity issue will occur in GNSS when transmitting in band 13 |
|   | 3G UMTS/HSDPA/HSUPA<br>Band 1 (2100 MHz), Band 2 (1900 MHz), Band 3 (1800 MHz),<br>Band 4 (2100 MHz), Band 5 (850 MHz), Band 6 (850 MHz), Band 8 (900 MHz), Band 19 (850 MHz)   |
|   | 2G GSM/GPRS/EDGE<br>GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz  |
|   | Cinterion PLS83-W<br>FCC ID QIPPLS83-W<br>TAC 35107264  |
| Specification                                     | ANT1, ANT2 - space diversity      2× SMA Antenna  |
|   | 4G LTE<br>3GPP Release 9<br>Long Term Evolution (LTE)<br>Evolved Uni. Terrestrial Radio Access (E-UTRA)<br>Frequency Division Duplex (FDD)<br>DL Multi-Input Multi-Output (MIMO) 2×2  |
|   | 3G UMTS/HSDPA/HSUPA<br>3GPP Release 8<br>Dual-Cell HS Packet Access (DC-HSPA+)<br>UMTS Terrestrial Radio Access (UTRA)<br>Frequency Division Duplex (FDD) DL Rx diversity   |
|   | 2G GSM/GPRS/EDGE<br>3GPP Release 8<br>Enhanced Data rate GSM Evolution (EDGE)<br>GSM EGPRS Radio Access (GERA)<br>Time Division Multiple Access (TDMA)<br>DL Advanced Rx Performance Phase 1  |
|   | Data rates up to 150 Mb/s downlink / 50 Mb/s uplink   |
|   | SIM slots      2x Micro SIM (3FF)<br>Both 1.8 and 3 V SIM types supported   |
|   |   |

| <b>Indication LEDs</b>            |   |
|-----------------------------------|---|
| LED panel                         | 5× tri-color status LEDs (SYS, WAN, EXT, VPN, COM)  |
| ETH                               | 4× RJ45 (Link and Activity LEDs), 1× SFP (Status LED)   |
| <b>Environmental</b>              |   |
| IP Code (Ingress Protection)      | IP40, for indoor use only   |
| MTBF (Mean Time Between Failure)  | > 900 000 hours (> 100 years)   |
| Service life of system            | >= 15 years   |
| Operating temperature             | -40 to +70 °C ( -40 to +158 °F)   |
| Operating humidity                | 5 to 95 % non-condensing  |
| Storage                           | -40 to +85 °C ( -40 to +185 °F) / 5 to 95 % non-condensing  |
| <b>Mechanical</b>                 |   |
| Casing                            | Metal   |
| Dimensions                        | H×W×D: 132×43×110 mm (5.20×1.69×4.33 in)  |
| Weight                            | 0.50 kg (1.1 lbs)   |
| Mounting                          | DIN rail, optionally: flat-bracket or corner-bracket  |
| <b>SW</b>                         |   |
| User protocols on COM             | DNP3, DF1, IEC101, Modbus RTU, PR2000, RDS, Siemens 3964(R), COMLI, SAIA S-bus, Mars-A, UNI, Async Link |
| User protocols on Ethernet        | Modbus TCP, IEC104, DNP3 TCP, Comli TCP, Terminal server...   |
| Serial to IP convertors           | DNP3 / DNP3 TCP, Modbus RTU / Modbus TCP  |
| <b>Security</b>                   |   |
| Management                        | HTTPS (own certificate), SSH  |
| Role-based access control (RBAC)  | 4 levels (Guest, Tech, SecTech, Admin)  |
| WiFi management access (optional) | WPA2-PSK secured  |
| VPN                               | IPsec, GRE  |
| VLAN                              | IEEE 802.1Q (tagging)   |
| AAA protocol                      | RADIUS  |
| Firewall                          | Layer 2 - MAC, Layer 3 - IP, Layer 4 - TCP/UDP  |
| FW                                | Digitally signed  |
| HW tamper                         | Case opening evidence   |

| <b>Diagnostic and Management</b> |  |
|----------------------------------|--|
| Link testing                     | ICMP ping  |
| Status information               | User interfaces  |
| Statistics                       | Historical and differential statistics for Rx / Tx Packets on all user interfaces (e.g. ETH 1-5, COM 1-3, TS 1-5)                          |
| Statistics history               | Several weeks  |
| Event log                        | Events filtered by time, severity, user, remote IP address and type of event   |
| SNMP                             | SNMPv1, SNMPv2c, SNMPv3<br>Trap / Inform notifications generation as per settings  |
| NTP                              | Client / Server  |
| Monitoring                       | Real time analysis of all interfaces (e.g. ETH 1-5 , COM 1-3, TS 1-5) and internal interfaces between software modules, <i>see details</i> |

| <b>Standards</b>                       |   |
|--|---|
| CE                                     | <i>RED, RoHS, WEEE</i>  |
| Spectrum                               | ETSI EN 301 511 V12.5.1<br>ETSI EN 301 908-01 V13.1.1<br>ETSI EN 301 908-02 V11.1.2<br>ETSI EN 301 908-13 V13.1.1<br>ETSI EN 303 413 V1.1.1 |
| EMC<br>(electromagnetic compatibility) | ETSI EN 301 489-1 V2.2.3<br>ETSI EN 301 489-5 V3.2.1<br>ETSI EN 301 489-19 V2.1.0<br>ETSI EN 301 489-52 V1.1.0                              |
| Product safety                         | EN 62368-1:2014 + A11:2017  |
| RF health safety                       | EN 62311:2008   |
| Electric power substations environment | IEEE 1613:2009<br>IEEE 1613.1:2013<br>EN 61850-3:2014   |
| Environmental                          | EN 61850-3: 2014  |
| Vibration & shock                      | EN 60068-2-6:2008<br>ETS 300 019-2-3:1994, Class 3.4<br>EN 61850-3:2014   |
| Seismic qualification                  | EN 60068-2-27:2010  |
| IP rating                              | EN 60529:1993 + A1:2001 + A2:2014   |

| Optional interfaces                        |   |
|--|---|
| Extension module 'G'<br>GPS (GNSS) pending | Active antenna 3.3 VDC SMA female (EXT1 on bottom)  |
|  | 72-channel u-blox M8 engine GPS/QZSS L1 C/A, GLONASS L10F, BeiDou B1I, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN   |
| Extension module 'C'<br>COM ports          | COM2:<br>RS232 - 5 pin (RxD, TxD, GND, RTS, CTS)<br>600 b/s to 2 Mb/s<br>COM3:<br>RS232 -3 pin (RxD, TxD, GND)<br>2.4 kb/s to 921.6 kb/s<br>RJ45 (DI/DO on front panel) |
| Extension module 'W'<br>Cellular           | see <i>Cellular interface</i>   |

| List of connected cables                            |  |                        |                        |
|---|--|------------------------|------------------------|
| Input / Output                                      | Specified length for EN 61850-3                                | Shielded / Nonshielded | Recommended cable type |
| DC power supply 10 – 50 V                           | As needed  | N                      | V03VH-H 2×0,5          |
| GPIO (Sleep Input, HW Alarm Input, HW Alarm Output) | As needed  | S                      | LiYCY 6×0,14           |
| Antenna connection                                  | As needed  | S                      | Coaxial                |
| COM (RS232/485)                                     | As needed, typically up to 15 m (RS232) or up to 400 m (RS485) | S                      | LiYCY 4×0,14           |
| EXT1  | As needed (for cellular)                                       | S                      | Coaxial                |
|   | Max. 2 m (GPS antenna)   |                        |                        |
| EXT2  | As needed (for cellular)                                       | S                      | Coaxial                |
|   | Max. 2 m (time pulse output)                                   |                        |                        |
| ETH (4 ports)                                       | As needed, typically up to 100 m                               | S                      | STP CAT 5e             |
| Optical Ethernet                                    | As needed, typically up to 2 km                                | N/A                    | Optical fibre          |
| USB   | Max. 2 m   | S                      | USB3                   |
| DI / DO   | As needed  | S                      | STP CAT 5e             |

| <b>Rx Power consumption @24Vdc</b> |  |
|------------------------------------|--|
| Rx                                 | 4.8 W  |
| LTE Tx                             | +3.0 W   |
| +Ethernet                          | +0.1 W @ 10BaseT<br>+0.12 W @ 100BaseT<br>+0.5 W @ 1000BaseT<br>per Eth interface with connected equipment |
| +1st COM                           | +0.2 W   |
| +GNSS                              | +0.15 W  |
| +2 <sup>nd</sup> COM               | +0.1 W   |
| +2 <sup>nd</sup> LTE               | Rx +0.3, Tx +3.0 W   |
| +SFP module typ.                   | +1.0 W   |

## 10. Safety, regulations, warranty

### 10.1. Safety instructions

The M!DGE3 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!DGE3 cellular 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!DGE3 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 to prevent possible injury to health sets, radio receivers and personal computers, M!DGE3 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 40 cm 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. High temperature



If the M!DGE3 is operated in an environment where the ambient temperature exceeds 55 °C, the M!DGE3 must be installed within a restricted access location to prevent human contact with the enclosure heatsink.

## 10.3. Battery disposal

Battery Disposal - This product may contain a battery (e.g. CRC1225, 3V, 48 mAh). Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste. 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.

## 10.4. Instructions for Safe Operation of Equipment

Please read these safety instructions carefully before using the product:

- The radio equipment can only be operated on frequencies stipulated by the body authorized by the radio operation administration in the respective country and cannot exceed the maximum permitted output power. RACOM is not responsible for products used in an unauthorized way.
- Equipment mentioned in this User manual may only be used in accordance with instructions contained in this manual. Error-free and safe operation of this equipment is only guaranteed if this equipment is transported, stored, operated and controlled in the proper manner. The same applies to equipment maintenance.
- In order to prevent damage to the cellular router and other terminal equipment the supply must always be disconnected upon connecting or disconnecting the cable to the cellular router data interface. It is necessary to ensure that connected equipment has been grounded to the same potential.
- Only undermentioned manufacturer is entitled to repair any devices.

## 10.5. SW license

Conditions of use of this product software abide by the license mentioned below. The program spread by this license has been freed with the purpose to be useful, but without any specific guarantee. The author or another company or person is not responsible for secondary, accidental or related damages resulting from application of this product under any circumstances.

### RACOM Open Software License

Version 1.0, November 2009

Copyright (c) 2001, RACOM s.r.o., Mírová 1283, Nové Město na Moravě, 592 31

Everyone can copy and spread word-for-word copies of this license, but any change is not permitted.

The program (binary version) is available for free on the contacts listed on <https://www.racom.eu>. This product contains open source or another software originating from third parties subject to GNU General Public License (GPL), GNU Library / Lesser General Public License (LGPL) and / or further author licenses, declarations of responsibility exclusion and notifications. Exact terms of GPL, LGPL and some



further licenses is mentioned in source code packets (typically the files COPYING or LICENSE). You can obtain applicable machine-readable copies of source code of this software under GPL or LGPL licenses on contacts listed on <https://www.racom.eu>. This product also includes software developed by the University of California, Berkeley and its contributors.

## 10.6. EU Compliance

### 10.6.1. RoHS, WEEE and WFD

The image shows a document titled "EU DECLARATION OF CONFORMITY" for RACOM equipment. It lists the equipment models (RipEX, RipEX2, RAY2, RAY3, MIDGE2, MIDGE3, RipEX-HS, RipEX2-HS) and the manufacturer (RACOM s.r.o., Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic). The document states that the equipment is in conformity with the RoHS and WEEE directives. It also includes a signature of Jiri Hruska, CEO, dated 3rd June 2022, and contact information for RACOM s.r.o.

**RACOM**  
www.racom.eu

**EU DECLARATION OF CONFORMITY**

|                     |  |
|---------------------|--|
| <b>Equipment</b>    | RipEX, RipEX2<br>RAY2, RAY3<br>MIDGE2, MIDGE3<br>RipEX-HS, RipEX2-HS     |
| <b>Manufacturer</b> | RACOM s.r.o.<br>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, 3<sup>rd</sup> June 2022  
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. 1.2

Fig. 10.1: EU Declaration of Conformity RoHS, WEEE

## Waste Framework Directive Statement

According to the Directive 2008/98/EC on waste amended by Directive (EU) 2015/1127 and Directive (EU) 2018/851 (Waste Framework Directive) we hereby state that our products doesn't contain substances of very high concern (SVHC) listed on European chemical agency (ECHA) SCIP database candidate list in concentrations above 0.1 % w/w.

### 10.6.2. EU Declaration of Conformity RED

**RACOM**  
www.racom.eu

**EU DECLARATION OF CONFORMITY**

Radio equipment type MIDGE3

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:

|                                 |                          |
|---------------------------------|--------------------------|
| Radio Spectrum (Article 3.2)    | EN 301 511 V12.5.1       |
|                                 | EN 301 908-1 V13.1.1     |
|                                 | EN 301 908-2 V13.1.1     |
|                                 | EN 301 908-13 V13.1.1    |
|                                 | EN 303 413 V1.2.1        |
| EMC (Article 3.1b)              | EN 301 489-1 V2.2.3      |
| Product Safety (Article 3.1a)   | EN 62368-1:2020+A11:2020 |
| RF Health Safety (Article 3.1a) | EN 62311:2008            |

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 3<sup>rd</sup> of June 2022  
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. 10.2: EU Declaration of Conformity RED

### 10.6.3. Simplified EU declaration of conformity

BG

С настоящото RACOM s.r.o. декларира, че този тип радиосъоръжение MIDGE3 е в съответствие с Директива 2014/53/EC.

ES

Por la presente, RACOM s.r.o. declara que el tipo de equipo radioeléctrico MIDGE3 es conforme con la Directiva 2014/53/UE.

CS

Tímto RACOM s.r.o. prohlašuje, že typ rádiového zařízení MIDGE3 je v souladu se směrnicí 2014/53/EU.

DA

Hermed erklærer RACOM s.r.o., at radioudstyrstypen MIDGE3 er i overensstemmelse med direktiv 2014/53/EU.

DE

Hiermit erklärt RACOM s.r.o., dass der Funkanlagentyp MIDGE3 der Richtlinie 2014/53/EU entspricht.

ET

Käesolevaga deklareerib RACOM s.r.o., et käesolev raadioseadme tüüp MIDGE3 vastab direktiivi 2014/53/EL nõuetele.

EL

Με την παρούσα ο/η RACOM s.r.o., δηλώνει ότι ο ραδιοεξοπλισμός MIDGE3 πληροί την οδηγία 2014/53/EE.

EN

Hereby, RACOM s.r.o. declares that the radio equipment type MIDGE3 is in compliance with Directive 2014/53/EU.

FR

Le soussigné, RACOM s.r.o., déclare que l'équipement radioélectrique du type MIDGE3 est conforme à la directive 2014/53/UE.

HR

RACOM s.r.o. ovime izjavljuje da je radijska oprema tipa MIDGE3 u skladu s Direktivom 2014/53/EU.

IT

Il fabbricante, RACOM s.r.o., dichiara che il tipo di apparecchiatura radio MIDGE3 è conforme alla direttiva 2014/53/UE.

LV

Ar šo RACOM s.r.o. deklarē, ka radioiekārta MIDGE3 atbilst Direktīvai 2014/53/ES.

LT

Aš, RACOM s.r.o., patvirtinu, kad radijo įrenginių tipas MIDGE3 atitinka Direktyvą 2014/53/ES.

HU

RACOM s.r.o. igazolja, hogy a MIDGE3 típusú rádióberendezés megfelel a 2014/53/EU irányelvnek.

MT

B'dan, RACOM s.r.o., niddikjara li dan it-tip ta' tagħmir tar-radju MIDGE3 huwa konformi mad-Direttiva 2014/53/UE.

NL

Hierbij verklaar ik, RACOM s.r.o., dat het type radioapparatuur MIDGE3 conform is met Richtlijn 2014/53/EU.

PL

RACOM s.r.o. niniejszym oświadcza, że typ urządzenia radiowego MIDGE3 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 MIDGE3 está em conformidade com a Diretiva 2014/53/UE.

RO

Prin prezenta, RACOM s.r.o. declară că tipul de echipamente radio MIDGE3 este în conformitate cu Directiva 2014/53/UE.

SK

RACOM s.r.o. týmto vyhlasuje, že rádiové zariadenie typu MIDGE3 je v súlade so smernicou 2014/53/EÚ.

SL

RACOM s.r.o. potrjuje, da je tip radijske opreme MIDGE3 skladen z Direktivo 2014/53/EU.

FI

RACOM s.r.o. vakuuttaa, että radiolaitetyyppi MIDGE3 on direktiivin 2014/53/EU mukainen.

SV

Härmed försäkrar RACOM s.r.o. att denna typ av radioutrustning MIDGE3 överensstämmer med direktiv 2014/53/EU.

## 10.7. 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.

## 10.8. M!DGE3 maintenance

| Action  | Period      | Note   |
|---|-------------|--|
| <b>Visual check – Antenna:</b><br>Draining hole on dipole must be downward pointing<br>There should be no damaged elements on the antenna<br>Angle of elevation of antenna<br>Azimuth (angle of horizontal deviation) in accordance with design                           | Quarterly   |  |
| <b>Visual check – Coaxial Cable:</b><br>Mechanical damage<br>Solar degradation<br>Entire cable correctly mounted to surface<br>Connectors tightened to function optimally<br>Self-vulcanizing tape used for all connections requiring insulation<br>PSV & RF measurements | Annually    |  |
| <b>Visual check – Cabinet:</b><br>Mechanical damage<br>Damage resulting in lower categorization for cabinet coverage<br>Bushings for running cables   | Annually    |  |
| <b>Visual check – Electricity Supply:</b><br>Insulation damage<br>Connection to terminals   | Annually    |  |
| <b>Visual check – Accumulator:</b><br>Capacity in accordance with customer requirements<br>Condition of the accumulator   | Annually    |  |
| <b>Functionality check – power source:</b><br>Overcharging<br>Accumulator damage  | Annually    |  |
| <b>Full utilization</b> of provided protective coverings  | Annually    |  |
| <b>Remove</b> any items which are not part of the installation  | Annually    |  |
| <b>Fix</b> and secure makeshift installations correctly   | Annually    |  |
| <b>Check</b> grounding connections  | As required |  |
| <b>Check</b> lightning arrester : connectors must be tightened  | As required |  |
| <b>Check</b> data connectors connected including securing screws  | Annually    |  |
| <b>Evaluate</b> the signal strength values of the cellular connection as a preventive measure against the failure of the connection.  | Monthly     | <i>Section 8.5.4.3, "Cellular signal statistics"</i> |
| <b>Check</b> activity logs to detect abnormalities in data transmissions  | Monthly     | <i>Section 8.5.4.2, "Cellular state statistics"</i>  |

| <b>Action</b>   | <b>Period</b> | <b>Note</b>  |
|---|---------------|--|
| <b>Check</b> if internal temperature alarm has been triggered   | Monthly       | <i>Section 8.4, "Events"</i><br><i>Section 8.2.1, "Measurements"</i> |
| <b>Check</b> that firmware is latest stable version – upgrading FW recommended when new features required | As required   | <i>F i r m w a r e M!DGE3<sup>1</sup></i>                            |

If you are unsure on any of the above, please contact RACOM technical support.

---

<sup>1</sup> [https://www.racom.eu/eng/products/cellular-router-midge.html#dnl\\_fw3](https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fw3)

## Appendix A. Abbreviations

|                 |                                     |       |  |
|-----------------|-------------------------------------|-------|--|
| AES             | Advanced Encryption Standard        | MDIX  | Medium dependent interface crossover           |
| BER             | Bit Error Rate                      | MSE   | Mean Square Error                              |
| CLI             | Command Line Interface              | MIB   | Management Information Base                    |
| CRC             | Cyclic Redundancy Check             | NMS   | Network Management System                      |
| dBc             | decibel relative to the carrier     | N.C.  | Normally Closed                                |
| dB <sub>i</sub> | decibel relative to the isotropic   | N.O.  | Normally Open                                  |
| dBm             | decibel relative to the milliwat    | NTP   | Network Time Protocol                          |
| DCE             | Data Communication Equipment        | MRU   | Maximum Reception Unit                         |
| DHCP            | Dynamic Host Configuration Protocol | MTU   | Maximum Transmission Unit                      |
| DNS             | Domain Name Server                  | OS    | Operation System                               |
| DTE             | Data Terminal Equipment             | PC    | Personal Computer                              |
| EMC             | Electro-Magnetic Compatibility      | PER   | Packet Error Rate                              |
| FCC             | Federal Communications Commission   | PWR   | Power  |
| FEC             | Forward Error Correction            | RF    | Radio Frequency                                |
| FEP             | Front End Processor                 | RoHS  | Restriction of the use of Hazardous Substances |
| GPL             | General Public License              | RSS   | Received Signal Strength                       |
| HT-TPS          | Hypertext Transfer Protocol Secure  | RTS   | Request To Send                                |
| IP              | Internet Protocol                   | RTU   | Remote Terminal Unit                           |
| LAN             | Local Area Network                  | RX    | Receiver                                       |
| MAC             | Media Access Control                | SCADA | Supervisory control and data acquisition       |
|                 |                                     | SDR   | Software Defined Radio                         |
|                 |                                     | SNMP  | Simple Network Management Protocol             |



|      |   |
|------|---|
| TCP  | Transmission Control Protocol             |
| TS5  | Terminal server 5                         |
| TX   | Transmitter                               |
| UDP  | User Datagram Protocol                    |
| WEEE | Waste Electrical and Electronic Equipment |

## Revision History

### Revision

This manual was prepared to cover a specific version of firmware code. Accordingly, some screens and features may differ from the actual unit you are working with. While every reasonable effort has been made to ensure the accuracy of this publication, product improvements may also result in minor differences between the manual and the product shipped to you.

|   |            |
|---|------------|
| Revision 1.0<br>First issue                             | 2022-09-12 |
| Revision 1.01<br>General improvements                   | 2022-11-16 |
| Revision 1.01<br>Section Sleep mode added               | 2022-12-16 |
| Revision 1.02<br>Minor improvements of chapter SETTINGS | 2023-02-24 |
| Revision 1.03<br>Minor improvements of chapter SETTINGS | 2023-05-11 |
| Revision 1.04<br>Section <i>Credentials</i> added       | 2023-07-28 |