RACOM

User manual



RipEX2
Radio modem & Router

Quick start

Hardware

Configuration

Parameters

fw 2.3.6.0
2026-06-11
version 1.39

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

Table of Contents

Important Notice 7
1. Quick guide 8
    1.1. Bench testing 9
2. Product 11
    2.1. Dimensions 12
    2.2. Connectors 15
    2.3. Cellular interface 25
    2.4. Wi-Fi interface 26
    2.5. Indication LEDs 27
    2.6. Ordering codes 29
3. Accessories 32
4. Installation 33
    4.1. Step-by-step checklist 33
    4.2. Minimal required settings to set-up cellular connection 33
    4.3. Mounting 34
    4.4. Antenna installation 38
    4.5. Antenna feed line 39
    4.6. Grounding 39
    4.7. Full duplex operation 39
    4.8. Connectors 39
    4.9. Power supply 40
5. RipEX2 in detail 41
    5.1. Bridge mode 41
        5.1.1. Functionality example 42
        5.1.2. Configuration examples 44
        5.1.3. Point-to-Point Full duplex links 45
    5.2. Router mode 45
        5.2.1. Router - Base driven 46
        5.2.2. Router - Flexible 49
    5.3. Combination of IP and serial communication 53
        5.3.1. Detailed Description 53
6. Web interface 55
    6.1. Supported web browsers 57
    6.2. Changes to commit 58
    6.3. Notifications 60
    6.4. User menu 61
    6.5. Remote access 61
    6.6. Refresh settings 62
    6.7. Status info area 63
    6.8. Help 63
    6.9. Shortcuts 64
7. Settings 65
    7.1. Interfaces 65
        7.1.1. Ethernet 65
        7.1.2. Radio 70
        7.1.3. COM 85
        7.1.4. Terminal servers 110
        7.1.5. Cellular 112
        7.1.6. PPPoE client 121
        7.1.7. Wi-Fi 123
    7.2. Routing 127

7.2.1. Static 127
7.2.2. Link management 130
7.2.3. Babel 135
7.2.4. OSPF 148
7.2.5. BGP 155
7.3. Firewall 164
7.3.1. Firewall L2 164
7.3.2. Firewall L3 168
7.3.3. NAT - Network address translation 178
7.4. VPN 183
7.4.1. IPsec 184
7.4.2. GRE 194
7.4.3. OpenVPN 197
7.5. Security 208
7.5.1. Policy 211
7.5.2. Local authentication 212
7.5.3. Credentials 215
7.5.4. Management access 218
7.5.5. RADIUS 222
7.5.6. Tamper reset 224
7.6. Device 225
7.6.1. Unit 225
7.6.2. Configuration 233
7.6.3. Events 237
7.6.4. SW keys 239
7.6.5. Firmware 241
7.7. Services 249
7.7.1. Firmware distribution 249
7.7.2. DHCP servers 253
7.7.3. DNS 257
7.7.4. SNMP 262
7.7.5. Syslog 264
7.7.6. SMS 266
7.7.7. Hot standby 268
7.7.8. GNSS server 273
7.8. Advanced 273
8. Diagnostics 276
8.1. STATUS overview 276
8.2. Overview 277
8.2.1. Measurements 277
8.2.2. Statistics 278
8.3. Information 279
8.3.1. Interfaces 279
8.3.2. Routing 288
8.3.3. Firewall 288
8.3.4. Quality of service 291
8.3.5. DHCP servers 292
8.3.6. SNMP 292
8.3.7. Syslog 293
8.3.8. SMS 293
8.3.9. Device 294
8.3.10. Diagnostic package 296

8.4. Events 297
8.5. Statistics 299
8.5.1. Parameters 300
8.5.2. Radio interface statistics 301
8.5.3. Radio protocol statistics 302
8.5.4. Radio protocol non-addressable statistics 303
8.5.5. Radio signal statistics 304
8.5.6. Radio signal non-addressable statistics 305
8.5.7. Serial protocol statistics 305
8.5.8. Ethernet statistics 306
8.5.9. Cellular statistics 307
8.5.10. Wi-Fi statistics 311
8.5.11. Measurements 313
8.6. Monitoring 313
8.6.1. Settings 314
8.6.2. File output 322
8.6.3. Console output 323
8.7. Tools 323
8.7.1. ICMP ping 324
8.7.2. RSS ping 324
8.7.3. Routing 327
8.7.4. Logs 328
8.7.5. RF Transmission test 328
8.7.6. Antenna detection 329
8.7.7. System 331
8.8. Syslog 331
9. Technical parameters 333
9.1. Detailed radio channel parameters 345
9.2. Recommended MSE thresholds 363
10. Safety, regulations, warranty 364
10.1. Frequency 364
10.2. Safety distance 364
10.3. High temperature 365
10.4. Battery disposal 365
10.5. Explosive atmospheres 366
10.6. Instructions for Safe Operation of Equipment 370
10.7. SW license 370
10.8. EU Compliance 371
10.8.1. RoHS, WEEE and WFD 371
10.8.2. EU restrictions or requirements notice 372
10.8.3. EU Declaration of Conformity RED 373
10.9. Compliance Federal Communications Commission and Innovation, Science and Economic Development Canada 373
10.10. Compliance ANATEL Brasil 381
10.11. Country of origin 382
10.12. Warranty 382
10.12.1. EU Compliance 384
10.13. RipEX2 Availability and service life time 385
10.14. RipEX2 maintenance 386
A. Security Hardening Procedure 388
A.1. Password and accounting 388
A.2. Physical access 388

A.3. Encrypt data on Radio network 389
A.4. Encrypt data on cellular network 389
A.5. Disable Remote access or configure it securely 389
A.6. Exchange of certificates 390
A.7. Services 390
A.8. Firewall 391
A.9. HTTPS certificate 391
A.10. Backup files 392
A.11. Firmware 392
A.12. Secure disposal guidelines 393
A.12.1. Physical Removal and Asset Prep 393
A.12.2. Configuration Purge 393
A.12.3. Comprehensive Data Deletion (Total Purge) 393
A.12.4. Hardware Destruction (Non-Operational Units) 393
A.13. Known vulnerabilities and their mitigations 393
A.13.1. Blast-RADIUS 393
B. Proprietary UDP/TCP ports 394
Revision History 395

Important Notice

Copyright

© 2026 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 RipEX2 are used in an appropriate manner within a well-constructed network. RipEX2 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 RipEX2, or for the failure of RipEX2 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.
- Ⓔx The equipment should be used in hazardous locations under conditions according to *Section 10.5, “Explosive atmospheres”* only.

1. Quick guide

RipEX2 is a widely configurable compact radio modem, more precisely a radio IP 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.

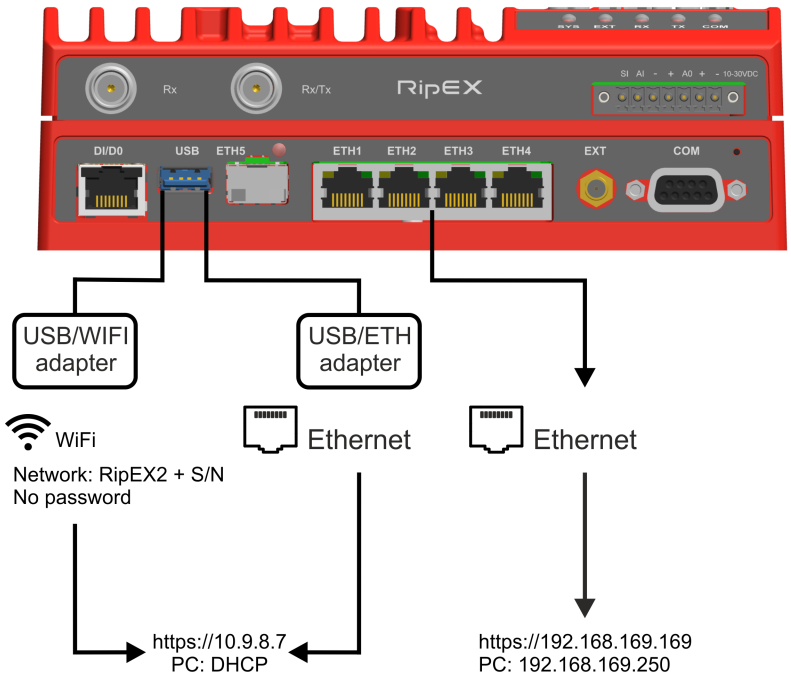


Fig. 1.1: Connecting RipEX2 to a PC over Wi-Fi, ETH/USB adapter, ETH interface

Unit has no Username and Password in default setting.

To configure RipEX2 you can connect it to your PC in three ways:

PC (tablet, smartphone) connected via Wi-Fi adapter

External Wi-Fi adapter (an optional accessory of the RipEX2 see *USB adapter*[1]) needs to be used. Any other adapter will not work correctly when connected to RipEX2 unit. Connect your PC, tablet or smartphone to RipEX2 Wi-Fi AP first. Its default SSID is RipEX2 S/N. By default, the WPA2 PSK is disabled, so no password is required. The Wi-Fi 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 RipEX2 unit, for access over the ETH/USB adapter, is 10.9.8.7.

PC connected via ETH/USB adapter

External ETH/USB adapter Part No. OTH-USB/ETH-XR (an optional accessory of the RipEX2 see *ETH/USB adapter*[2]). 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 RipEX2 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 to 192.168.169.0/24 (e.g.192.168.169.250, subnet mask 255.255.255.0).

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb
[2] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

Important

When you change the RipEX2 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 is used for the communication between the PC and RipEX2. The https protocol requires a security certificate. You must install this certificate into your web browser. The first time you connect to the RipEX2, your computer will ask you for authorisation to import the certificate into your computer. The certificate is signed by the certification authority RACOM s.r.o. 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.

Warning

Before you start any configuration, make sure only one unit is powered ON, otherwise a different radio modem could reply to your requests! (In default settings: all units share the same IP address and are in Bridge mode - which means, they can connect together over the air and create unwanted responds.)

Note

If you do not know unit IP address or password, you can reset the access parameters to defaults, see *Section 2.2.9, "HW button"*.

1.1. Bench testing

Before installing a RipEX2 network in the field, a bench-test should be performed in the lab. The RipEX2 Demo case is great for this as it contains everything necessary: 3× RipEX2 unit, Power supply, dummy load antennas, etc.
If you use your own installation for lab tests, do not forget:

- A dummy load or an actual antenna with 50 ohm impedance should be connected to the RipEX2
- Minimum RF output must be set to avoid overloading the dummy antenna and to keep the received signal at reasonable level, between -40 and -80 dBm.
- The power supplies must meet the requirements given in the specifications. Make sure the power supplies do not generate interference in the radio channel and that they can handle very fast changes in the load when RipEX2 switches from reception to transmission and back.
- Set radio parameters—including the radio protocol, channel width, and frequency—according to your radio frequency license.

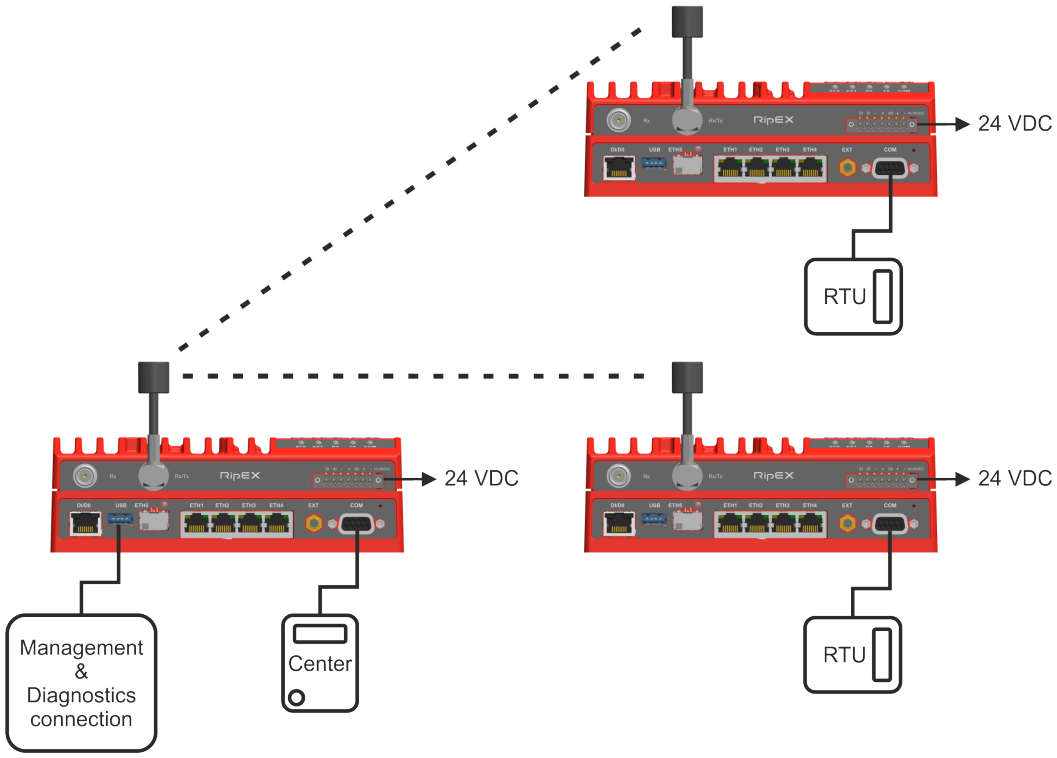
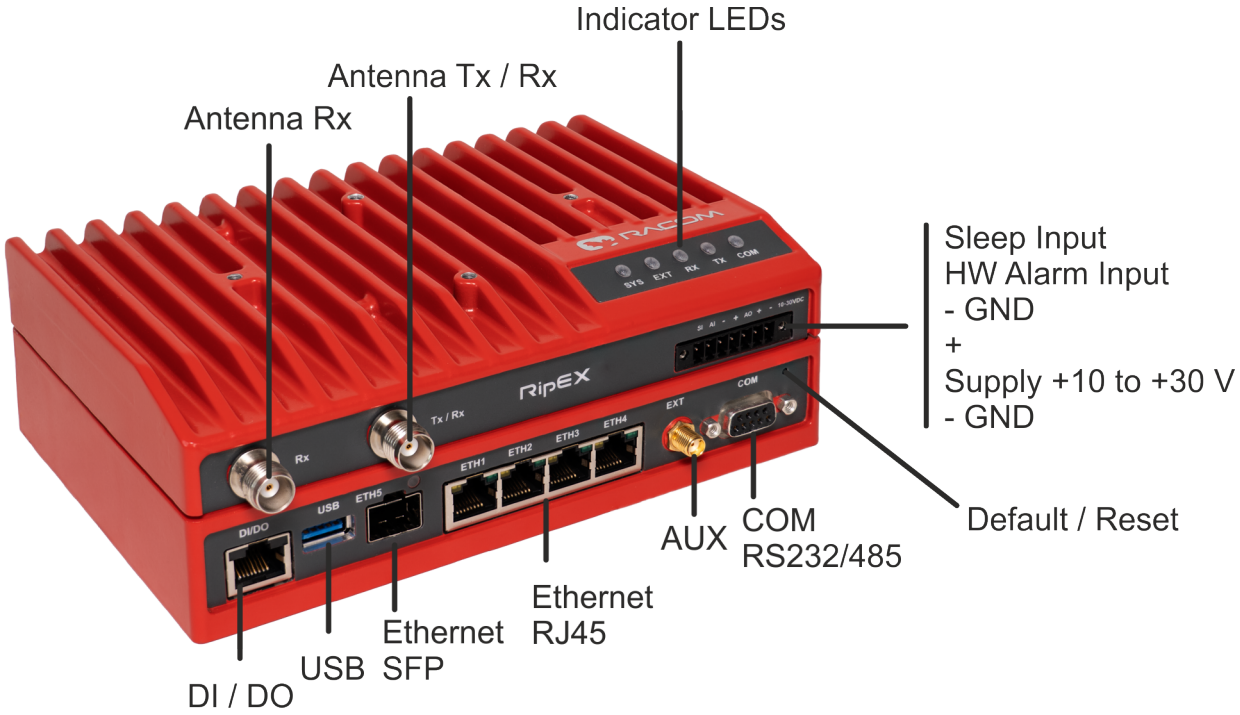


Fig. 1.2: RipEX2 bench testing

2. Product



RipEX2 is a radio modem platform renowned for overall data throughput in any real-time environment. RipEX2 radio modems are native IP devices, Software Defined with Linux OS that have been designed with attention to detail, performance and quality.

RipEX2 is built into a rugged die-cast aluminium casing that allows for multiple installation possibilities, see *Section 4.3, "Mounting"*.

Explosive atmospheres

DO NOT HANDLE UNLESS THE AREA IS KNOWN TO BE NON-HAZARDOUS

2.1. Dimensions

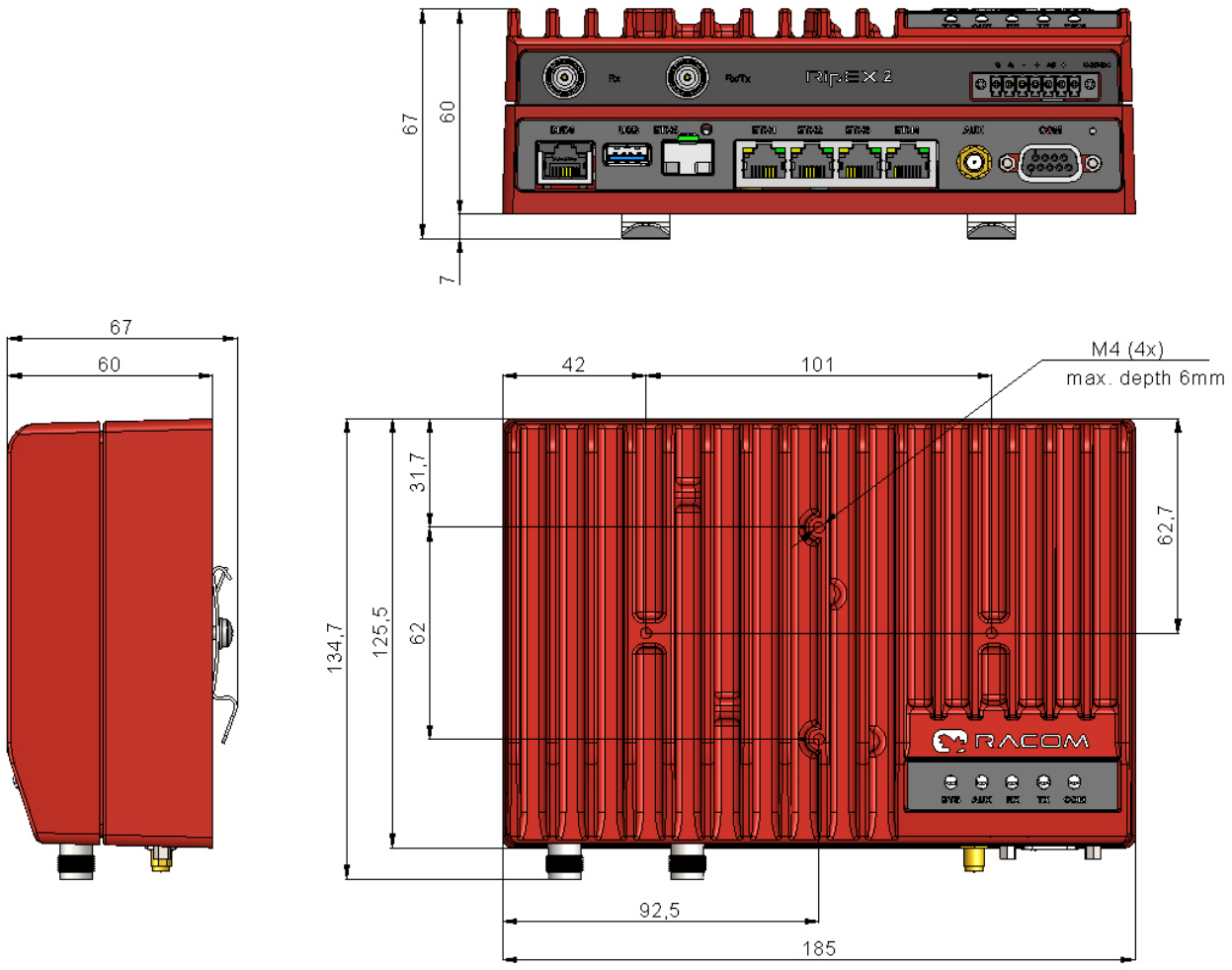


Fig. 2.1: RipEX2 dimensions

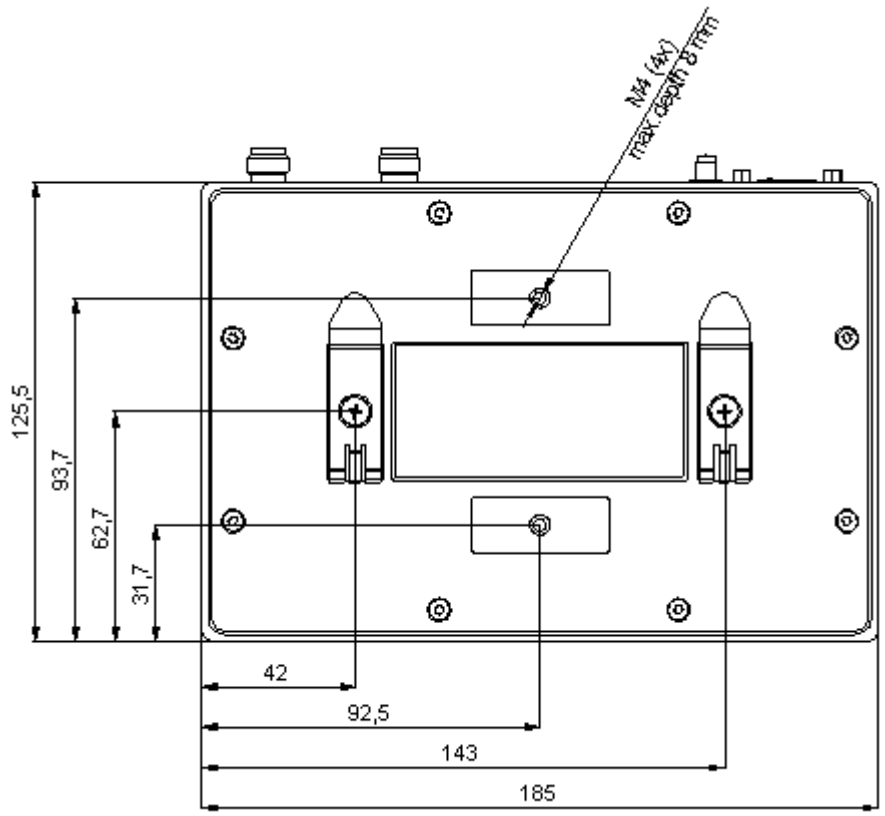


Fig. 2.2: RipEX2 dimensions – bottom

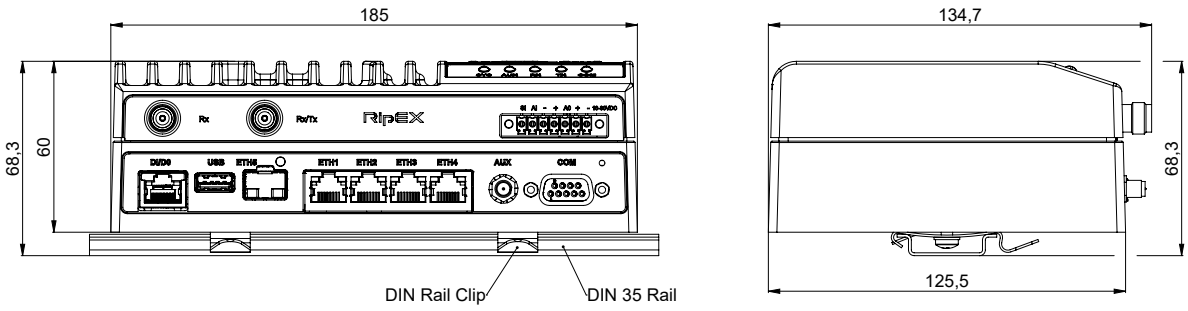


Fig. 2.3: RipEX2 with DIN rail

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

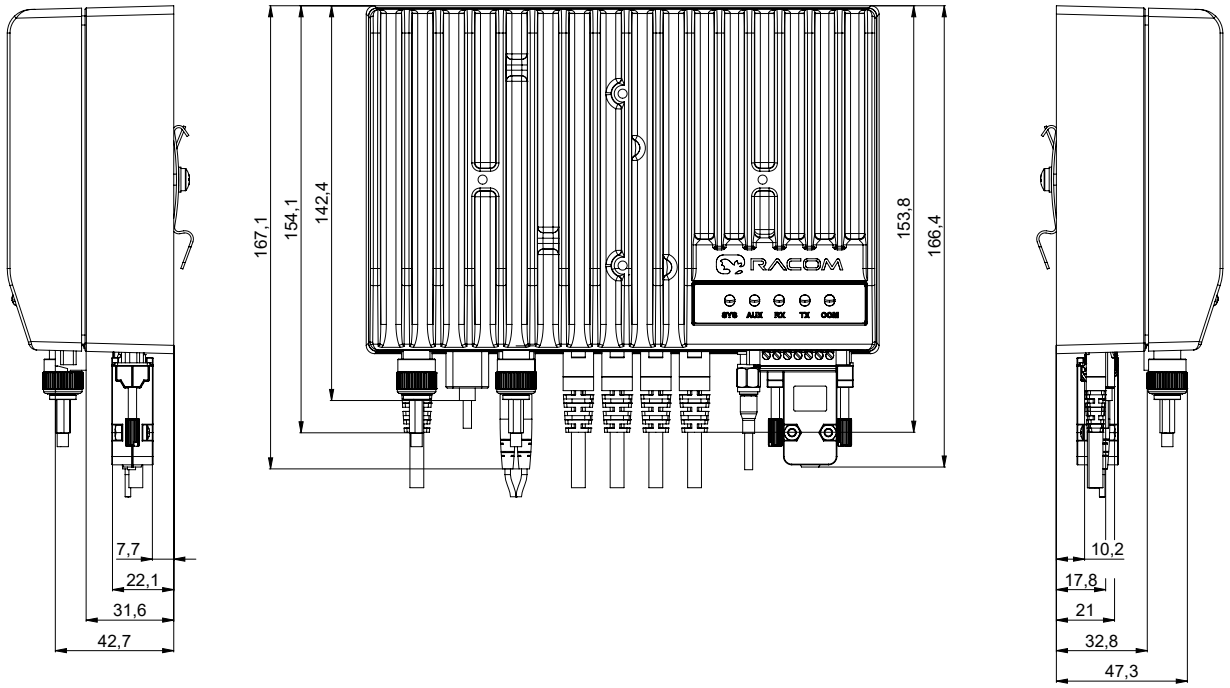


Fig. 2.4: RipEX2 dimensions with connectors

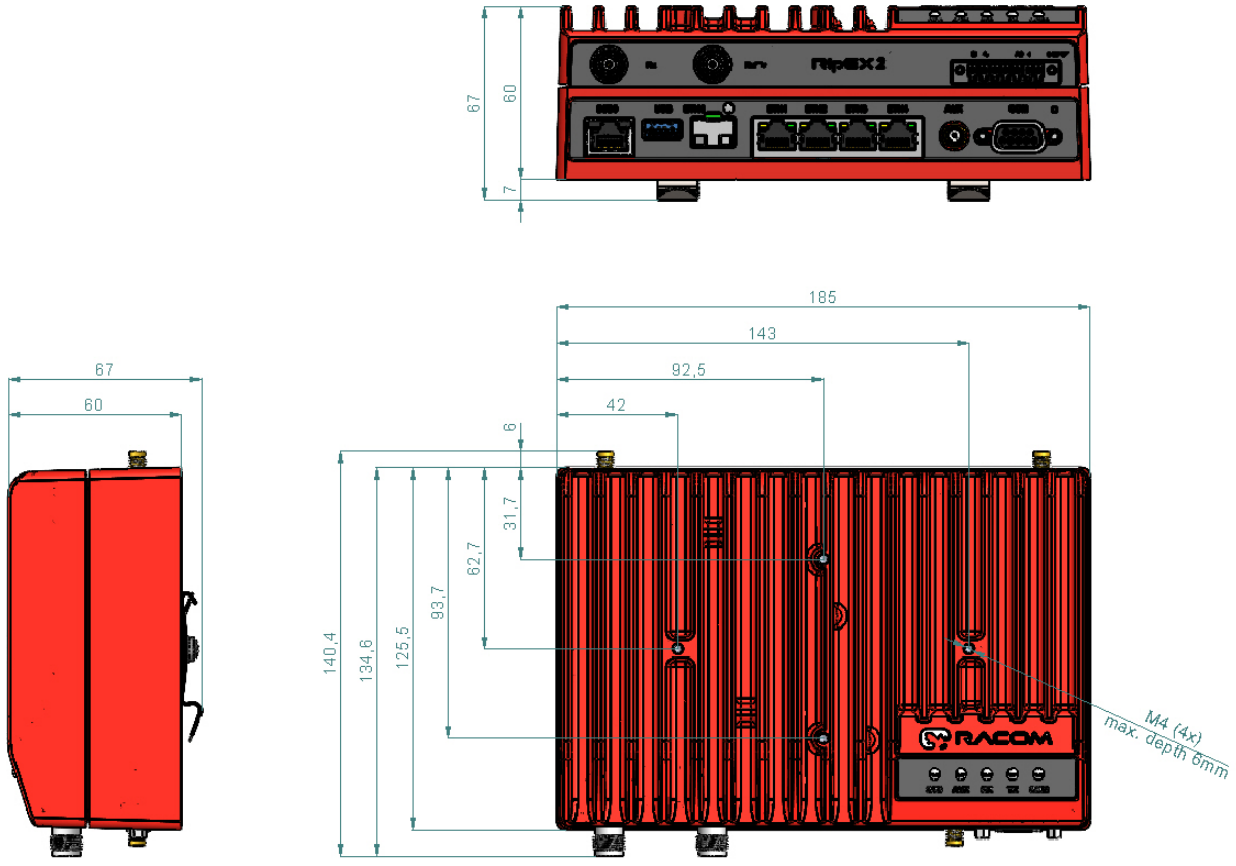


Fig. 2.5: RipEX2- with optional cellular interface dimensions

2.2. Connectors

All connectors are located on the front panel. The upper side features a LED panel. The HW button is located on the front panel as well (close to the COM1, 2 connector).

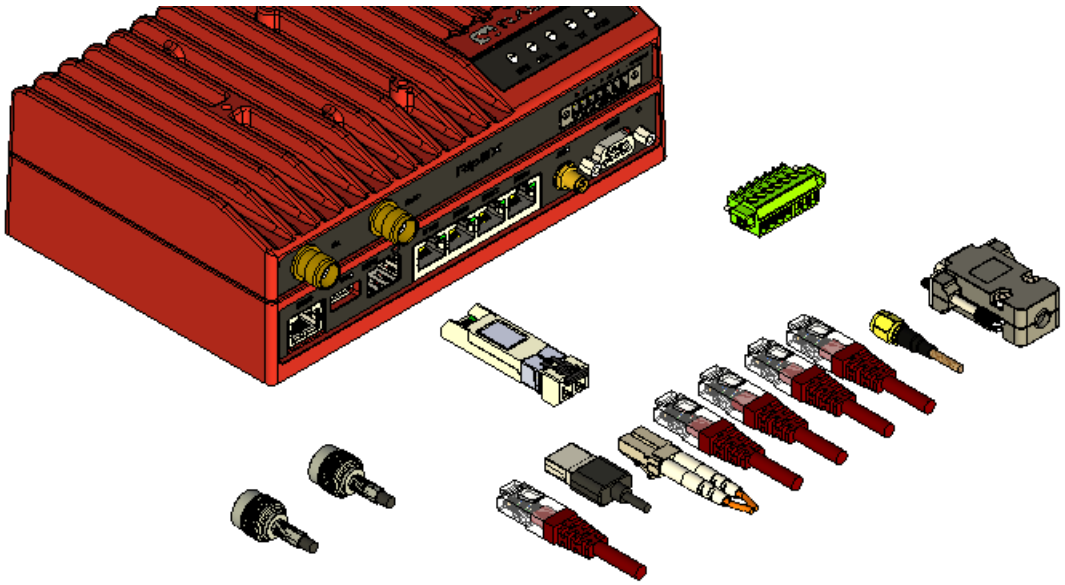


Fig. 2.6: Connectors

Explosive atmospheres

Do not manipulate the RipEX (e.g. plug or unplug connectors) unless powered down or the area is known to be non-hazardous.

2.2.1. Antenna

An antenna can be connected to RipEX2 via TNC female 50Ω connector.

RipEX2 is equipped with two connectors. The Tx/Rx connector will be used for common transmitting and receiving single antenna installation (even with different Rx and Tx frequencies).



Fig. 2.7: Antenna connectors

Both Rx and Tx/Rx connectors for split installation (separated Tx and Rx antennas or full duplex operation with duplexer) - Rx for receiving and Tx/Rx for transmitting.

Note

HW option RipEX2e (product variant ‘H' and 'J’) provides only Tx/Rx connector.

Warning

RipEX2 radio modem may be damaged when operated without an antenna or a dummy load.



Explosive atmospheres

Antenna has to be installed outside of the hazardous zone.

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 RipEX2. 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^2. 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 • pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis) • max. 30 VDC
2	AI	HW ALARM INPUT • pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis) • max. 30 VDC
3	−	−(GND) – for SLEEP IN, HW ALARM INPUT
4	+	+(POWER) – for HW ALARM OUTPUT
5	AO	HW ALARM OUTPUT open drain output max. 30 VDC, 1 A
6	+	+ POWER (10 to 30 V) Undervoltage threshold 8.5 VDC Overvoltage threshold 41 VDC
7	−	− POWER (GND)

Pins 3 and 7 are connected internally.
Pins 4 and 6 are connected internally.

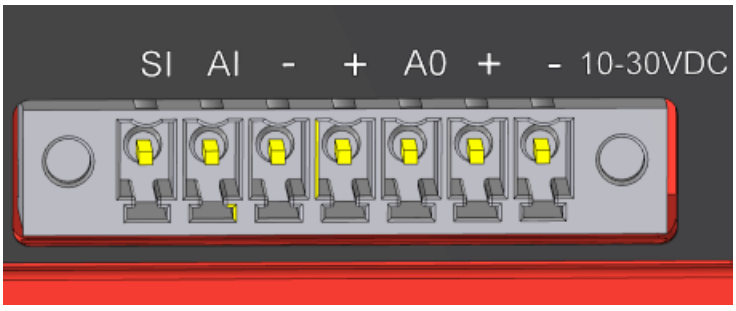


Fig. 2.8: Supply connector

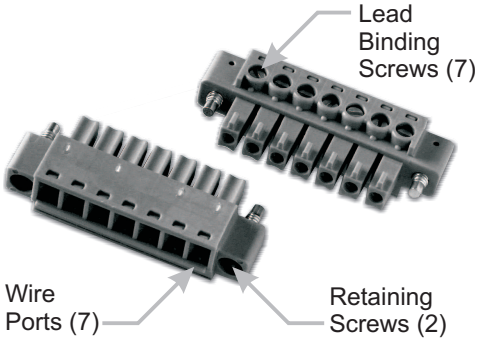


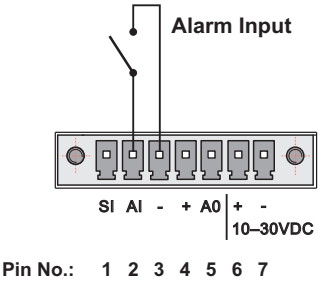
Fig. 2.9: Power and Control - cable plug

Explosive atmospheres

The unit must be powered with an intrinsic save power source for use in hazardous locations.

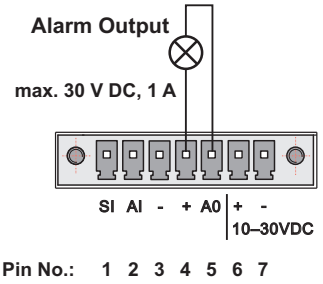
HW ALARM INPUT

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 10–30 VDC. The requirements for a power supply are defined in *Section 4.9, "Power supply"* and *Chapter 9, Technical parameters*.

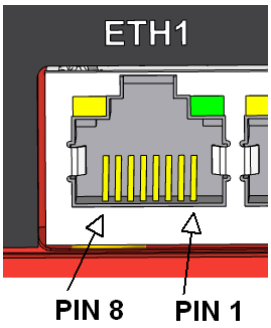
2.2.3. ETH1 - ETH4

Standard RJ45 connectors for Ethernet connection. RipEX2 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 RipEX2. RipEX2 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



Note

HW option RipEX2e (product variant ‘H' and 'J’) provides only ETH1 - ETH2 interfaces.

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 RipEX2 compatible as a standard accessory.

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.

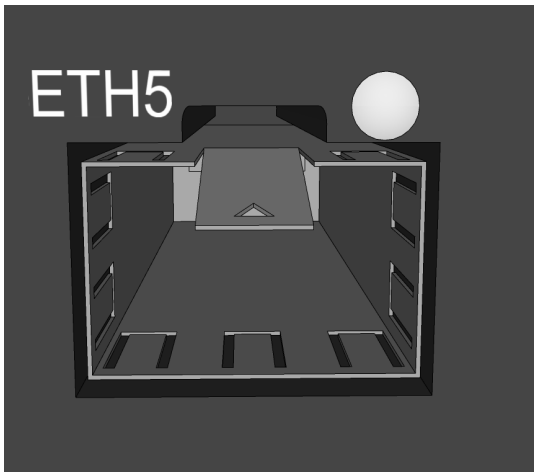


Fig. 2.10: SFP slot

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 RipEX2 units. It is possible to use any other SFP module, but RACOM cannot guarantee they will be completely compatible with RipEX2 units.

Note

HW option RipEX2e (product variant ‘H' and 'J’) does not provide ETH5 interface.

2.2.5. COM

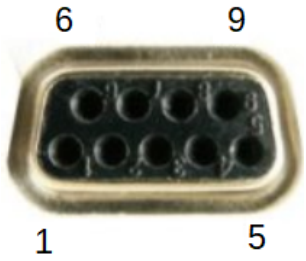
RipEX2 provides serial interface terminated by DSUB9F connector. RipEX2e and RipEX2 starting with version 'F' and 'O' provide two serial interfaces on the “COM” connector: COM1 and COM2. COM1 can be configured as RS232 or RS485. COM2 can only be used if COM1 is set to RS232 (not RS485).

RS232 of RipEX2 is a hard-wired DCE (Data Communication Equipment) device. Equipment connected to the serial port of RipEX2 unit should be DTE (Data Terminal Equipment) and a straight-through cable should be used. If a DCE device is connected to the serial port of RipEX2, a null modem adapter or cross cable has to be used.

RS485 of RipEX2 is not galvanic isolated and it is not terminated.

Tab. 2.3: COM pin description RipEX2 (except variant ‘F’ and ‘O’)

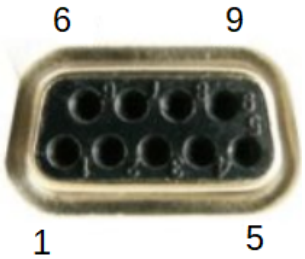
DSUB9F	COM – RS232		COM – RS485	
Pin	**Signal**	**In/ Out**	**Signal**	**In/ Out**
1	CD	Out	—	
2	RxD	Out	line B	In/Out
3	TxD	In	line A	In/Out
4	DTR	In	—	
5	GND		GND	
6	DSR	Out	—	
7	RTS	In	—	
8	CTS	Out	—	
9	RI	Out	—	



RipEX2 keeps pin 6 DSR at the level of 0 (state ON, approx. +6.2 V) by RS232 standard permanently.

Tab. 2.4: COM pin description RipEX2e and RipEX2 (variant ‘F’ and ‘O’)

DSUB9F	COM1 – RS232		COM1 – RS485		COM2 - RS232 (optional)	
Pin	**Signal**	**In/ Out**	**Signal**	**In/ Out**	**Signal**	**In/ Out**
1	CD	Out	—		—	
2	RxD	Out	line B	In/Out	—	
3	TxD	In	line A	In/Out	—	
4	—		—		TxD	In
5	GND		GND		GND	
6	—		—		RxD	Out
7	RTS	In	—		—	
8	CTS	Out	—		—	
9	RI	Out	—		—	



Extension module 'C' (2 × RS232)

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

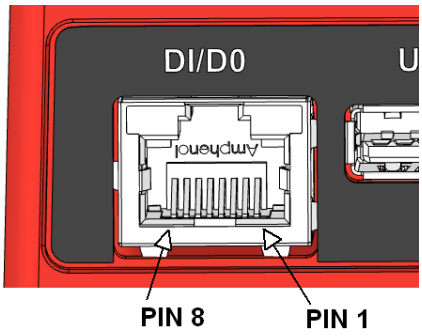
COM2 and COM3 parameters:

COM2: RS232 - 5 pin (RxD, TxD, GND, RTS, CTS) 300 b/s to 2 Mb/s

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

Tab. 2.5: DI, DO connector when 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



This interface is not compatible with RipEX2-HS.
If the RipEX2 unit is installed in the RipEX2-HS (Hot Standby chassis), the DI, DO interface is dedicated for the Hot standby operation.

Note

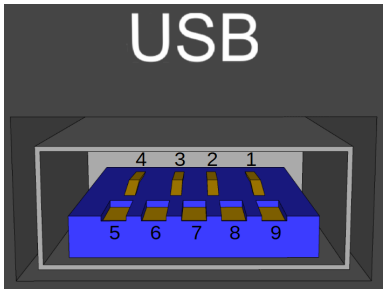
Extension module 'C' allows to expand the unit by two additional RS232 serial ports. In the current firmware version it is not supported on HW which already provides COM2 in the basic version (*Var. F and O.*).

2.2.6. USB

RipEX2 uses USB 3.0, Host A interface. USB interface is wired as standard:

Tab. 2.6: 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
9	StdA_SSTX+	Orange



Pin	Signal	Wire	
Shell	Shield	Connector Shell	

The USB interface is designed for the connection to an external ETH/USB adapter or a Wi-Fi adapter. They are optional accessories to RipEX2, for more details see *www/ripex/accessories*[1]. The adapters are used for service access to web configuration interface of RipEX2 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.

Explosive atmospheres

Only USB equipments dedicated for hazardous locations shall remain connected permanently.

2.2.7. EXT

EXT SMA female 50 Ohm connector is used for several purposes according to HW variant.

Standard basic model – the EXT is used as an synchronization signal input.

Input frequency range 1 Hz (PPS) - 25 MHz

Input signal level >200 mVp-p @ 220R, up to 5V TTL levels

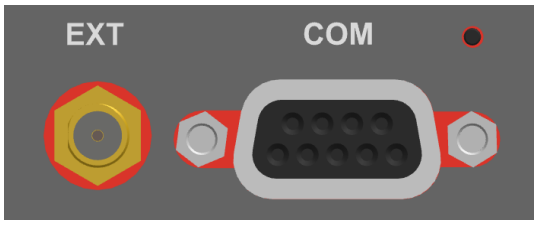


Fig. 2.11: EXT connector SMA

Time synchronisation from outer source will be implemented in future FW releases.

RipEX2 can be equipped with an internal G – Extension GPS (GNSS) module (*see details*). The GPS module is used for time synchronization of the NTP server inside RipEX2. In this case the EXT connector serves for connecting the GPS antenna:

- active antenna
- 3.3 VDC supply

Note

Interface AUX was renamed to EXT (FW version 2.0.13.0. and newer).

Note

For the RipEX2 version with narrowband LTE (cellular modules 'M' and 'O'), the EXT connector is used to connect the antenna.

Note

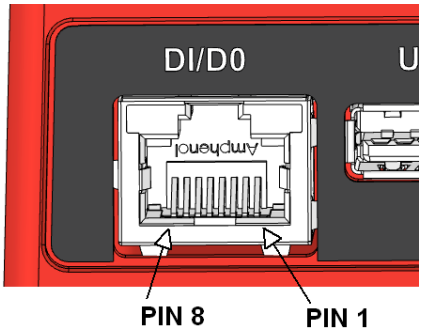
HW option RipEX2e (product variant ‘H' and 'J’) does not provide EXT interface.

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

2.2.8. DI, DO

Tab. 2.7: 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



Digital Outputs:

- Open drain output max. 30 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 30 V

Digital inputs:

- Schmitt-triggered inverted input
- Pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis)
- Max. 30 VDC

If the RipEX2 unit is installed in the RipEX2-HS (Hot Standby chassis), the DI, DO interface is dedicated for the Hot standby operation.

Note

HW option RipEX2e (product variant ‘H' and 'J’) does not provide DI, DO interface.

Note

These Digital Inputs and Outputs cannot be used if the unit is equipped with the 'C' Expansion module providing additional serial ports.

2.2.9. HW button

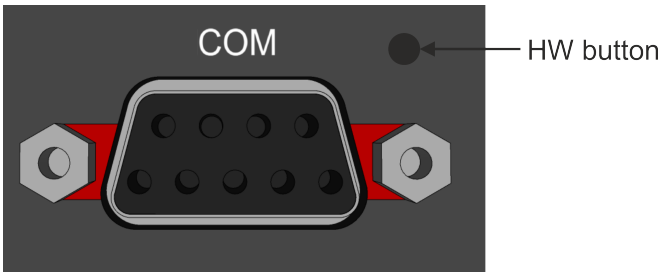


Fig. 2.12: HW button

HW button is placed on the right side of COM interface.

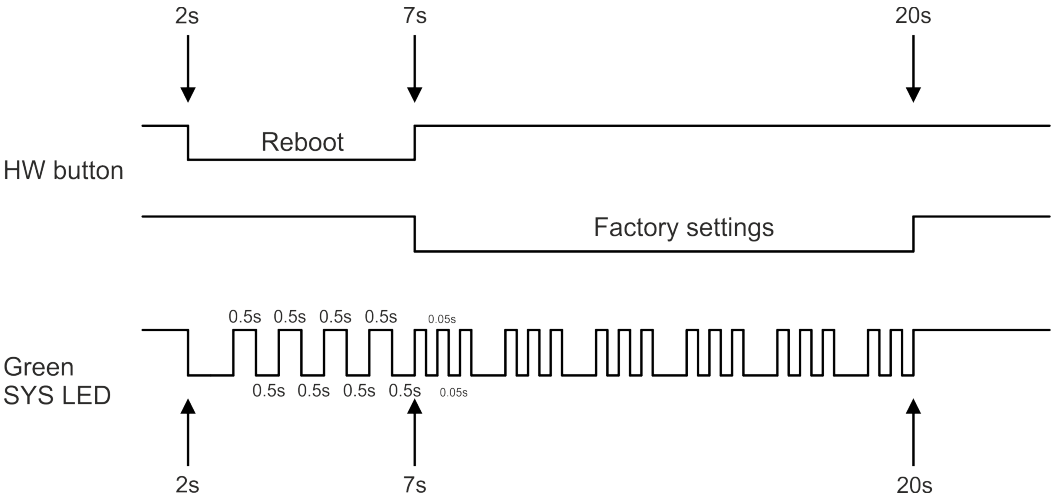


Fig. 2.13: HW button scheme

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

2.3. Cellular interface

RipEX2 radio modem can be delivered with the cellular extension.

2.3.1. Antenna

RipEX2 radio modem equipped with the LTE cellular module has two additional SMA antenna connectors mounted on the opposite side than radio antenna connectors.



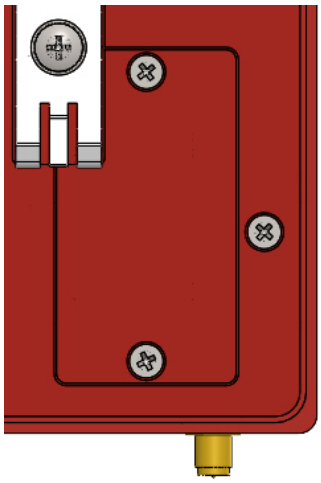
It is recommended to use both antennas (Rx diversity) for the LTE connection. In case of using only one antenna, attach it to the EXT1 connector. The EXT1 connector is used for both transmitting and receiving, or for single-antenna setups. The EXT2 connector is specifically for Rx diversity.

Note

For the RipEX2 version with narrowband LTE (cellular modules 'M' and 'O'), the EXT connector is used to connect the antenna.

2.3.2. SIM cards

Two SIM card holders for Micro SIM (3FF) are available under the screwed cover on the RipEX2 bottom side.



Warning

Disconnect RipEX2 unit from a power supply before opening the cover and manipulating with SIM cards.

2.4. Wi-Fi interface

RipEX2 radio modem can be delivered with the Wi-Fi extension.

2.4.1. Antenna

RipEX2 radio modem equipped with the Wi-Fi module has two additional SMA antenna connectors mounted on the opposite side than radio antenna connectors. See *chapter 2.3.1* for the corresponding picture of the antenna connectors.

It is possible to use either one or two antennas. Antenna configuration needs to be setup accordingly in the EXT1 and EXT2 antenna configuration parameters in the Settings > Interfaces > Wi-Fi menu.

2.5. Indication LEDs

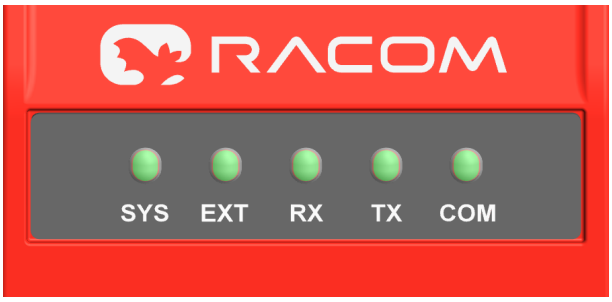


Fig. 2.14: Indication LEDs

Tab. 2.8: Key to LEDs

LED	Colour	Status	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
		Flashing regularly - period 2000 ms	Sleep mode activated
	Red	Permanently lit	Alarm
		Flashing regularly - period 500 ms	Serious system error
	Orange	Permanently lit	Unit booting
		Three fast (75 ms) flashes	USB flash disc inserted
		Flashing fast (75ms) - period 1000 ms	Interaction with USB flash disc
	Green / Orange	Flashing regularly - period 300 ms	FW activation - do not shut down the device
EXT	Green	Permanently lit	Activity of mPCIe connected equipment (like GPS fix, LTE connected, ...)
	Red	Permanently lit	Alarm of mPCIe connected equipment
	Table of Signal levels for individual services for cellular interface		
	Table of GNSS activity		
Rx	Green	Permanently lit	Receiver is synchronized to a packet
	Yellow	Permanently lit, or flashing in 1 sec intervals	Rx mode of operation - High resiliance (strong interfering signals - above -45 dBm - are present within the frequency band)
Tx	Red	Permanently lit	Transmitting to radio channel
COM1 ,2	Green	Permanently lit	Data receiving
	Yellow	Permanently lit	Data transmitting

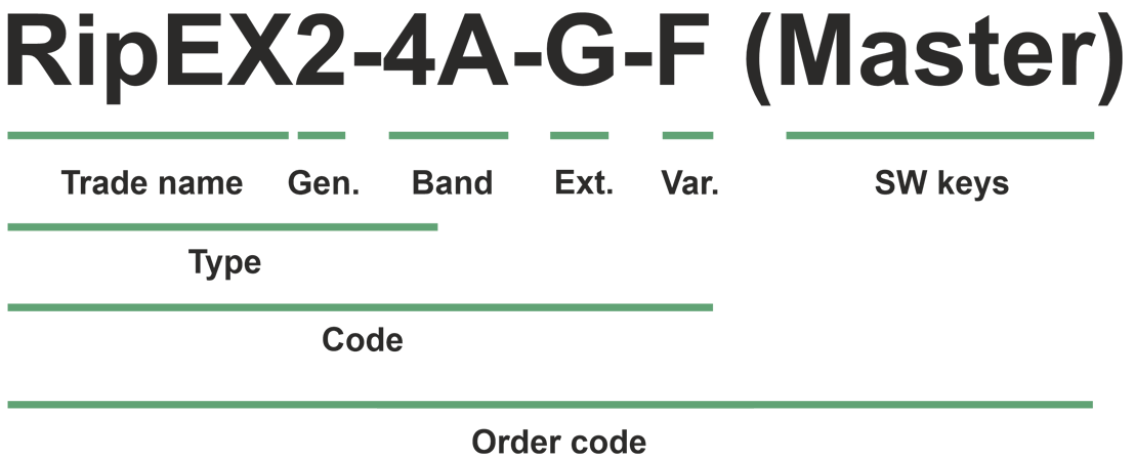
Alarm

An Alarm is triggered by any event with severity Error or higher (see *Section 8.4, “Events”*).

High resilience mode

LED signalization of receiver High resilience mode can be enabled/disabled by configuration item ADVANCED > Interfaces > Radio > Radio parameters > High resilience LED indication (see *Section 7.1.2.8.2, “Radio channel - advanced ”* for details).

2.6. Ordering codes



Trade name – trade and marketing name of the product. This name is used for all products within the same product family.
Possible values: **RipEX**

Gen. – generation of the product of specific Trade name. The very first generation does not have any number in this position.
Possible values: **none, 2**

Band – frequency band and sub-band
Possible values:
1A: 135–175 MHz
2A: 215–240 MHz
3A: 285–335 MHz
3B: 335–400 MHz
4A: 400–470 MHz
4B: 450–520 MHz
8A: 803–897 MHz
9A: 860–960 MHz

Ext. – Extension module embedded in mPCIe slot. The module cannot be changed later on.
Possible values:
N – not used (the only option for RipEX2e)
W – Extension cellular module; Part No.: mPCIe-W
Bands W - 4G/3G/2G, Global
R – Extension cellular module; Part No.: mPCIe-R
Bands R – LTE Cat M1/NB1/NB2, LatAm, Europe (incl. 410 MHz, 450 MHz)
S – Extension cellular module; Part No.: mPCIe-S
Bands S – LTE Cat M1/NB1/NB2, Global
G – Extension GPS (GNSS) module; Part No.: mPCIe-GPS
F – Extension Wi-Fi module; Part No.: mPCIe-WIFI

Note

Only one option for mPCIe slot is possible

Legacy values:
E – Extension cellular module E; Part No.: mPCIe-E.
P – Extension cellular module P; Part No.: mPCIe-P.
A – Extension cellular module A; Part No.: mPCIe-A.
M – Extension cellular module M Part No.: mPCIe-M.
O – Extension cellular module O; Part No.: mPCIe-O.
C – Extension module 2× RS232; Part No.: mPCIe-COMS.

Var. – designation of product variant. This variant is fixed in unit HW and cannot be changed later on.
Possible values:
F – RipEX2, Data encryption possible. COM2 available. Directly succeeds 'E' version.
H – RipEX2e (essential version), Data encryption possible. COM2 available.
J – RipEX2e (essential version), Data encryption never possible (AES256, IPsec, OpenVPN never possible). COM2 available.
O – RipEX2, Data encryption never possible (AES256, IPsec, OpenVPN never possible). COM2 available. Directly succeeds 'N' version.

Legacy values:
C – RipEX2e, processor without HW encryption support. Discontinued from 8/2023
D – RipEX2e, processor without HW encryption support. Encryption features will never be possible. Discontinued from 8/2023
E – RipEX2, Data encryption possible. Discontinued from 8/2024
N – RipEX2, Data encryption never possible (AES256, IPsec, OpenVPN never possible). Discontinued from 8/2024
X*– RipEX2, processor with HW encryption support. Discontinued from 12/2022

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 (subject to availability of a respective SW feature with a particular HW configuration):
Master – enables all functionalities of all possible SW feature keys, excl. Ex; Part No.: RipEX2-SW-MASTER, RipEX2e-SW-MASTER
Protocols – enables Radio protocols (Flexible, Base driven); Part No.: RipEX2-SW-PROTOCOLS
Dynamic routing – enables Dynamic routing (Babel, OSPF, BGP, Link management, PPPoE); Part No.: RipEX2-SW-DYNAMIC-ROUTING
Speed – enables 256QAM, ACM, Channels > 50kHz, Full duplex, RipEX2 only; Part No.: RipEX2-SW-SPEED
Power – enables RF power 40 dBm PEP; Part No.: RipEX2-SW-POWER
Security – enables IPsec, OpenVPN, RADIUS, Multiple users; Part No.: RipEX2-SW-SECURITY
SFP – enables SFP interface, RipEX2 only; Part No.: RipEX2-SW-SFP
COM2 – enables COM2 interface, RipEX2e, RipEX2 variant 'F' and 'O' only; Part No.: RipEX2-SW-COM2
Ex - authorization for use RipEX2 in hazardous location II 3G Ex ic IIA T4 Gc. Part No.: RipEX2-Ex (Note: Ex keys are available only for units produced after 1st of January 2022)

Region – used for countries where specific restrictions are required. Available only on special request when ordering. If used, it is indicated in bracket along with the SW keys.
Possible values:
US – USA, Allowed freq. according to FCC part 90
RipEX2 - 1A: 150.8 - 156.2475, 157.1875 - 161.575, 161.775 - 161.9625, 162.0375 - 170.0 MHz; Reg. ID: 1A-FCC_Part_90
RipEX2 - 4A: 4A: 406.1 - 454.0, 456 - 462.5375, 462.7375 - 467.5375, 467.7375 - 470.0 MHz; Reg. ID: 4A-FCC_Part_90

RU – Russia, Allowed freq. according to Russian regulations
RipEX2 - 1A: 146.0 - 174.0 MHz; Reg. ID: 1A-Russia
RipEX2 - 4A: 403.0 - 410.0, 433.0 - 450.0 MHz; Reg. ID: 4A-Russia
RipEX2 - 4A: 433.0 - 450.0 MHz; Adjusted product label; Reg. ID: 4-Russia
BR – Brazil, 6.25 kHz channel not allowed
RipEX2 - 4A: Additional sticker (Anatel 16763) on product and paper box; Reg. ID: 4A-Brazil
MX – Mexico, Additional sticker on product and paper box

Type – specific product type
Possible values:
RipEX2-1
RipEX2-3
RipEX2-4

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*[2].

* The processor included in the unit uses an encryption module listed as 5A002 a.1 in the Regulation (EU) 2021/821, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. Units are subject to export control when exporting outside the European union, according to national, EU and US law (ECCN 5A002 a.1), see *https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en*.
In the case of export from the country where the units were delivered by RACOM, the exporter must inform RACOM of the new country of delivery. X was under production until XII/2022

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

3. Accessories

Whole accessory list is available on *RACOM*[1] website.

1. **L-bracket**
   (see *https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting*

   L-bracket cannot be used if a cellular Extension module (any of W/E/P/A) is installed.

2. Flat-bracket
   (see https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting)[2]

3. RipEX2 Hot standby
   (see https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting)[3]

4. RipEX2-RD
   (see https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting)[4]

5. RipEX2-RS
   (see https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting)[5]

6. USB adapters (ETH, Wi-Fi)
   https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

   Note

   Wi-Fi adapter Part No.: OTH-USB/WIFI-W1, which was suitable for previous generation of RipEX does not work with RipEX2 units. Please use OTH-USB/WIFI-W2 adapter instead. Since FW 2.0.14.0 it is possible to use OTH-USB/WIFI-W3 adapter.

7. Demo case
   https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_democase

8. Ingress Protection IP52
   https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting

9. Dummy load antenna
   Dummy load antenna for RipEX2 is used to test the configuration on a desk. It is unsuitable for higher output – use transmitting output of 1.0 W only.

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories
[2] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting
[3] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting
[4] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting
[5] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting

4. Installation

4.1. Step-by-step checklist

1. Mount RipEX2 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 RipEX2.
7. Connect configuration PC (*Ripex2 "Connecting"*).
8. Configure RipEX2.
9. Test radio link quality (e.g. using Monitoring tool or RSS ping).
10. Connect the SCADA equipment.
11. Test your application.

Explosive atmospheres

The equipment should be used in hazardous locations under conditions according to *Section 10.5, “Explosive atmospheres”*.

4.2. Minimal required settings to set-up cellular connection

When cellular option is available

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*[1].

[1] mailto:support@racom.eu

4.3. Mounting

4.3.1. DIN rail mounting

The radio modem RipEX2 is directly mounted using clips to the DIN rail. The mounting can be done lengthwise (recommended) or widthwise; in both cases with the RipEX2 lying flat. The choice is made by mounting the clips, one M4 screw per clip. RipEX2 is delivered with two clips, two screws and four threaded holes. Use solely the M4×5 mm screws that are supplied.



Fig. 4.1: Flat lengthwise mounting to DIN rail – recommended

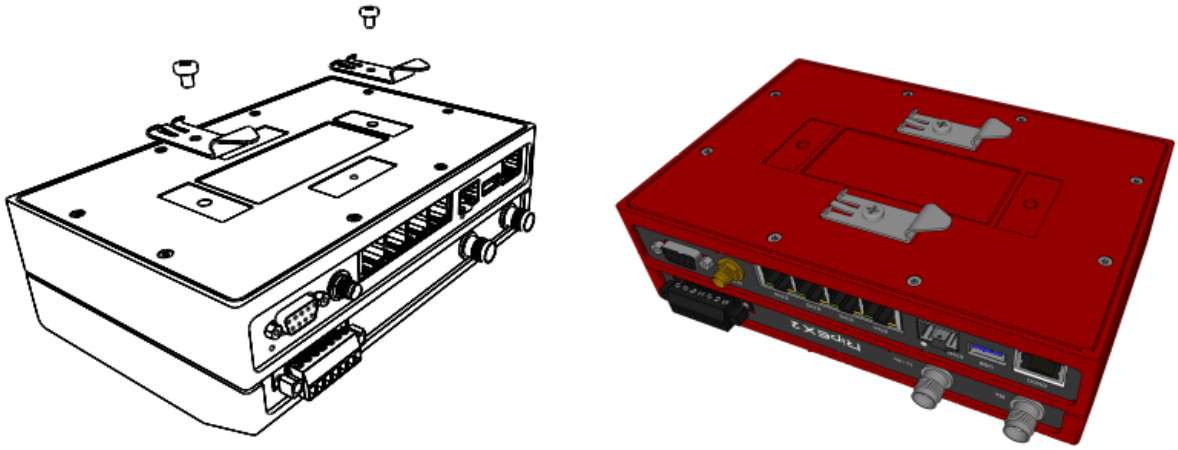


Fig. 4.2: Flat widthwise mounting to DIN rail

When tightening the screw on the clip, leave a 0.5 mm gap between the clip and the washer.

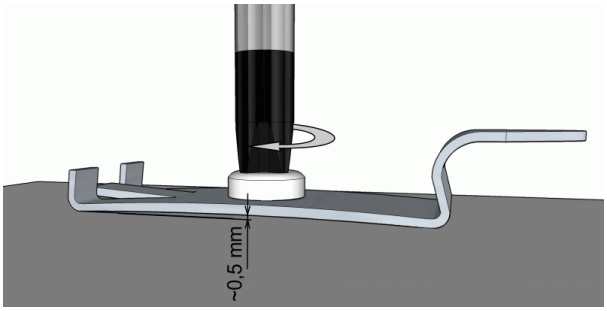


Fig. 4.3: Clip mounting

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

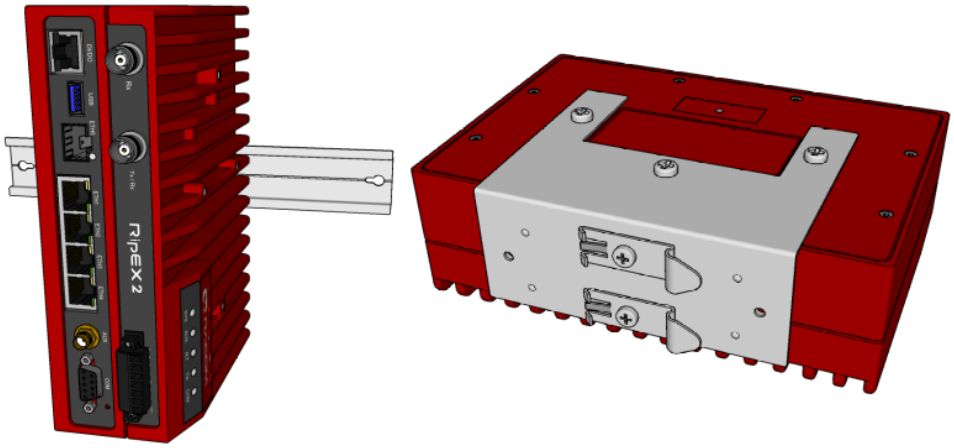


Fig. 4.4: Vertical widthwise mounting to DIN rail

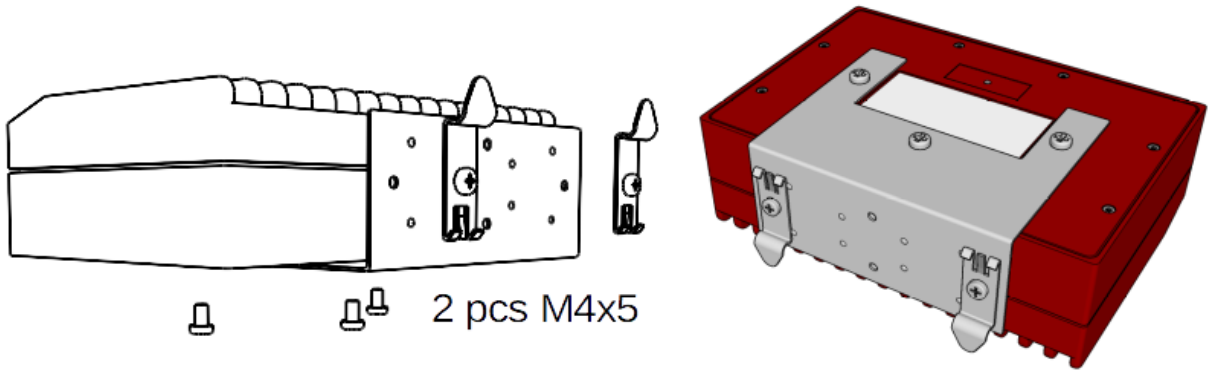


Fig. 4.5: Vertical lengthwise mounting to DIN rail

For more information see *L-bracket*[2].

[2] https://www.racom.eu/eng/products/radio-modem-ripex.html#HOL-RipEX-L

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; tighten with torque 0.9 Nm.

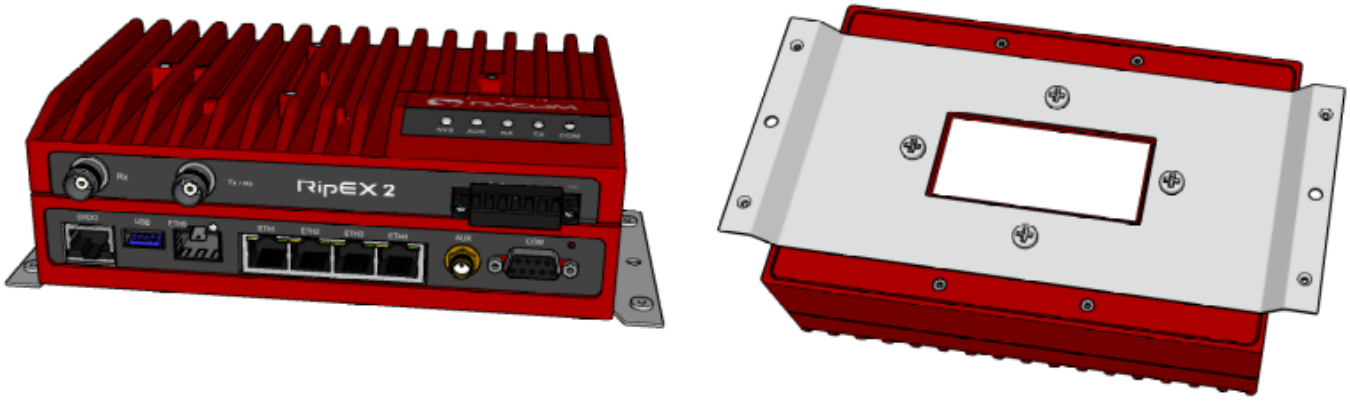


Fig. 4.6: Flat mounting using Flat bracket

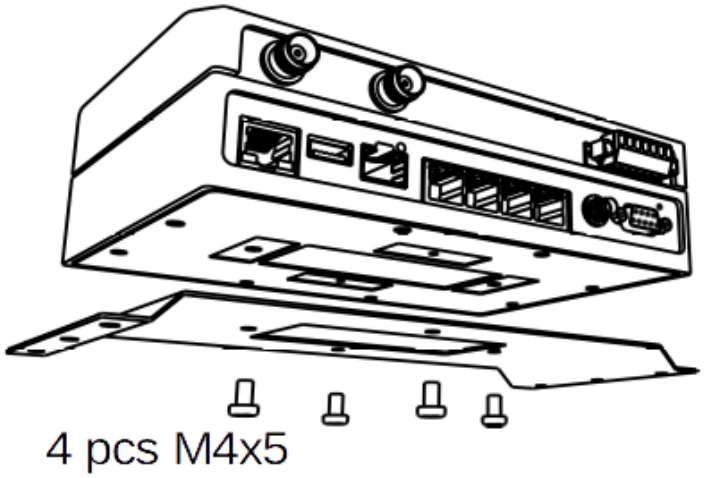


Fig. 4.7: Flat mounting using Flat bracket

For more information see *Flat-bracket*[3].

[3] https://www.racom.eu/eng/products/radio-modem-ripex.html#HOL-RipEX-FLAT

4.3.3. Full duplex mounting

The standard mounting for full-duplex operation is possible for surrounding temperatures bellow + 60 °C (see *Table 9.1, "Technical parameters"*), but it is recommended to use external passive cooler (e.g. installation in RipEX2-RS chassis) or keep the surrounding temperature bellow +35 °C for increasing of a long term reliability .

4.3.4. IP52 mounting

RipEX2 unit provides IP41 level of environmental protection. It is possible to reach higher level of protection IP52 (Limited dust ingress protection and protection from water spray < 15 degrees from vertical).

To obtain **IP5x protection**: plug in all connectors and cover unused ports (COM port does not need to be covered) with dust covers from the *SET-RipEX2-IP5x*[4].

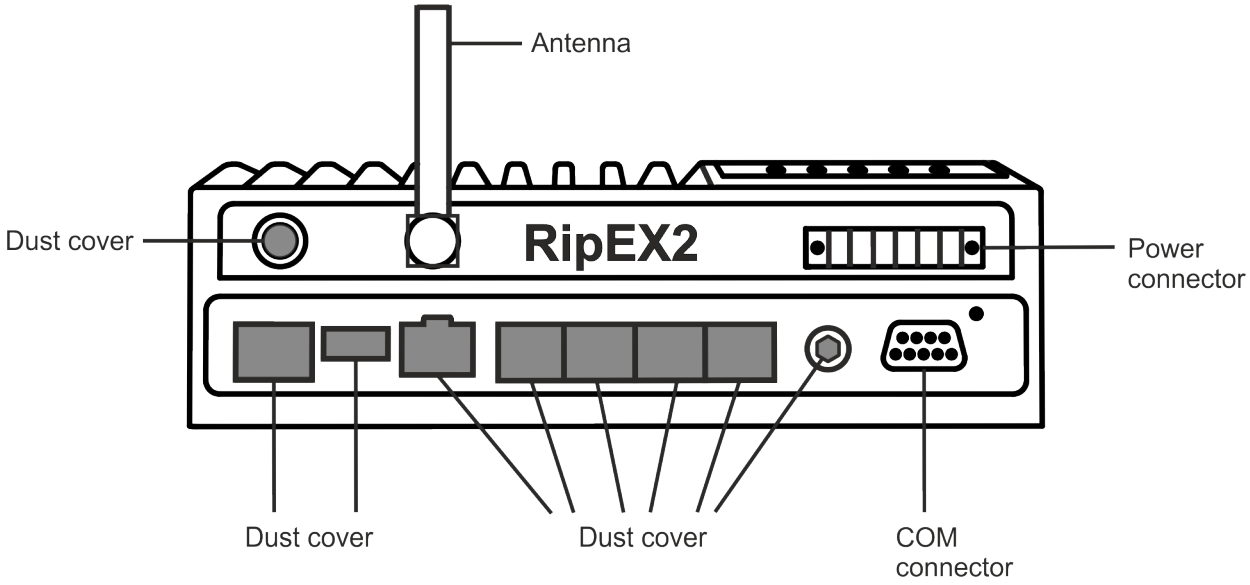


Fig. 4.8: IP5x protection

To obtain **IPx2 protection**: RipEX2 unit must be physically installed with the connectors facing downward.

[4] https://www.racom.eu/download/hw/ripex/free/eng/7_accessories/SET-RipEX2-IP5x.pdf

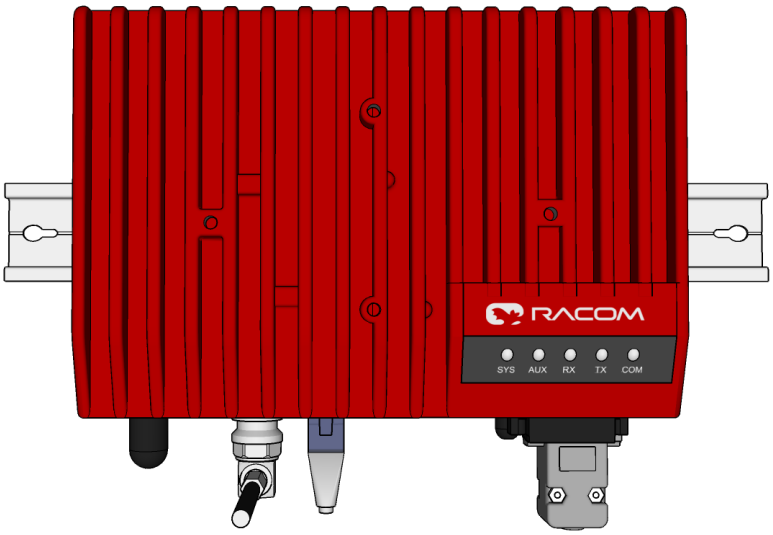


Fig. 4.9: IPx2 mounting

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. Proper network planning, including field signal measurements, should decide antenna types in the whole network. The plan will also determine what type of mast or pole should be used, where it should be located and where the antenna should be directed to.

The antenna pole or mast should be chosen with respect to the antenna dimensions and weight, to ensure adequate stability. Follow the antenna manufacturer's instructions during installation.

The antenna should never be installed close to potential sources of interference, especially electronic devices like computers or switching power supplies. A typical example of totally wrong placement is mount a whip antenna directly on top of the box containing all the industrial equipment which is supposed to communicate via RipEX2, including all 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.

Explosive atmospheres

Antenna has to be installed outside of the hazardous zone.

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 Ω impedance cables only.

The shorter the feed line, the better. If RipEX2 is installed close to antenna, the data cable can be replaced by an Ethernet cable for other protocols utilizing the serial port, see *Section 7.1.4, "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 RipEX2 radio modem is generally considered adequately grounded if the supplied flat mounting brackets are used to mount the radio modem to a properly grounded metal surface. If the radio modem is not mounted to a grounded surface, you should attach a safety ground wire to one of the mounting brackets or a screw on the radio modem's casing.

It is strongly recommended to install an appropriate lightning protection system where the antenna cable enters the building.



Note

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

4.7. Full duplex operation

When the Full duplex operation is required, the Tx and Rx signals must be separated. The level of Tx to Rx signal attenuation must be at least 70 dB or better. Such a high level of Tx to Rx signal attenuation is typically achived by using a duplexer. Separate installation of Tx and Rx antenna can be used instead of using a duplexer.

4.8. Connectors

RipEX2 uses standard connectors. Use only standard counterparts to these connectors.

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



Explosive atmospheres

Please note that connectors - or their individual pins - are connected to the housing. The housing is connected with the minus pin of the power connector.

4.9. Power supply

We do not recommend switching on power supply of the RipEX2 unit before connecting the antenna and other devices. Connecting the RTU and other devices to RipEX2 while powered increases the likelihood of damage due to the discharge of difference in electric potentials.

RipEX2 may be powered from any well-filtered 10 to 30 VDC power source. The supply must be capable of providing the required input for the projected RF output. The power supply must be sufficiently stable so that voltage doesn't drop when switching from receiving to transmission, which takes less than 1.5 ms. To avoid radio channel interference, the power supply must meet all relevant EMC standards. Never install a power supply close to the antenna. Connector is internally connected to the casing of the RipEX2 unit.

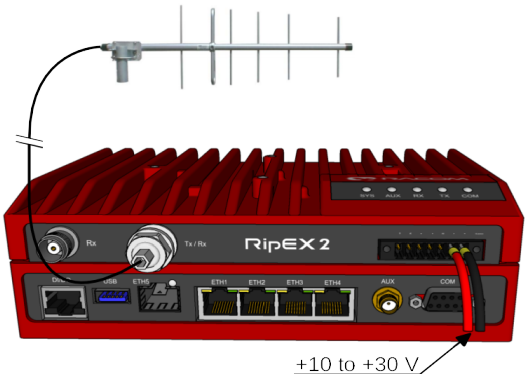


Fig. 4.10: 10–30 VDC Supplying

Explosive atmospheres

The unit must be powered with an intrinsic save power source for use in hazardous locations.

5. RipEX2 in detail

5.1. Bridge mode

Bridge mode enables transparent data transfer over the RipEX2 network. It is suitable for Point-to-Multipoint networks, where Master-Slave applications with polling-type communication protocol are used. The Bridge mode is suitable also for Point-to-Point links (both half and full duplex).

One of the advantages of the Bridge mode (together with Radio Transparent protocol) is its transparency. For example: both IPv4 and IPv6 type of traffic passes through; Frames defined by IEEE802.1Q-2018 are supported (e.g. VLAN, QinQ).

Bridge mode operation depends on the following system settings:

- Radio channel: Transparent protocol selected
- Ethernet ports: The Ethernet ports, intended to be used in Bridge mode, are grouped together in the Network interface (default name "bridge"), which is bridged with the Radio interface (parameter "Bridged with radio" enabled)
- COM ports: "Transparent protocol" selected

Radio channel

Transparent radio channel protocol does not solve collisions. There is a CRC check of data integrity to assure once a message is delivered, it is error free.

Ethernet ports

The whole radio network build from RipEX2 radio modems behaves as a standard Ethernet bridge. An Ethernet bridge ("Network interface" in RipEX2) automatically learns which devices (MAC addresses) are located in the local LAN and which devices are accessible over the radio channel. Consequently, only the Ethernet frames addressed to remote devices are physically transmitted over the radio channel. This arrangement saves the precious RF spectrum from extra load which would be otherwise generated by local traffic.

By default all Ethernet ports are bridged together with the Radio interface. It is possible to remove some Ethernet ports from this Network interface (having the Radio interface attached) to prevent unwanted traffic to enter the radio channel.

At least one Eth interface has to be bridged with the Radio

It is possible to form another Network interface(s). Any needed Ethernet traffic can be routed in between individual Network interfaces.

It is a good practice to detach one (or more) Ethernet port(s) from the main Network interface (described above) for other purpose than transparent data transfer. One typical example is: dedicated port for the unit management. It is very useful to use such a separated port for unit management, because there is no danger of transferring unwanted traffic (e.g. system updates or similar traffic) from the client PC over the radio channel. You can create another Network interface (e.g. called LAN-mgmt). Attach the previously detached ETH port and configure an IP address to be able to access the unit management.

COM port

The COM port needs to be Enabled and a Protocol needs to be selected to transfer any data. "Transparent" type of COM protocol is dedicated for Bridge mode purposes. This protocol transfers data between the COM port and the RipEX2 network transparently. Any other Protocol can be selected when needed.

When the "Transparent" protocol is selected, all frames received from the COM port are broadcasted over the radio channel and transmitted to all COM ports on all radio modems within the network. If the remote COM port is also configured for "Transparent" protocol, the received data are transparently transmitted over the COM port.

Terminal Servers

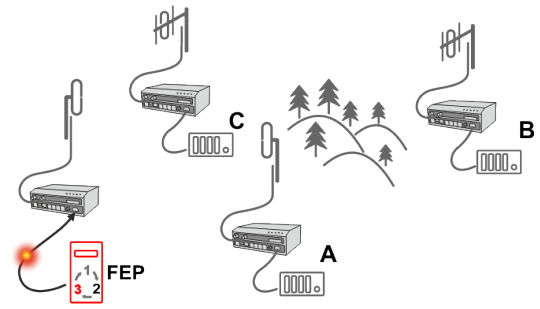
Behavior of Terminal Servers is similar to COM port. "Transparent" protocol needs to be selected when transparent data transfer to whole network (broadcasts) is needed. The other protocol types can be used for "Router mode" type of addressed communication.

5.1.1. Functionality example

In the following, common acronyms from SCADA systems are used:

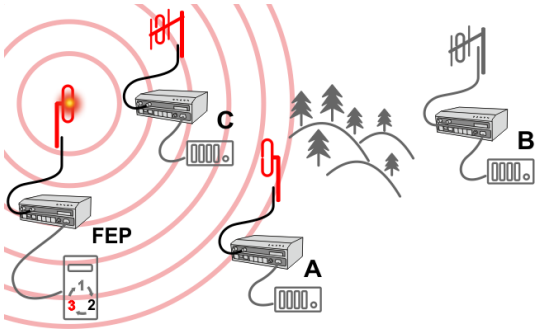
- FEP - Front End Processor, designates the communication interface equipment in the center
- RTU - Remote Telemetry Unit, the terminal SCADA equipment at remote sites

The single digits in illustrations are “site names” and do not necessarily correspond with actual addresses of both the RipEX2's and SCADA equipment. Address configuration examples are given in the *Section 5.1.2, “Configuration examples”*.



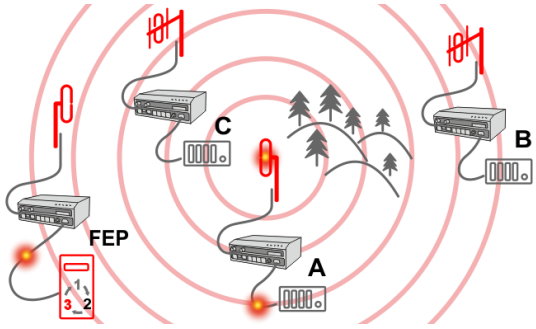
Step 1

Polling cycle starts:
FEP sends a request packet for RTU C through COM to the connected RipEX2.



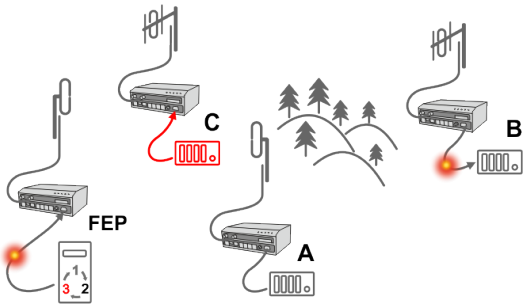
Step 2

RipEX2 FEP broadcasts this packet on Radio channel.
RipEX2 C and RipEX2 A receive this packet.
RipEX2 B does not receive this packet, because it is not within radio coverage of RipEX2 FEP .



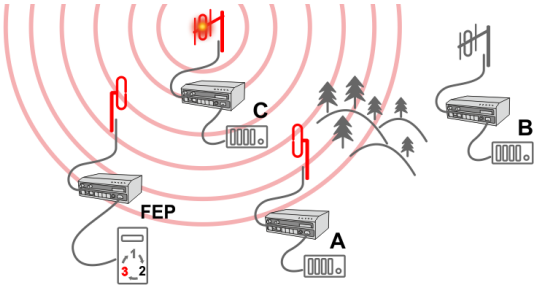
Step 3

RipEX2 C and RipEX2 A send the received packet to their COM ports.
Packet is addressed to RTU C, so only RTU C responds.
RipEX2 A is set as a repeater, so it retransmits the packet on Radio channel. Packet is received by all RipEX2 units.



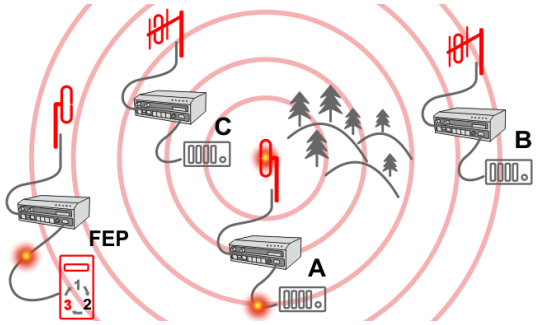
Step 4

RipEX2 B sends repeated packet to its COM.
RTU B does not react, because the packet is addressed to RTU C.
RipEX2 C and RipEX2 FEP **do not** send the repeated packet to their COM ports, because it has already been sent (RipEX2 C) or received (RipEX2 FEP) on their COM (anti-duplication mechanism).
RTU C sends the reply packet.



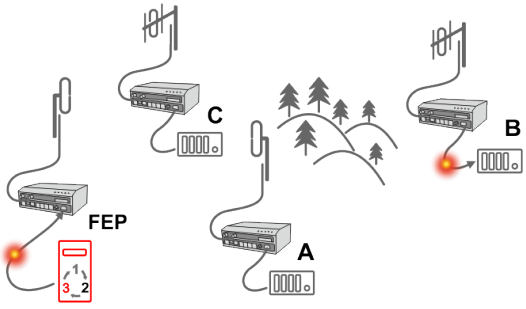
Step 5

RipEX2 C broadcasts the reply packet from RTU C on Radio channel.
Packet is received by RipEX2 A and RipEX2 FEP.



Step 6

RipEX2 FEP sends the packet (the reply from RTU C) to FEP through COM.
RipEX2 A sends this packet to RTU A. RTU A does not react, because the packet is addressed to FEP.
RipEX2 A repeats the packet on Radio channel.
All RipEX2 units receive the packet.



Step 7

RipEX2 B sends repeated packet to its COM.
RTU B does not react, because the packet is addressed to FEP.
RipEX2 C and RipEX2 FEP units **do not** send the repeated packet to their COM ports, because it has been handled already.
FEP processes the reply from RTU C and polling cycle continues…

5.1.2. Configuration examples

You can see an example of IP addresses of the SCADA equipment and RipEX2 ETH interfaces in the picture below.

In Bridge mode, the IP address of the ETH interface of RipEX2 is not relevant for user data communication. However it is strongly recommended to assign a unique IP address to each RipEX2 Network interface, since it allows for easy local as well as remote service access. Moreover, leaving all RipEX2 units with the same (= default) IP on the ETH interface may cause serious problems, when more RipEX2 units are connected to the same LAN, even if by accident (e.g. during maintenance).

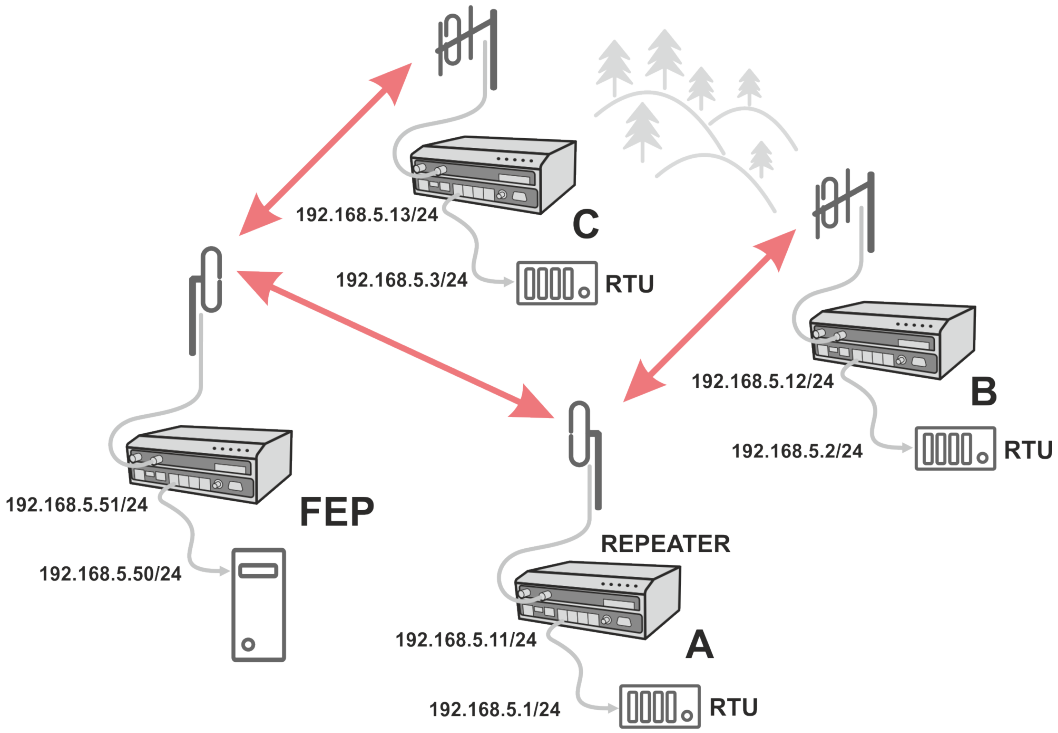


Fig. 5.1: Bridge mode example

Repeater

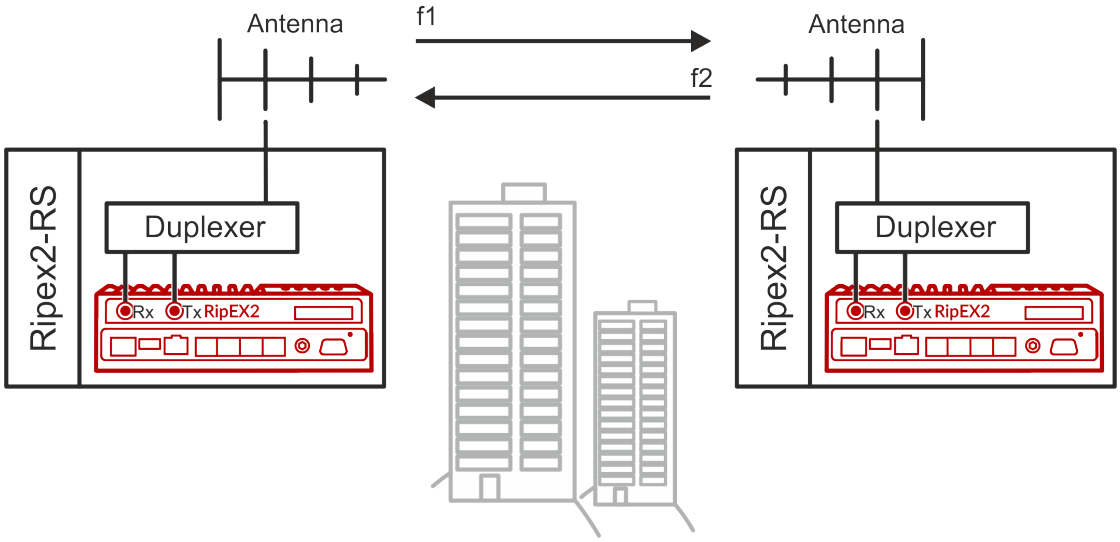
Because using the bridge mode makes the radio network transparent, the use of repeaters has certain limitations. To keep matters simple we recommend using a single repeater. However, if certain rules are observed, using multiple repeaters in the same network is possible.

The total number of repeaters in the network is configured for every unit individually under SETTINGS > Interfaces > Radio > Radio protocol parameters. This information is contained in every packet sent. All units that receive such packet will resume transmission only after sufficient time has been allowed for the packet to be repeated. The packets received from user ports remain buffered and are sent after the appropriate time passes. This prevents collisions between remote radio modems. There can be no repeater collisions if only one repeater is used.

Where two or more repeaters are used, collisions resulting from simultaneous reception of a repeated packet must be eliminated. Collisions happen because repeaters repeat packets immediately after reception, i.e. if two repeaters receive a packet from the center, they both relay it at the same time. If there is a radio modem which is within the range of both repeaters, it receives both repeated packets at the same time rendering them unreadable.

5.1.3. Point-to-Point Full duplex links

- To establish a PtP link it is recommended to use a Bridge mode. In context of PtP it has following advantages:
  - Simple configuration
  - Transparent data transfer (VLAN - single, double, tripple tagged; IPv6; MPLS; etc.)
  - Possibility of using Full duplex
  - Low latency
- In case of using Full duplex, it is required to:
  - Install a duplexer (exact type for a given channel link). A recommended duplex distance is 75 dB and more.
  - Due to high duty cycle, proper cooling is required. We recommend to use *RipEX2-RS*[1].



For more details see *RipEX2 PtP link tutorial video*[2].

5.2. Router mode

RipEX2 works as a standard IP router with multiple independent interfaces: Radio and Ethernets. Each interface has its own MAC address, IP address and mask.

IP packets are processed according to routing table rules. You can also set the router's default gateway (applies to both interfaces) in the routing table.

The COM ports are treated as standard host devices, messages can be delivered to them as UDP datagrams to selected port numbers. The destination IP address of a COM port is either the IP of an ETH or the IP of a radio interface.

[1] https://www.racom.eu/eng/products/m/ripex2-hs/product.html#rip2rs
[2] https://www.youtube.com/watch?v=Mg-ioFV0wDo&ab_channel=RACOMCompany

The additional Virtual COM ports and Terminal server can act as other IP router ports. This enables Serial and TCP based RTUs to be combined in one network.

Two different Radio protocols are available in the Router mode: Base driven and Flexible.

- Base driven
  This protocol is optimized for TCP/IP traffic and/or 'hidden' Remotes in report-by-exception networks, when a Remote is not be heard by other Remotes and/or different Rx and Tx frequencies are used. It is suitable for a star network topology with up to 255 Remotes under one Base station, where each Remote can simultaneously work as a Repeater for one or more additional Remotes.

- Flexible
  Suitable for master or even multi master-slave polling and report by exception from remotes concurrently. No limits in network design – each radio can work as base station, a repeater, a remote, or all of these simultaneously

5.2.1. Router - Base driven

All traffic over the Radio channel is managed by the Base station. Radio channel access is granted by a deterministic algorithm resulting in collision free operation regardless of the network load. Uniform distribution of Radio channel capacity among all Remotes creates stable response times with minimum jitter in the network.

All communication on Radio channel is controlled by the Base station; all frames inside the radio network have to be routed through the Base station. Appropriate routing has to be set.

Base station can communicate with the Remote stations using individual modulation and FEC settings.

Any Remote can work as a Repeater for another Remote. Only one Repeater is possible between the Base station and Remote, however a number of Remotes can use the same Repeater.

There is no need to set any routes in Routing table(s) for Remote stations located behind Repeater. Forwarding of frames from the Base station over the Repeater in either direction is provided transparently by the Base driven protocol.

When Remote to Remote communication is required, respective routes via the Base station must be set in Routing tables in the Remotes.

Frame acknowledgement, retransmissions and CRC check, guarantee data delivery and integrity even under harsh interference conditions on the Radio channel.

5.2.1.1. Router - Base driven, Functionality example

A star topology with one repeater is used in the following example of a SCADA network using a polling and report by exception combination. The Repeater is also serving as a Remote radio. The packets' acknowledgement on Radio channel is used in both directions in the example.

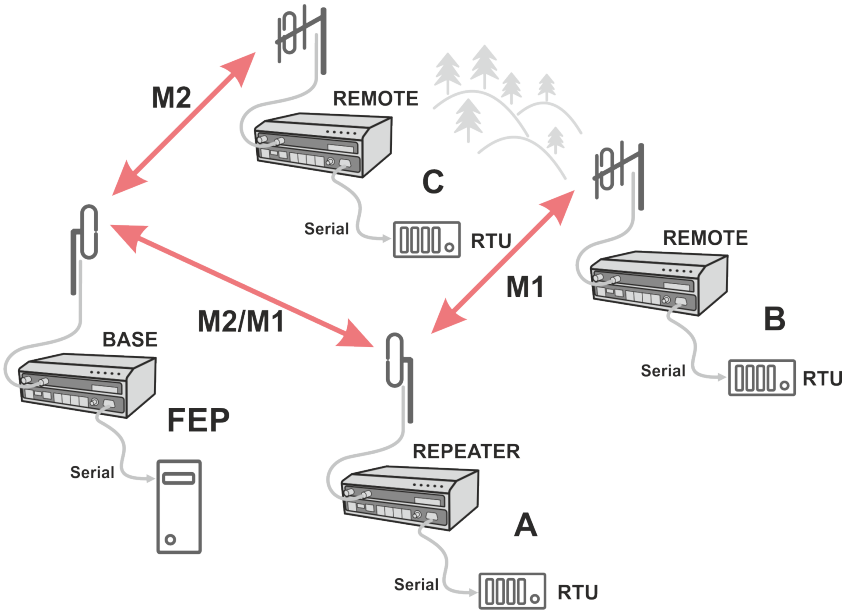


Fig. 5.2: Router - Base driven, Functionality example

Step 1
RipEX2 base station regularly checks the queue status of RipEX2 Remote stations for which it has no queueing information. The feedback enables the Base station to manage time allocations for all Remotes to transmit.

Step 2
FEP sends a request packet to RTU A via Base station; Base station transmits packet in shortest possible time. Remote station 1 receives the packet and hands it over to RTU A, simultaneously acknowledging packet receipt to the Base station.

Step 3
RTU A processes the request and sends the reply to Remote station 1. During the checking process the Base station detects a prepared packet in the queue of Remote station 1 and subsequently allots a Radio channel for transmission of the packet. Remote station 1 transmits the packet. If the Base station successfully receives the packet, it sends an acknowledgement and then the Remote station 1 clears the packet from the queue. A part of the relation includes a hand over of information about the number of packets waiting in the queue.

Step 4
RTU B is connected to Remote station 2 behind Repeater station 1, which manages all communication between the Base station and Remote station 2.

5.2.1.2. Router - Base driven, Configuration example

As already mentioned, RipEX2 works as a standard IP router with multiple independent interfaces: Radio and Ethernets. Each interface has its own MAC address, IP address and mask.
When Base driven protocol is used, Radio IP addresses for all RipEX2 units must share the same IP subnet.

The Base driven protocol routing table for each RipEX2 Remote station can be simplified to a default gateway route rule directed to RipEX2 Base station Radio IP. Only one record with respective IP address/mask combination for each remote station is needed in the Base station routing table.
The repeaters are not considered in routing in Base driven protocol. Each Remote station uses its own Radio IP address as a gateway in the routing table of the Base station.

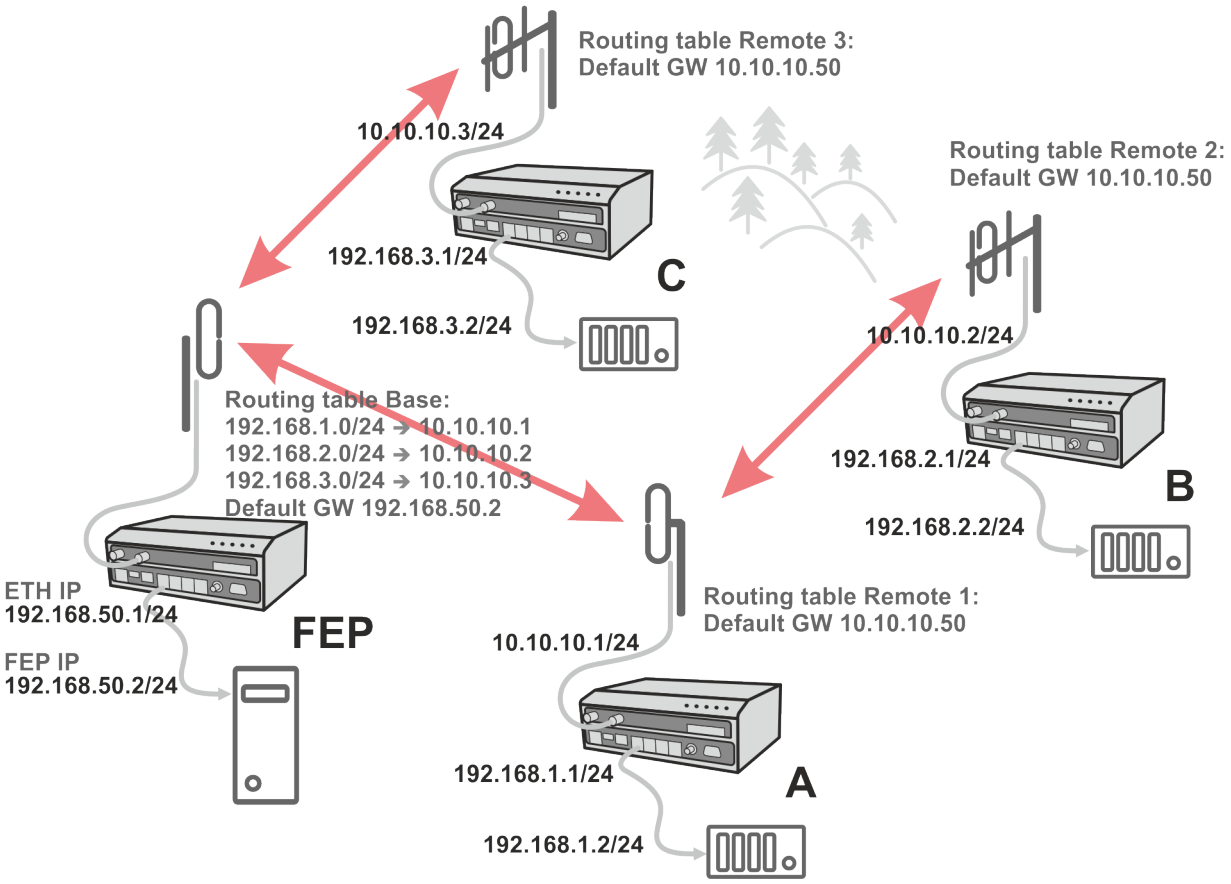


Fig. 5.3: Router - Base driven, Addressing

Important

For those accustomed to using the Flexible Radio protocol:
Settings for radios connected over a Repeater differ considerably in Base driven protocol.

Note

When only serial protocols are used, there is no need to use Routing tables. Instead of using Routing tables records, Address translation in COM protocol settings is used. Serial protocol address to IP address translation rules apply where the Radio IP addresses are used. Radio IP addresses will only be used for maintenance in such circumstances.

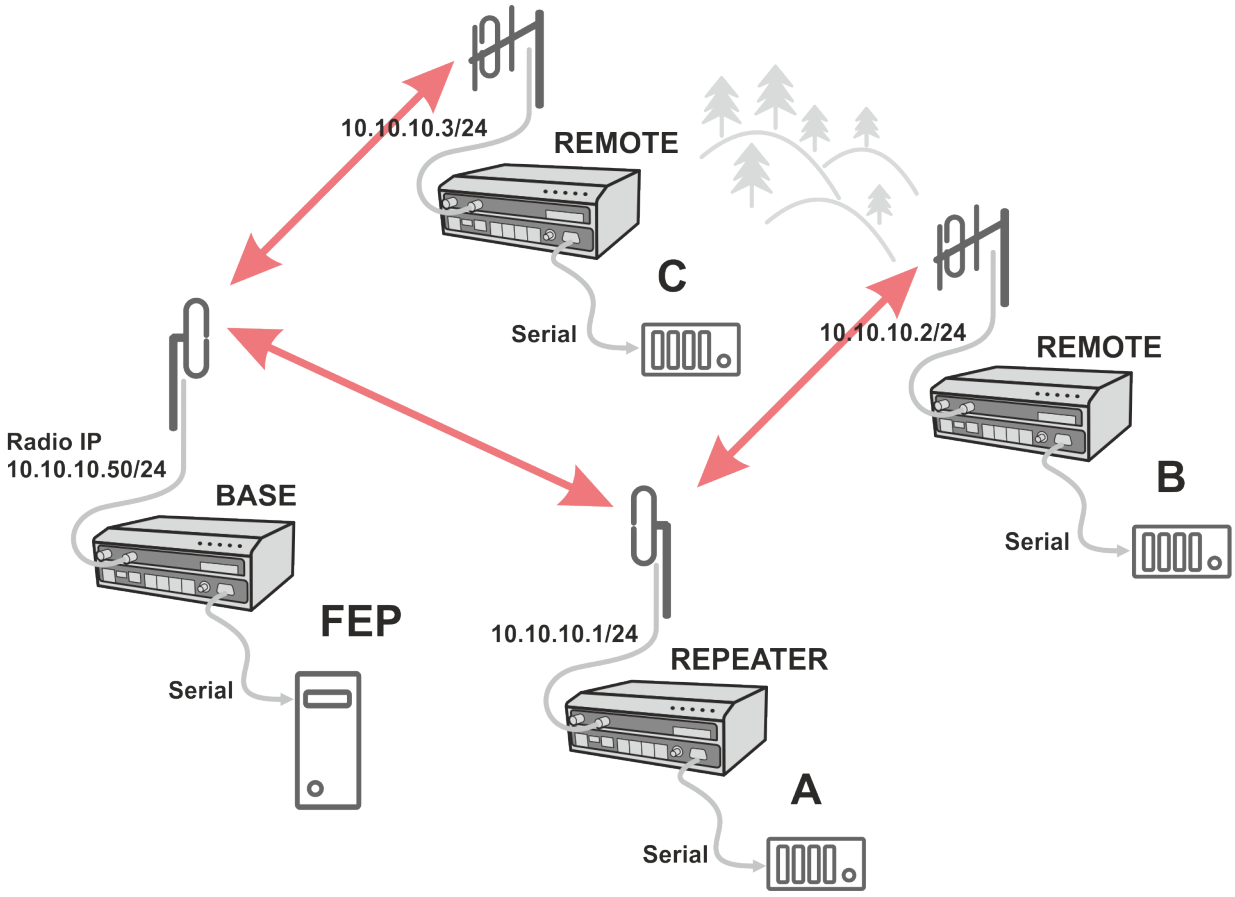


Fig. 5.4: Router - Base driven, Addressing - Serial

5.2.2. Router - Flexible

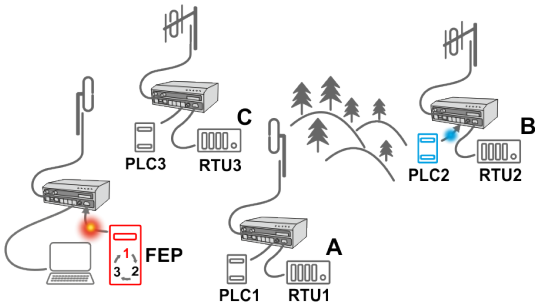
Router mode with Flexible protocol is suitable for Multipoint networks of all topologies with unlimited number of repeaters on the way, and all types of network traffic where Multi-master applications and any combination of simultaneous polling and/or report-by-exception protocols can be used.

Each RipEX2 can access the Radio channel spontaneously using sophisticated algorithms to prevent collisions when transmitting to the Radio channel. Radio channel access is a proprietary combination of CSMA and TDMA; the Radio channel is deemed to be free when there is no noise, no interfering signals and no frames being transmitted by other RipEX2 stations. In this situation, a random selection of time slots follows and a frame is then transmitted on the Radio channel.

Frame acknowledgement, retransmissions and CRC check, guarantee data delivery and integrity even under harsh interference conditions on the Radio channel.

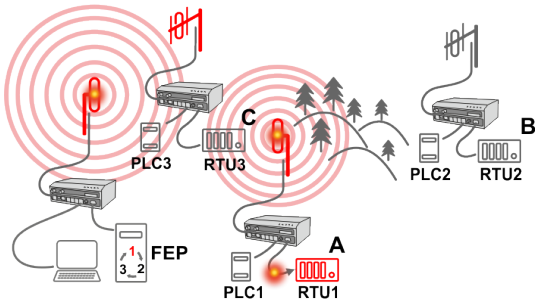
5.2.2.1. Functionality example

In the following example, there are two independent SCADA devices connected to RipEX2's ports (COM and ETH). One is designated RTU (Remote Telemetry Unit) and is assumed to be polled from the center by the FEP (Front End Processor). The other is labelled PLC (Programmable Logic Controller) and is assumed to communicate spontaneously with arbitrary chosen peer PLCs.



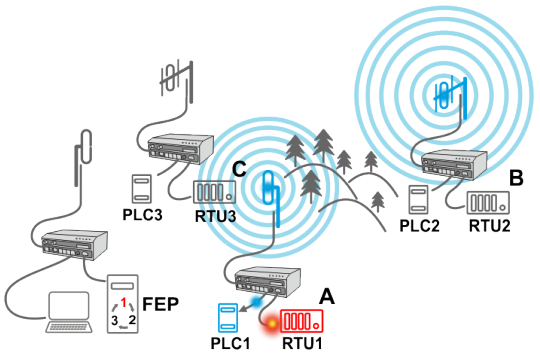
Step 1

FEP sends a request packet for RTU1 through COM to its connected RipEX2.
Simultaneously PLC2 sends a packet for PLC1 to RipEX2 B through ETH4.



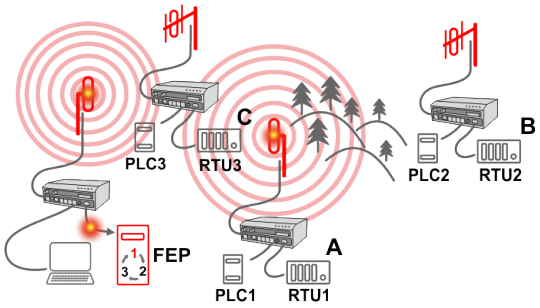
Step 2

FEP's RipEX2 transmits an addressed packet for RTU1 on Radio channel.
RipEX2 1 receives this packet, checks data integrity and transmits the acknowledgement.
At the same time packet is sent to RTU1 through COM.
RipEX2 3 receives this packet too. It doesn't react, because this packet is directed to RipEX2 1 only.



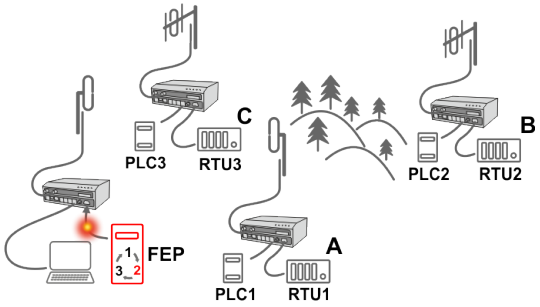
Step 3

RipEX2 2 waits untill previous transaction on Radio channel is finished (anti-collision mechanism).
Then RipEX2 2 transmits on Radio channel the addressed packet for PLC1.
RipEX2 1 receives this packet, checks data integrity and transmits acknowledgement.
At the same time packet is sent to PLC1 through ETH4.
Simultaneously the reply packet from RTU1 for FEP is received on COM.



Step 4

RipEX2 1 transmitts the reply packet from RTU1 for FEP on Radio channel.
All RipEX2 units receive this packet. This packet is addressed to FEP's RipEX2, so only FEP's RipEX2 reacts. It checks data integrity and transmits the acknowledgement to RipEX2 1.
At the same time the packet is sent to FEP through COM.



Step 5

FEP receives the response from RTU1 and polling cycle continues…

However any PLC or RTU can spontaneously send a packet to any destination anytime.

5.2.2.2. Configuration example

As it was mentioned above, RipEX2 radiomodem works as a standard IP router with two independent interfaces: radio and ETH. Each interface has got its own MAC address, IP address and mask.

The IP router operating principles stipulate that every unit can serve as a repeater. Everything what is needed is the proper configuration of routing tables.

Radio IP addresses of the RipEX2 units required to communicate over the radio channel must share the same IP network. We recommend planning your IP network so that every RipEX2 is connected to a separate sub-network over the Ethernet port. This helps to keep the routing tables clear and simple.

Note

Even if the IP addresses of all RipEX2 units in a radio channel share a single IP network, they may not be communicating directly as in a common IP network. Only the RipEX2 units that are within the radio range of each other can communicate directly. When communication with radio IP addresses is required, routing tables must include even the routes that are within the same network (over repeaters), which is different from common IP networks. The example configuration below does not show such routing rules for the sake of simplicity (they are not needed in most cases).

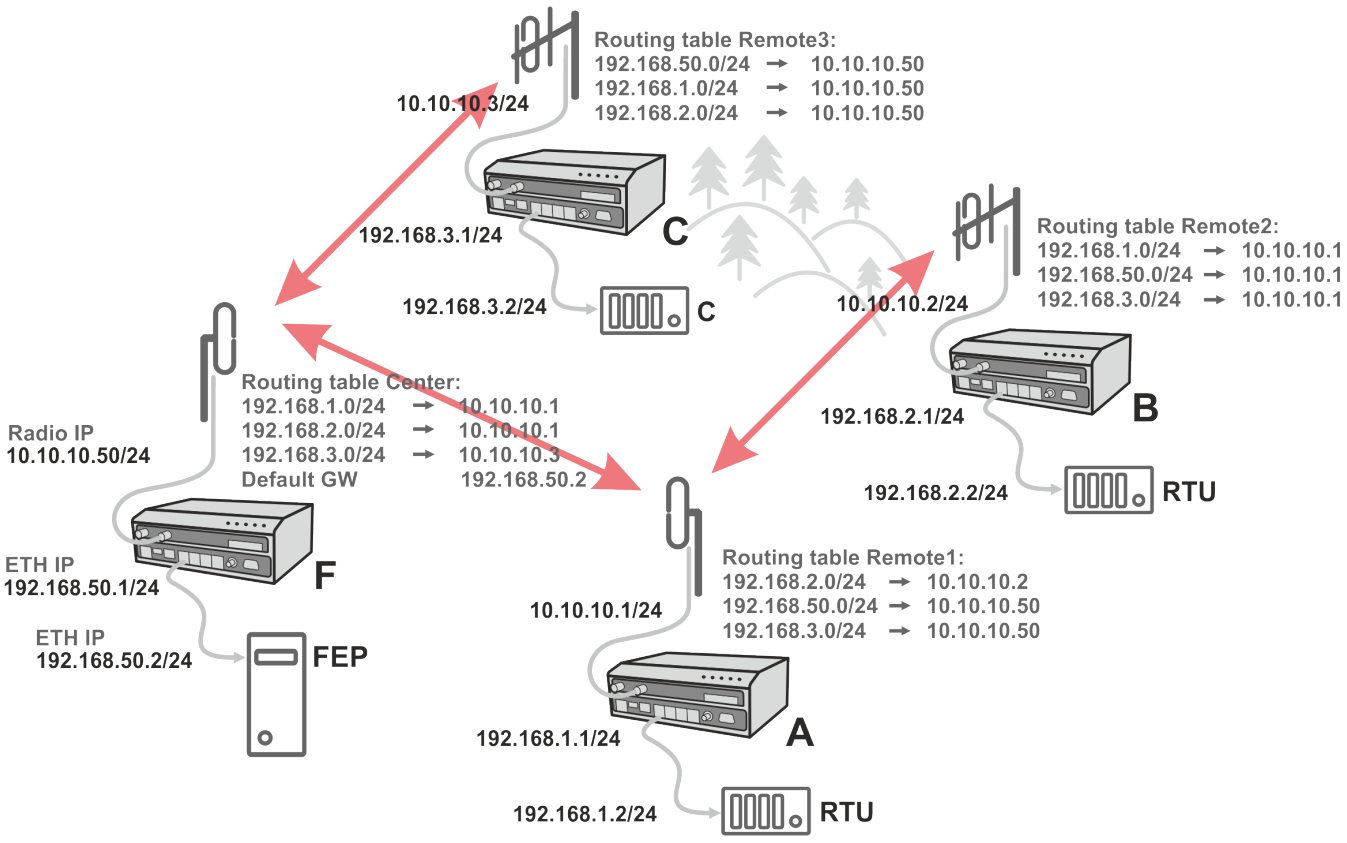


Fig. 5.5: Router - Flexible, Addressing

Formal consistency between the last byte of the radio IP address and the penultimate byte of the Ethernet address is not necessary but simplifies orientation. The “Addressing” image shows a routing table next to every RipEX2. The routing table defines the next gateway for each IP destination. In radio transmission, the radio IP of the next radio-connected RipEX2 serves as the gateway.

Example of a route from FEP (RipEX2 50) to RTU 2:

- The destination address is 192.168.2.2
- The routing table of the RipEX2 50 contains this record:
  Destination 192.168.2.0/24 Gateway 10.10.10.1
- Based on this record, all packets with addresses in the range from 192.168.2.1 to 192.168.2.254 are routed to 10.10.10.1
- Because RipEX2 50's radio IP is 10.10.10.50/24, the router can tell that the IP 10.10.10.1 belongs to the radio channel and sends the packet to that address over the radio channel
- The packet is received by RipEX2 1 with the address 10.10.10.1 where it enters the router
- The routing table of RipEX2 1 contains the record:
  Destination 192.168.2.0/24 Gateway 10.10.10.2
  based on which the packet is routed to 10.10.10.2 over the radio channel
- The packet is received by RipEX2 2
- The router compares the destination IP 192.168.2.2 with its own Ethernet address 192.168.2.1/24 and determines that the packet's destination is within its ETH network and sends the packet over the Ethernet interface – eventually, the packet is received by RTU 2.

5.2.2.3. Addressing hints

In large and complex networks with numerous repeaters, individual routing tables may become long and difficult to comprehend. To keep the routing tables simple, the addressing scheme should follow the layout of the radio network.

More specifically, every group of IP addresses of devices (both RipEX2's and SCADA), which is accessed via a repeater, should fall in a range which can be defined by a mask and no address defined by that mask exists in different part of the network.

A typical network consisting of a single center and number of remotes has got a tree-like layout, which can be easily followed by the addressing scheme – see the example in the figure "Optimised addressing" below.

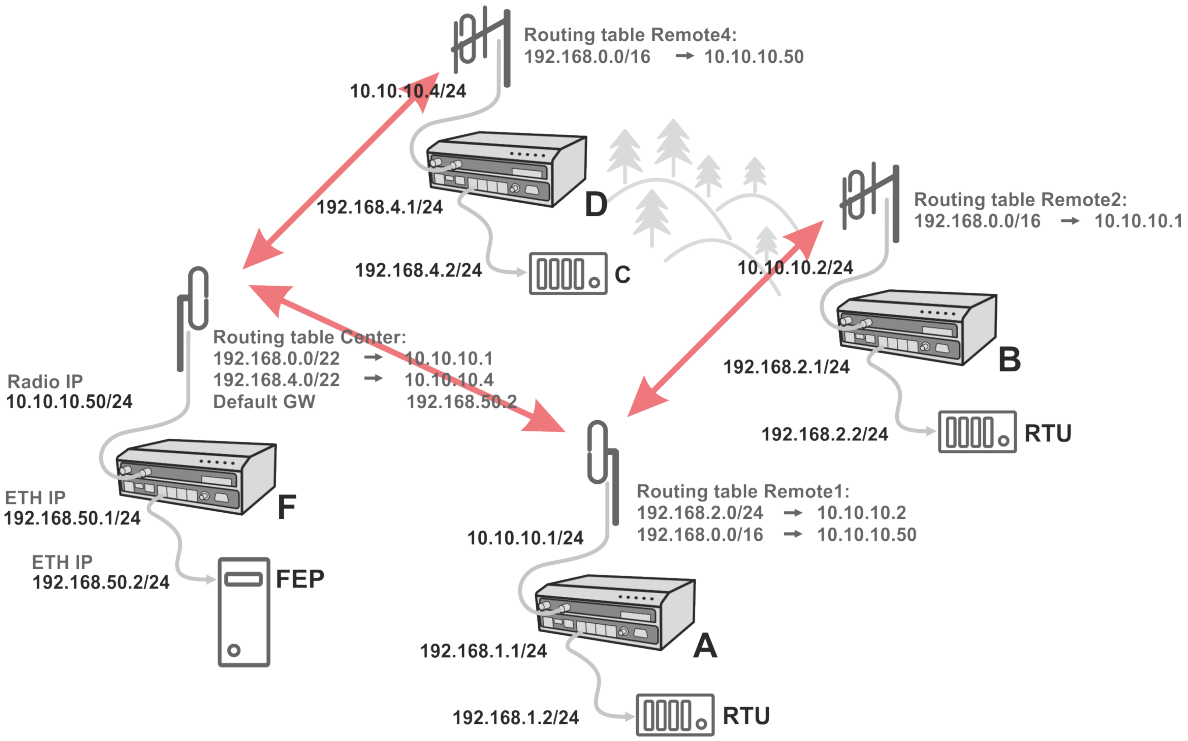


Fig. 5.6: Router - Flexible, Optimised addressing

The default gateway is also a very powerful routing tool, however be very careful whenever the default route would go to the radio interface, i.e. to the radio channel. If a packet to non-existing IP destination came to the router, it would be transmitted over the radio channel. Such packets increase the load of the network at least, cause excessive collisions, may end-up looping etc. Consequently the default route should always lead to the ETH interface, unless you are perfectly certain that a packet to non-existing destination IP may never appear (remember you are dealing with complex software written and configured by humans).

5.3. Combination of IP and serial communication

RipEX2 enables combination of IP and serial protocols within a single application.

Five independent terminal servers are available in RipEX2. 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** over the radio channel.

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).

5.3.1. Detailed Description

Generally, a Terminal server (also referred to as Serial server) enables connection of devices with a serial interface to a RipEX2 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 radio 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 RipEX2. This type of connection between RipEX2 SCADA and application is beneficial in the following circumstances:

- There is no hardware serial interface on the computer
- Serial cable between RipEX2 and computer would be too long. E.g. the RipEX2 is installed very close to the antenna to reduce feed line loss.
- LAN already exists between the computer and the point of installation



Important

The TCP (UDP) session operates only locally between RipEX2 and the central computer, hence it does not increase the load on the radio channel.

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 RipEX2. User data are extracted from the TCP messages and processed as if it came from a COM port. When the data reaches the destination RipEX2, it can be transferred to the RTU either via the serial interface or via TCP (UDP), using the Terminal server again. Please note, that RipEX2 Terminal server implementation also supports the dynamical IP port change in every incoming application datagram. In such a case the RipEX2 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 RipEX2 and the locally connected application up to 10 on each Terminal server.

6. Web interface

RipEX2 can be easily managed from your computer using a web browser. If there is an IP connection between the computer and the respective RipEX2, you can simply enter the IP address of any RipEX2 in the network directly in the browser address line and log in. However, it is not recommended to manage an over-the-air connected RipEX2 in this way, because high amounts of data would have to be transferred over the Radio channel, resulting in quite long response times.

System fonts are utilized to accelerate the loading of web pages. This functionality was introduced in FW 2.2.5.0. As system fonts are dependent on the operating system, the screenshots featured in this manual were captured on a Microsoft Windows OS.

When you need to manage an over-the-air connected RipEX2, log-in to a RipEX2, which your computer is connected to using either a cable (via LAN) or a high-speed WAN (e.g. Internet). The RipEX2 which you are logged-in to in this way is called Local. Then you can manage any remote RipEX2 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 RipEX2 and only information specific to the remote unit is transferred over the Radio channel. RipEX2 accessed in such a way is called Remote.

When in Router mode, the IP address of either the Radio or Ethernet interface in the remote unit can be used for such a Remote management. IP routing between the source (Local RipEX2) and the destination IP (Remote RipEX2) needs to be configured properly.

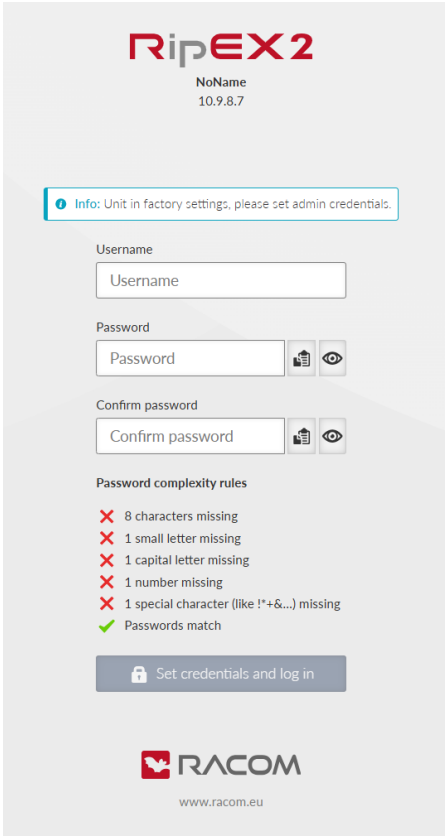
When in Bridge mode, IP address of the Network interface the Radio interface is bridged with is used for Remote access. When accessing the unit locally the IP address belonging to an Ethernet port, the management PC is connected to, is used. Be careful, each RipEX2 MUST have its unique IP address and all these IP addresses have to be within the same IP network (defined by the IP Mask) when Remote management is required in Bridge mode.

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

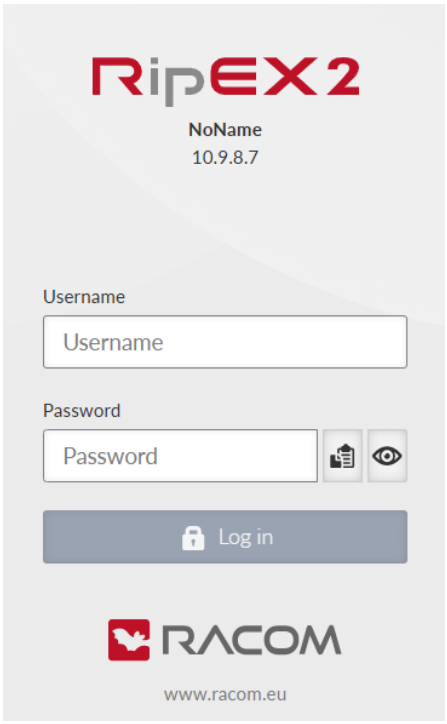
For the sake of security only HTTPS protocol is used for the connection between the web browser and RipEX2 unit. If the http://... is used into the web browser address line, the communication is immediately automatically redirected to HTTPS protocol.

For better protection against unauthorized access to the network there is a timer build within the RipEX2 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.

First time login page



Login page

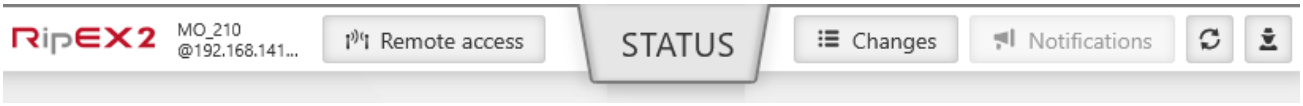


The login page informs you about the Unit name and IP address of the RipEX2 unit you are trying to log in.
The login page allows to view and copy the password.

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 RipEX2 unit you are connected to
- Remote access button
- Identification of the current web page (2nd or 3rd 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:

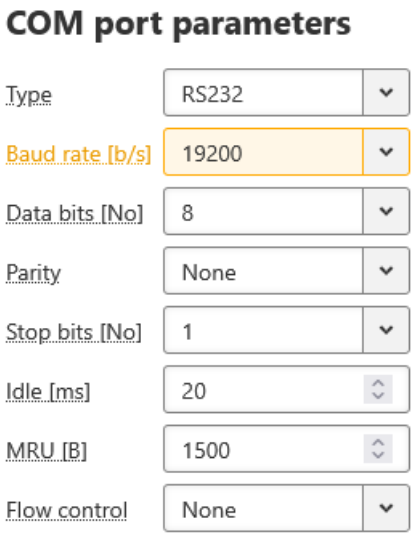
- Safari for iOS
- Chrome for Android

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

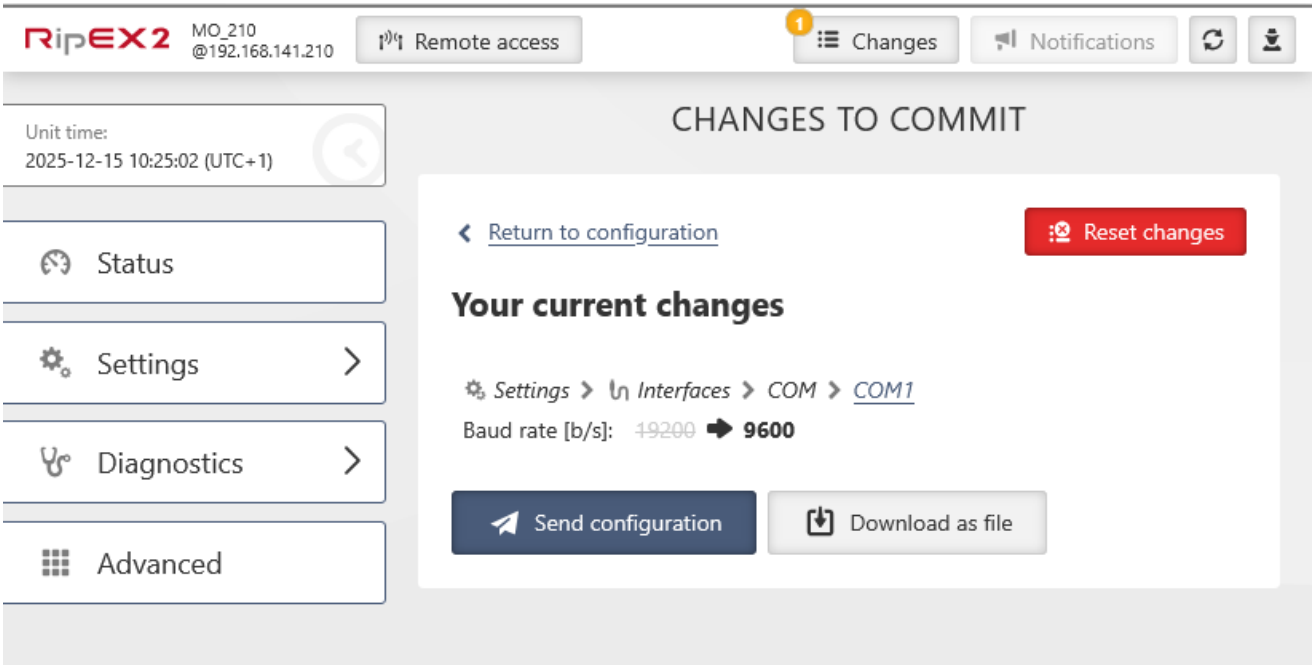
RipEX2 is capable of remembering changes, which were done in its configuration and collecting them in a Changes to commit "basket". All changes of configuration parameters are highlighted by different color.



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.

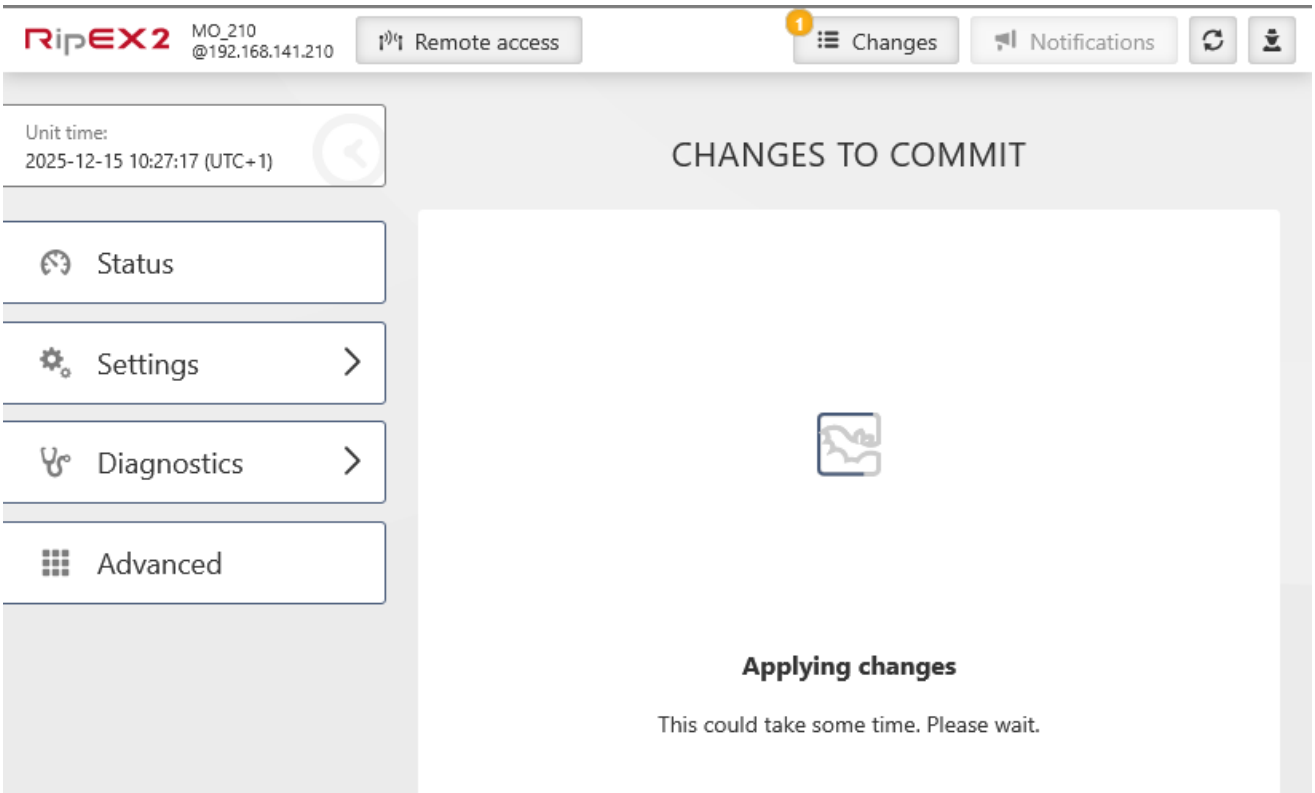
Changes to commit "basket" collects all changed settings, which:

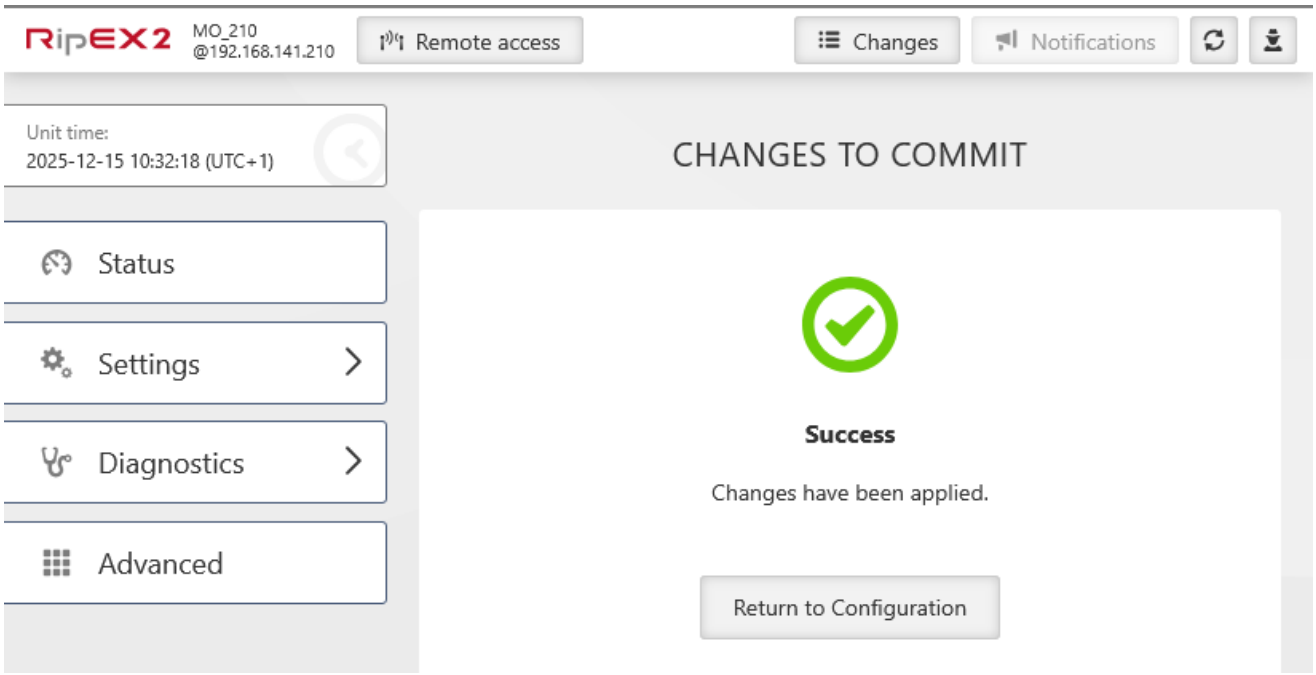
- Are separated in the menu alphabetically. Alphabetical separation is sorted hierarchically according to the name of items in the menu.
- Are displayed in the menu (including the path of their placement) and provided with a link for a quick transfer to its original placement.
- Carry an information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



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.



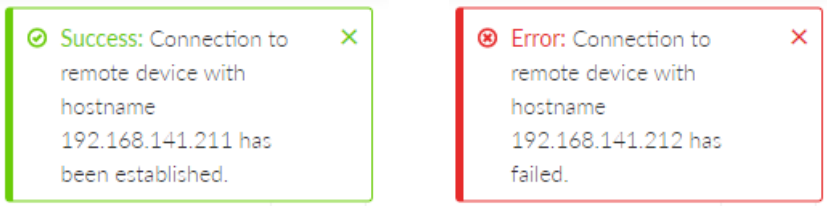


6.3. Notifications

With RipEX2 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.

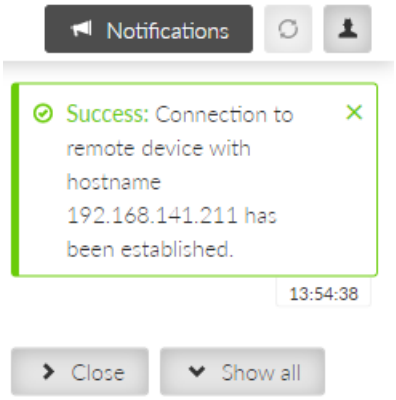
Note

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



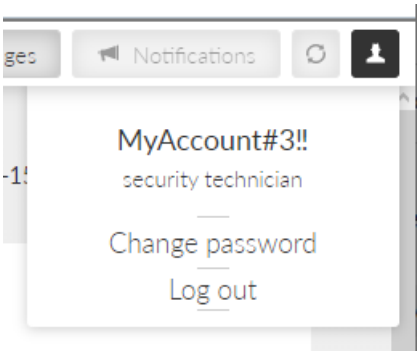
Notifications are mostly triggered by user actions in the interface, for example success or failure of Fast Remote Access connection. They are not to be confused with Events, which are triggered mostly by the system and are not shown in the Notification Center, but on Diagnostics > Events page. In other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

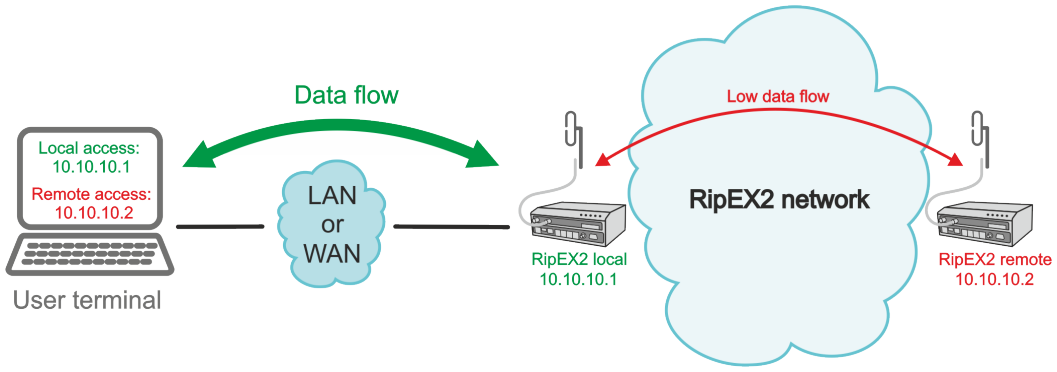


6.5. Remote access

RipEX2 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).

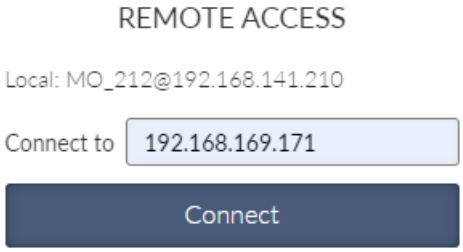
Note

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



RipEX2 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 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 RipEX2 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

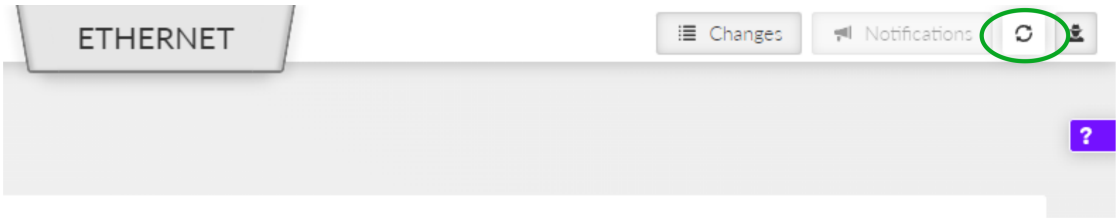
Note

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.

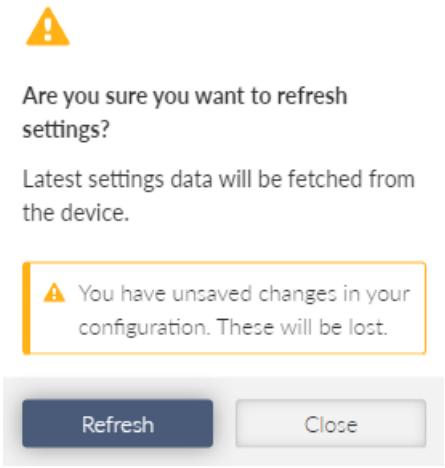
By default, remote access utilizes the **_RO_Rmt_Access_Host_Key** for establishing connections to remote units. However, for enhanced security purposes, we strongly recommend utilizing a custom **RMTACCESS Key** (menu SETTINGS > Security > Credentials).

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.



Note

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

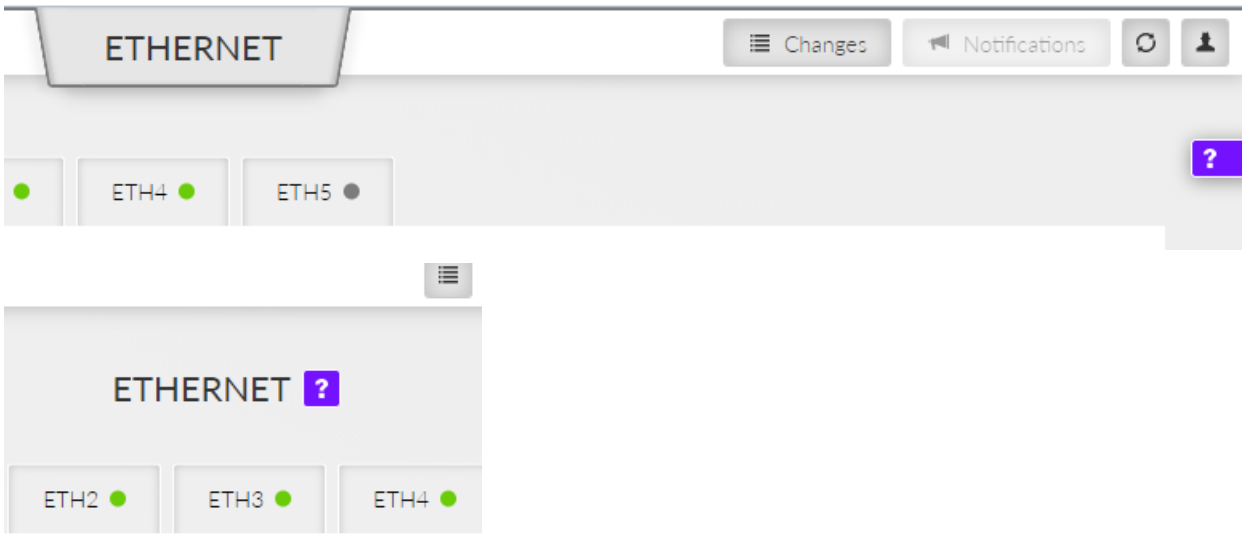
6.7. Status info area

Status info area provides a general overview about RipEX2'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).



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).



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	Shortcut on STATUS	Access to
Ctrl+Alt+R	R	Remote Access
Ctrl+Alt+O	O	DIAGNOSTICS > Overview
Ctrl+Alt+C	C	Changes
Ctrl+Alt+N	N	Notifications

7. Settings

The Settings chapter contains a description of all configuration parameters of the unit. The division into chapters corresponds to the menu structure in the graphical web interface. The Help pages, which are built into the unit firmware, are identical to this chapter of the manual.

7.1. Interfaces

7.1.1. Ethernet

RipEX2 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.

When unit is operating in Bridge mode - the default Network interface bridges together not only physical Ethernet ports, but also the Radio interface. All the Ethernet traffic received by those Ethernet ports is transferred to the Radio interface and transmit by the Radio channel and vice versa.

When unit is operating in Router mode - the Radio channel transmits only the traffic, which is destined to the Radio interface by Routing rules.

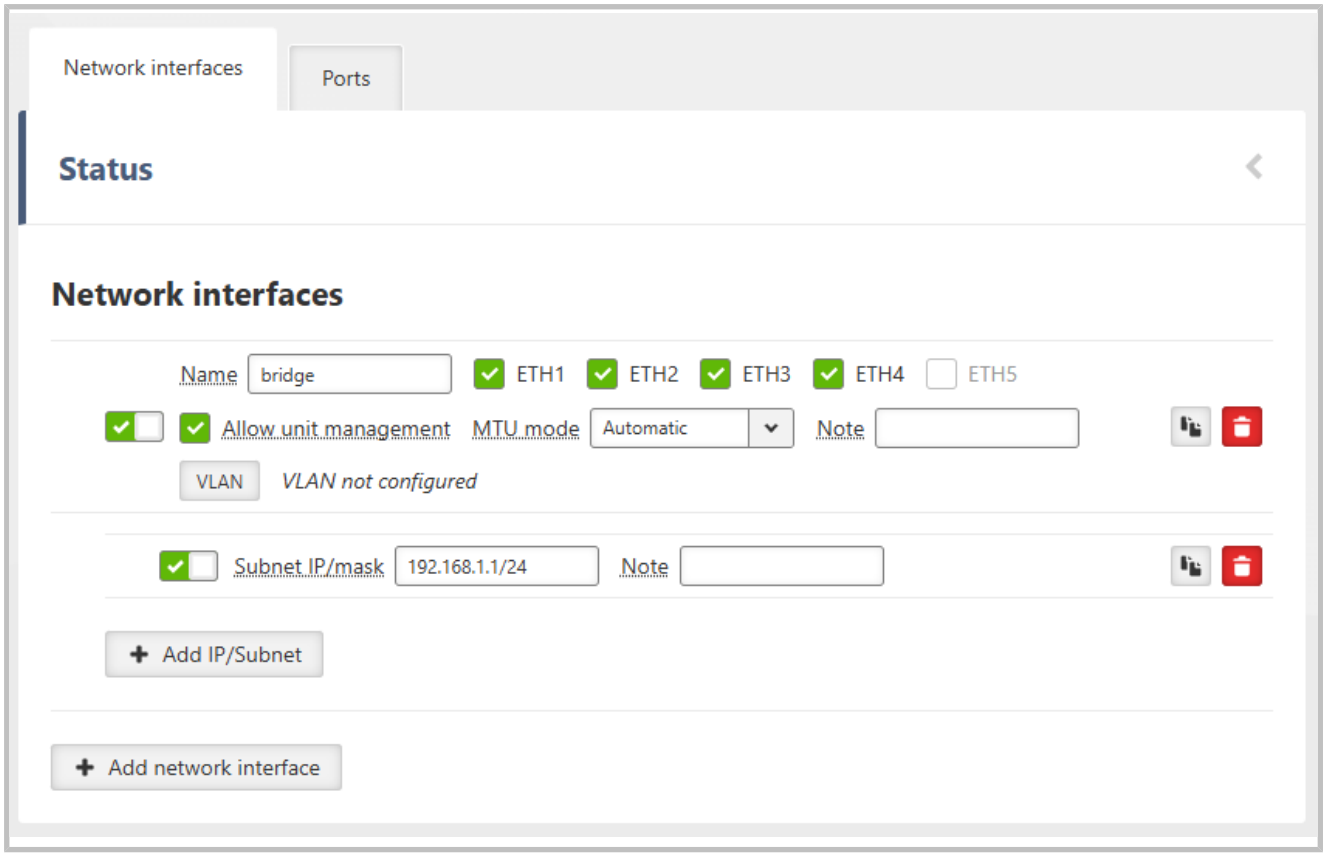


Fig. 7.1: SETTINGS > Interfaces > Ethernet > Nework interfaces

The radio 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
Checkbox {On, Off}
Toggle your network interface status.

Name
Text input
Enter a unique identifier for your network interface.

ETH1 - ETH5
Checkboxes
Assign specific Ethernet ports to your network interface.

Note
Hardware option RipEX2e product variants H and J provide only ETH1 and ETH2 interfaces.

Note
Your interface does not require assigned Ethernet ports if you configure either a Radio interface or GRE L2 tunnel.

Allow unit management
Checkbox {On, Off}
Permit administration access to your station through this interface.

MTU mode
List box {Automatic, Limited}, default = "Automatic"
Select your interface MTU calculation method. Automatic sets the MTU based on your subordinate ports. Limited restricts the MTU to your specified upper boundary.

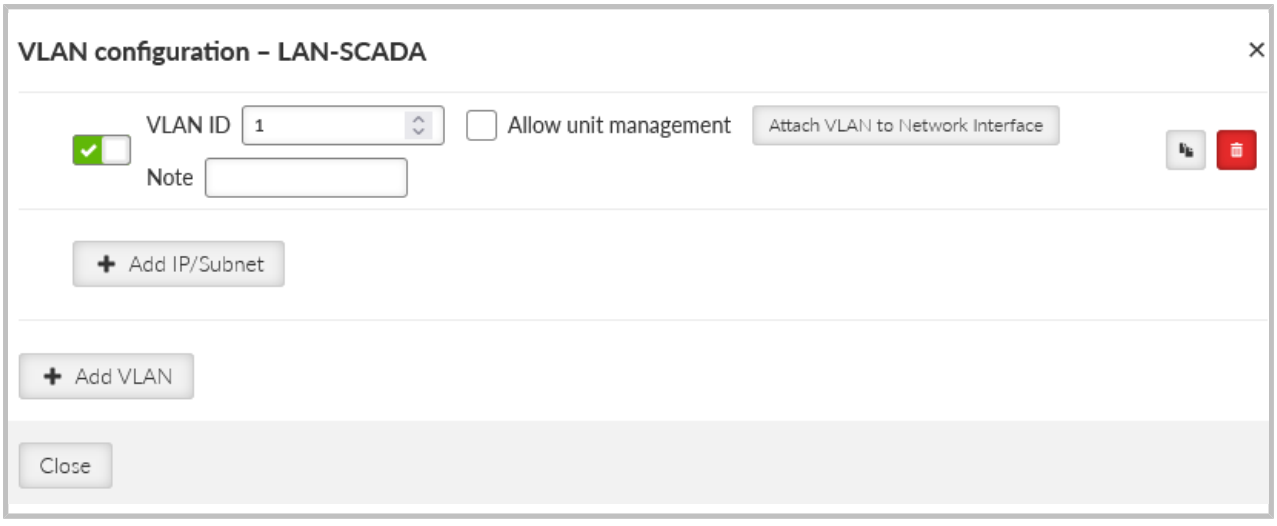
MTU limit [B]
Number [74, 1500], default = "1500"
Set your upper MTU boundary. The system applies this value when you select the Limited MTU mode. Your actual interface MTU decreases if your subordinate ports have a smaller MTU.

Add IP/Subnet
Button
Add a defined subnet to your network interface.

IP / Mask
IP address/Mask
Enter the IP address and mask in CIDR notation. This address identifies your network interface in the Layer 3 network.

Note
Text input
Add a custom description for your interface.

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



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

MTU mode
List box {Automatic, Limited}, default = "Automatic"
Select your interface MTU calculation method. Automatic sets the MTU based on your subordinate ports. Limited restricts the MTU to your specified upper boundary.

MTU limit [B]
Number [74, 1500], default = "1500"
Set your upper MTU boundary. The system applies this value when you select the Limited MTU mode. Your actual interface MTU decreases if your subordinate ports have a smaller MTU.

Note
Optional comment.

Add IP/Subnet
Adds defined subnet to the VLAN.

7.1.1.2. Ports

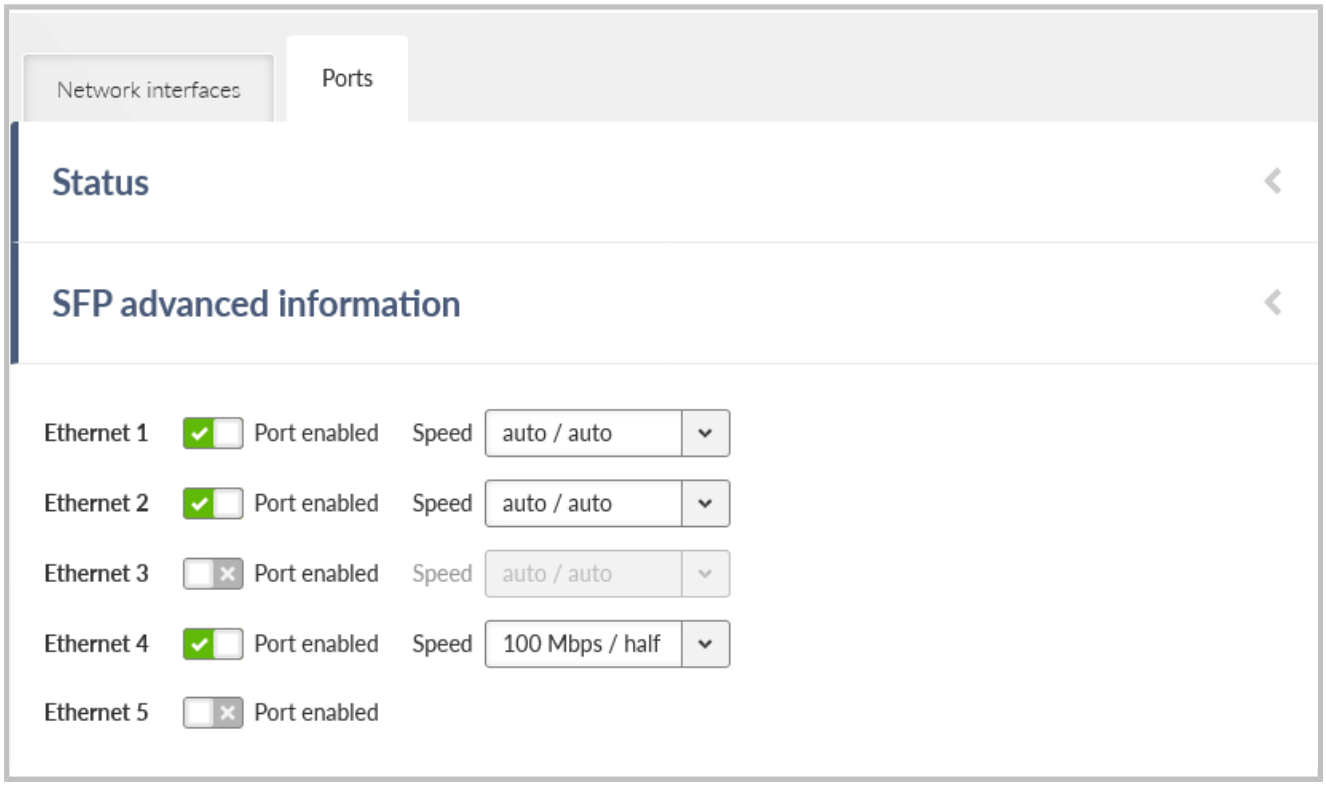


Fig. 7.2: SETTINGS > Interfaces > Ethernet > Ports

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

HW option RipEX2e (product variant ‘H' and 'J’) provides only ETH1 - ETH2 interfaces.



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. Radio

Settings of Radio is divided to 5 sections:

- Radio interface
- Radio protocol
- Radio parameters
- Encryption
- Individual link option (router mode only)

Radio interface behavior is heavily affected by a Radio interface mode. For Bridge mode, there is one protocol available:

- *Transparent* – This protocol is very simple; no channel access mechanism takes place. Suitable for star topology with maximum one repeater along the packet path. Available in Bridge mode.

For router mode, there are 2 protocols available:

- *Base driven* – TCP/IP optimized protocol having deterministic channel access mechanism. Suitable for star topology with maximum one repeater along the packet path. Available in Router mode.
- *Flexible* - Suitable for master or even multi master-slave polling and report by exception from remotes concurrently. No limits in network design – each radio can work as base station, a repeater, a remote, or all of these simultaneously.

Radio channel parameters (such as frequency, output power etc.) are common for all protocols. They are described later in this chapter.

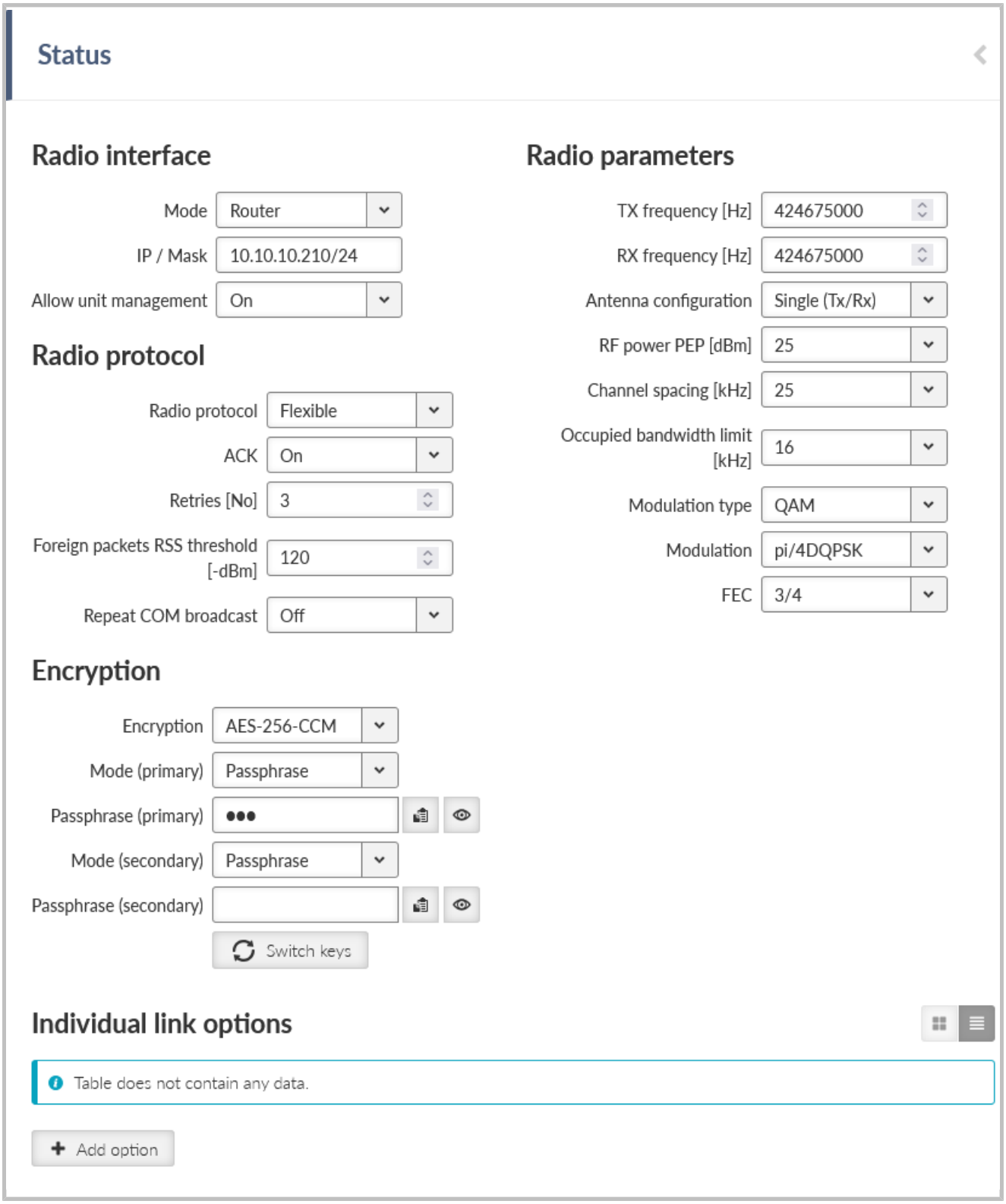


Fig. 7.3: SETTINGS > Interfaces > Radio

7.1.2.1. Radio interface



Mode

List box {Bridge; Router}, default = "Bridge"

Selecting Bridge or Router mode affects many other parameters across the unit. See *Section 5.1, "Bridge mode"* and *Section 5.2, "Router mode"* for detailed description.

IP / Mask

IP address of the radio interface and the mask of the radio network. This parameter occurs only, if parameter "**Mode**" is set to "Router".

Allow unit management

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

Allows / disables unit management for the Radio interface.

7.1.2.2. Radio channel parameters



TX frequency

Transmitting frequency in Hz. Step 5 kHz (for 25 kHz channel spacing) or 6.25 kHz (for 12.5 or 6.25 kHz channel spacing).

The value entered must be within the frequency tuning range of the product as follows:

RipEX2-1A: 135–175 MHz

RipEX2-2A: 215–240 MHz

RipEX2-3A: 285–335 MHz

RipEX2-3B: 335–400 MHz
RipEX2-4A: 400–470 MHz
RipEX2-4B: 450–520 MHz
RipEX2-8A: 803–897 MHz
RipEX2-9A: 860–960 MHz

RX frequency
Receiving frequency, the same format and rules apply as for TX frequency.

Antenna configuration
List box {Single (Tx/Rx); Dual (Rx, Tx/Rx)}, default = "Dual (Rx; Tx/Rx)"
See *chapter 1.2.1. Antenna* for details

Note
HW option RipEX2e (product variant ‘H' and 'J’) enables Single antenna operation only.

RF power PEP
See *PEP versus RMS RF power*[1].

Channel spacing [kHz]
List box {possible values}, default = "25 kHz"

Note
Channels 250 and 300 kHz are available only in Bridge mode.

Note
HW option RipEX2e (product variant ‘H' and 'J’) provides Channel spacing up to 50 kHz.

Occupied bandwidth limit [kHz]
List box {possible values}, default = "25 kHz"
Occupied bandwidth is limited by granted radio channel. The standards supported by using individual OBW limits are in *Section 9.1, “ Detailed radio channel parameters”* of this manual.

Modulation type
List box {FSK, QAM}, default = "FSK"

FSK
Suitable for difficult conditions – longer radio hops, non-line of sight, noise / interferences on Radio channel…

Note
FSK belongs to the continuous-phase frequency-shift keying family of non-linear modulations. Compared to QAM (linear modulations), FSK is characterized by narrower bandwidth, a lower symbol rate and higher sensitivity. As a result, the system gain is higher, power efficiency is higher, but spectral efficiency is lower.

QAM
Suitable for normal conditions offering higher data throughput.

[1] https://www.racom.eu/eng/products/m/ripex/app/pep/pep.html

Note
QAM belongs to the phase shift keying family of linear modulations. Compared to FSK (non-linear modulations), QAM is characterized by wider bandwidth. The spectral efficiency is higher, power efficiency is lower and system gain is typically lower.

Modulation

FSK modulations:
List box {2CPFSK; 4CPFSK}, default = "2CPFSK"

QAM modulations:
List box {DPSK; π/4DQPSK; D8PSK; 16DEQAM; 64QAM; 256QAM}, default = "DPSK"

Note
For more detailed information see *Section 9.2, "Recommended MSE thresholds"*.

Note
HW option RipEX2e (product variant 'H' and 'J') provides Modulation up to 64QAM.

FEC

List box {2/3; 3/4; 5/6; Off}, default = "Off"
FEC (Forward Error Correction) is a very effective method to minimize radio channel impairments. Basically, the sender inserts some redundant data into its messages. This redundancy allows the receiver to detect and correct errors; used is Trellis code with Viterbi soft-decoder. The improvement comes at the expense of the bitrate. The lower the FEC ratio, the better the capability of error correction and the lower the bitrate. Bitrate = Modulation rate × FEC ratio.

Radio can receive not only radio frames with the very same setting, but also frames with different type of modulation - the Auto-speed functionality.

Modulation types which can be combined (with the same radio frequencies, channel spacing and OBW limit) are:

2CPFSK & 4CPFSK with or without FEC

or

DPSK & π/4DQPSK & D8PSK & 16DEQAM & 64QAM & 256QAM with or without FEC.

This functionality is used especially in the Individual link option (Flexible protocol) and the setting of the Base - Remote communication settings (in Base Driven Protocol).

7.1.2.3. Adaptive coding and modulation (ACM)

The ACM mechanism adapts the current modulation and coding to the signal quality of each individual radio link between stations. Specific modulation and coding pairs (profiles) are arranged so that the transmission channel capacity increases with increasing signal quality due to the gradual switching of ACM profiles. ACM works independently for each direction of the link. The signal quality measurement required for the ACM algorithm is performed on the receiver side. The signal quality information is delivered to the transmitter as an extension of the data packets. ACM therefore brings a certain overhead in addition to the transmitted data.

Implementation differences according to the type of radio protocol:

Transparent: ACM can be used with only 2 stations in the network, i.e. only for point-to-point communication.

Flexible: ACM is not limited by the network topology. It therefore also works in point-to-multipoint communication including multiple retranslation in a daisy-chain scenarios.

Base driven: ACM is not limited by the network topology. It therefore also works in point-to-multipoint communication including retranslations.

The ACM parameter setting is global for the entire network. All stations in the entire radio network should either have ACM enabled or disabled.

ACM

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

Enables / Disables Adaptive coding and modulation (ACM) for the radio interface. When enabled, the **Modulation** and **FEC** parameters selection is disabled. Modulation a FEC is controlled automatically by ACM. To enable ACM, you must have the corresponding SW key installed.

Default profile

List box {2CPFSK 3/4 (FSK); 4CPFSK 3/4 (FSK); 4CPFSK 1/1 (FSK); DPSK 3/4 (QAM); pi/4DQPSK 3/4 (QAM); 16DEQAM 3/4 (QAM); 64QAM 3/4 (QAM); 256QAM 3/4 (QAM); 256QAM 5/6 (QAM)}, default = "2CPFSK 3/4"

Initial and also minimum ACM profile. Depending on the current setting of the Modulation type parameter, the ACM selection box will offer profiles containing only FSK or QAM modulation.

Best profile

List box {2CPFSK 3/4 (FSK); 4CPFSK 3/4 (FSK); 4CPFSK 1/1 (FSK); DPSK 3/4 (QAM); pi/4DQPSK 3/4 (QAM); 16DEQAM 3/4 (QAM); 64QAM 3/4 (QAM); 256QAM 3/4 (QAM); 256QAM 5/6 (QAM)}, default = "2CPFSK 3/4"

Maximum ACM profile. Depending on the current setting of the Modulation type parameter, the ACM selection box will offer profiles containing only FSK or QAM modulation. The Best profile can be the same or higher than the Default profile.

Fallback timeout [min]

Number {1 – 60}, default = 10

If no communication occurs on the monitored radio channel during this time interval, the information about the status of this channel is declared obsolete and the ACM is switched to the initial profile - the **Default profile** value.

Switching to the Default profile is performed at the next communication on the radio channel.

Note

HW option RipEX2e (product variant ‘H' and 'J’) cannot use ACM.

7.1.2.4. Encryption



Encryption

List box {Off; AES-256-CCM; AES-256-CCM+KEX}, default = "Off"

AES 256-CCM (Advanced Encryption Standard with Cipher Block Chaining-Message Authentication Code) according to RFC 6655 can be used for encryption and authentication of packets on Radio channel to protect your data from an intrusion and replay attack. When AES 256-CCM is On, a control block of 25 Bytes length (13 B nonce + 12 B TAG) is attached to each frame on Radio channel. AES requires an encryption key. The length of key is 256 bits. The same key must be stored in all units within the network. The AES-CCM provides assurance of the confidentiality and the authenticity of data according to NIST SP 800-38C.

AES-256-CCM+KEX uses a static shared key to negotiate dynamic keys that encrypt user data. Dynamic keys are unique to each station and are changed periodically. It encrypts the data content of packets and monitors the integrity of part of the headers.

Mode

List box {Passphrase; Key ID}, default = "Passphrase"

This parameters occur, if parameter "**Encryption**" is set to "AES-256-CCM; AES-256-CCM+KEX".

Passphrase

The key can be automatically generated based on a Passphrase. Fill in your Passphrase (any printable ASCII character, min. 1 char, max. 128 char). The same Passphrase must be set in all units within the network. This parameter occurs only, if parameter "**Mode**" is set to "Passphrase".

Key

The Key stored in SETTINGS > Security > Credentials is used. It is possible to use the default key with IDRadio_Encryption_Key or (highly recommended) to generate own key (Generate credential : your ID, Type PSK Key (PRI) AES, PSK length 32 B). The same key must be used in all units within the network (it is possible to download it from the first unit and upload it to allother units: SETTINGS > Security > Credentials > Add credential: fill your ID, change Type to PSK Key (PRI) AES and select the proper file with the key).

Note
The required key type is “PSK key” and it must be exactly 32 bytes long (256 bits).

This parameter occurs only, if parameter "**Encryption**" is set to "AES-256-CCM+KEX".

Key replacement period

Number {5 – 10080}, default = 1440 [min]

The average data channel key replacement period (randomized within a range of +- 10%).

7.1.2.5. Transparent protocol (Bridge mode)

Bridge mode with fully transparent Radio protocol is suitable for all polling (request-response) applications with star network topologies, however repeater(s) are possible.

A packet received through any interface (bridged with the radio interface) is broadcasted to the appropriate interfaces of all units within the network.

Any unit can be configured as a repeater. A repeater relays all packets it receives through the radio channel. The network implements safety mechanisms which prevent cyclic loops in the radio channel (e.g. when a repeater receives a packet from another repeater) or duplicate packets delivered to the user interface (e.g. when RipEX2 receives a packet directly and then from a repeater).

Transparent protocol does not solve collisions on the radio channel protocol. There is a CRC check of data integrity, however, i.e. once a message is delivered, it is 100% error free.



Radio protocol
List box {Transparent; None}, default = "None"

Communication mode
List box {Half Duplex; Full Duplex}, default = "Half Duplex"
Full duplex mode is intended to be used mainly for Point-to-Point communication. Full duplex operation is not possible in networks with repeaters.

Note
HW option RipEX2e (product variant ‘H' and 'J’) enables Half duplex operation only.

Unit is repeater

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

Each RipEX2 may work simultaneously as a Repeater (Relay) in addition to the standard Bridge operation mode.

If "On", every frame received from Radio channel is transmitted to the respective user interface (ETH, COM) and to the Radio channel again.

The Bridge functionality is not affected, i.e. only frames whose recipients belong to the local LAN are transmitted from the ETH interface.

It is possible to use more than one Repeater within a network. To eliminate the risk of creating a loop, the “Number of repeaters” has to be set in all units in the network, including the Repeater units themselves.

Warning: Should Repeater mode be enabled “Modulation rate” and “FEC” must be set to the same value throughout the whole network to prevent frame collisions occurring.

No of repeaters

Number {0 – 7}, default = 0

If there is a repeater (or more of them) in the network, the total number of repeaters within the network MUST be set in all units in the network, including the Repeater units themselves. After transmitting to or receiving from the Radio channel, further transmission (from this RipEX2) is blocked for a period calculated to prevent collision with a frame transmitted by a Repeater. Furthermore, a copy of every frame transmitted to or received from the Radio channel is stored (for a period). Whenever a duplicate of a stored frame is received, it is discarded to avoid possible looping. These measures are not taken when the parameter “Number of repeaters” is zero, i.e. in a network without repeaters.

Tx delay [B]

Number {0 – 1600}, default = 0

This parameter should be used when all substations (RTU) reply to a broadcast query from the master station. In such case massive collisions would ensue because all substations (RTU) would reply at nearly the same time. To prevent such collision, TX delay should be set individually in each slave RipEX2. The length of responding frame, the length of **Radio protocol overhead**, modulation rate have to be taken into account.

7.1.2.6. Base driven protocol (Router mode)

Router mode with Base driven protocol (BDP) is suitable for a star network topology with up to 256 Remotes under one Base station. Each Remote can work as a Repeater for one or more additional Remotes. This protocol is optimized for TCP/IP traffic and/or ‘hidden’ Remotes in report-by-exception networks, when a Remote is not be heard by other Remotes and/or different Rx and Tx frequencies are used.

Frame acknowledgement, retransmissions and CRC check guarantee data delivery and integrity even under harsh interference conditions on the Radio channel.



Note

There is no need to set any routes in Routing table(s) for Remote stations located behind Repeater. Forwarding of frames from the Base station over the Repeater in either direction is serviced transparently by the Base driven protocol.

Note

When Remote to Remote communication is required, respective routes via Base station have to be set in Routing tables in Remotes.

7.1.2.6.1. Radio protocol - Base station

The whole network traffic (including transactions) is controlled by the Base station. For this reason, the List of Remote stations is configured here.



Station type
List box {Base; Remote}, default = "Base"

Note
Only one Base station should be present within one radio coverage when Base driven protocol is used.

For each Remote station a BDP address (within the BDP network) and Radio parameters are configured here.

Note

HW option RipEX2e (product variant ‘H' and 'J’) cannot be used as a Base station.

7.1.2.6.2. Common Radio channel parameters

Common Radio channel parameters Modulation type, Modulation and FEC are used for transactions query on terminal status and for broadcast. The set type of modulation must match with settings in all terminals within the network.

7.1.2.6.3. Base station - List of Remote stations

All frames (to and from Base station) for a given Remote are transmitted with modulation set in this list. If the transaction is transmitted over a Repeater, the Repeater settings is not used.



BDP address (from), BDP address (to)

Protocol address [0 to 255] is the unique address assigned to each Remote and is only used by Base driven protocol. It is set in Remote unit in its Radio protocol settings. The default and recommended setting assigns Protocol address to be equal to the Radio IP last byte. If Protocol address mode in Remote unit is set to Automatic, this assignment is done automatically. If a specific address is required, fill both windows with the same number. If an interval is required, fill both windows with needed numbers.

Modulation type

List box {2CPFSK; 4CPFSK; DPSK; π/4DQPSK; D8PSK; 16DEQAM; 64QAM; 256QAM}, default = "2CPFSK"

Modulation and FEC settings for communication with terminal. Settings is used in both directions of communication. If the terminal is behind repeater, the settings is used all the way (Repeater settings is not used).

FEC

List box {Off; 2/3; 3/4; 5/6}, default = "Off"

For detailed description see Modulation type above.

ACK

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

Frame acknowledge enable. Applies to data frames transmitted from Base.

Retries

Number {0 – 15}, default = 3

Frame retries count. Applies to data frames transmitted from Base.

Set value is used in one direction from Base to Remote (Remote to Base direction is configured in Remote unit in its Radio protocol settings). If the Remote station is behind Repeater, set value is used for both radio hops: Base station - Repeater and Repeater - Remote.

CTS Retries

Number {0 – 15}, default = 3

Based on sophisticated internal algorithm, Base station sends a CTS (Clear To Send) packet which allows Remote station to transmit. If the Remote station is connected directly to the Base station (not behind Repeater), and the Base station doesn't receive a frame from the Remote station, the Base station repeats permission to transmit.

Connection
List box {Direct; Direct & Repeater; Behind repeater}, default = "Direct"

7.1.2.6.4. Radio protocol - Remote station



Automatic address mode
List box {On; Off}, default = "On"
When enabled, the Radio IP last byte is assigned as a BDP address - this setting is recommended.

BDP address
For detailed description see *Section 7.1.2.6.3, "Base station - List of Remote stations"*.

ACK
List box {On; Off}, default = "On"
Frame acknowledgement enable. Applies to data frames transmitted from Remote to Base.

Retries
Number {0 – 15}, default = 3
Frame retries count. Applies to data frames transmitted from Remote to Base.

7.1.2.7. Flexible Protocol (router mode)

Router mode with Flexible protocol is suitable for Multipoint networks of all topologies with unlimited number of repeaters on the way, and all types of network traffic where Multi-master applications and any combination of simultaneous polling and/or report-by-exception protocols can be used.



ACK
List box {On; Off}, default = "On"
General setting of acknowledging of received packets. It can be set differently in individual link options.

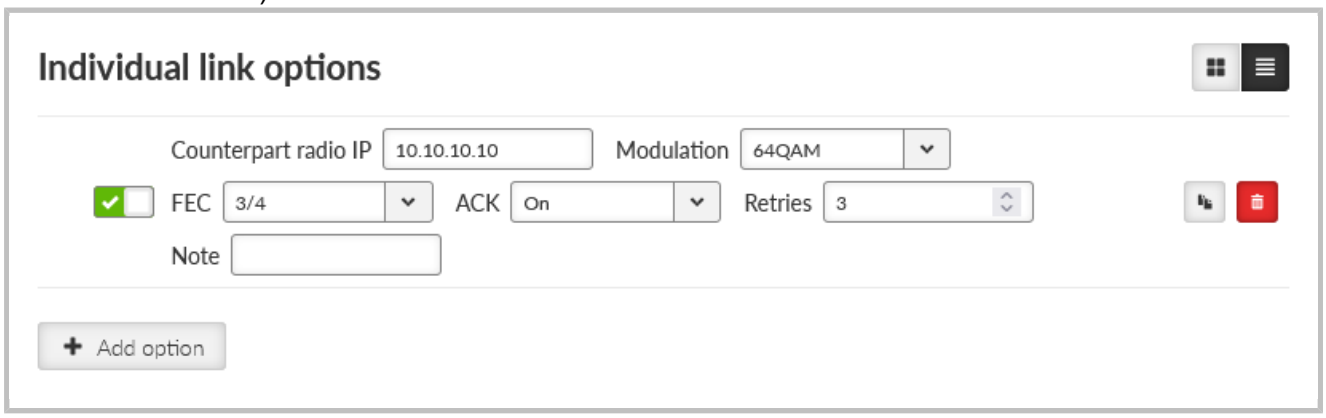
Retries
Number {0 – 15}, default = 3

Foreign packets RSS threshold [-dBm]
Number {50–150}, default = 120
When the received foreign packet (the packet which is not addressed to the actual unit) has weaker signal (the listed number bigger, e.g. the limit 120 - in minus dBm - compared with actual RSS -126 dBm), the channel is evaluated as free. If the foreign packet RSS is over this limit, the channel is occupied and the unit will wait till the end of it with the procedure of transmission.

Repeat COM broadcast
List box {On; Off}, default = "Off"
When On the broadcasted COM packets will be retranslated into the radio channel. When Off these packets will not be repeated.

7.1.2.7.1. Individual link option

It is possible to add some exceptions for radio links with particular conditions (e.g. longer or shorter ones than common).



The individual link is defined by **Counterpart radio IP**. For this link it is possible to set individually **Modulation, FEC, ACK, Retries.**

Retries are used to set a number of repeats, when the packet is not acknowledged (in case of ACK ON). The standard number of retries is 3.

Note

It is highly recommended to set common modulation to the lowest required modulation within the network. Modulation for Individual link is recommended to set higher, because broadcast frames are always transmitted over the common modulation.

7.1.2.8. Advanced radio parameters

The Advanced setting option allows to customize radio and radio protocol parameters. Typically these parameters should remain on default values.

These settings you can find in ADVANCED > Interfaces > Radio > menu

7.1.2.8.1. Radio interface - advanced

MTU [B]
Number {70 – 1500}, default = 1500 B
If a packet entering to an interface exceeds the maximum value, it is either discarded or fragmented.
Minimum MTU value to establish TCP between RipEX2 units = 576 B.
Minimum MTU value for IPv6 (Babel) = 1280 B.

Only for Flexible and Base Driven protocol

Gratuitous ARP broadcast
List box {On; Off}, default = "Off"
Enables regular sending of gratuitous ARP Reply broadcasts (notification of the radio's IP address to neighbors)

Gratuitous ARP interval
Number {1 – 24}, default = 2
Length of period [hours] of sending gratuitous ARP Reply

7.1.2.8.2. Radio channel - advanced

Maximal distance
Number {0 – 200}, default = 100
This parameter allows to set a maximal distance of a radio hop (in km). The same number shall be used for the whole network. We recommend to change the value only in case that the network uses radio hops longer than 100 km.

Resilience
List box {High sensitivity; Auto; High resilience; User}, default = "Auto"
RipEX2 is equipped with cognitive function of receiving mode selection. When exposed in a radio environment where strong interfering signals (stronger than -45 dBm) are present, RipEX2 senses them and adaptively increases its resistance to interference (by lowering its sensitivity by up to 2-3 dB).
Resilience parameter controls this functionality. By default the **Auto** is set - when intereference holds, RipEX2 stays in High resilience mode of receiver operation and signals this state by turning the yellow RX LED on. Once the interfering signals fade away, RipEX2 automatically returns to its High sensitivity mode of receiver operation. It is possible to switch this functionality permanently off (**High sensitivity**) or permanently on (**High resilience**).
The last option is to set this Resilience value to a fixed value from 0 to 31 dB (if the "User" option is specified).

High resilience LED indication
List box {On; Off}, default = "Off"
Enables indication of High resilience mode by yellow RX status LED.

Degradation detector sensitivity
Number {1.00 – 2.00}, default = 1.70
Setting the sensitivity (hysteresis) of the algorithm. The smaller, the greater the spacing between the thresholds for alarm occurrence and cancellation.

7.1.2.8.3. Queues

TX Buffers

The Radio protocol transmission buffer handles data waiting to be transmitted. Its size is defined by both the number of records (Queue length) and total storage space (Queue size) requirement. Records are held in a queue which is considered full, if either the Queue length or Queue size is reached. New incoming frames are not accepted when the queue is full.
The TX buffer is active for all radio protocols.
This functionality is available in ADVANCED > Interfaces > Radio > Queues menu

Queue length [packets]

Number {1 – 31}, default = 5
Queue length dictates the maximum number of records held in the queue.

Queue size [kB]

Number {1 – 48}, default = 5
Queue size dictates the total size of all records that can be held in the queue.

TX Buffer timeout enabled

List box {Off; On}, default = "Off "
The frames waiting for transmission in the Radio protocol output frame queue will be discarded after the TX Buffer timeout expires. This parameter should be enabled for types of applications where sending old frames brings no benefit.
When the frame is discarded the event is recorded, both in the statistics (as “Rejected”) and in the monitoring (the respective frame is displayed with the “Tx buffer timeout” tag).

TX Buffer store timeout [s]

Number {0.01 – 150}, granularity 0.01, default = 5
Radio protocol transmit buffer timeout. The “TX Buffer timeout” must be enabled for this parameter to be initiated.

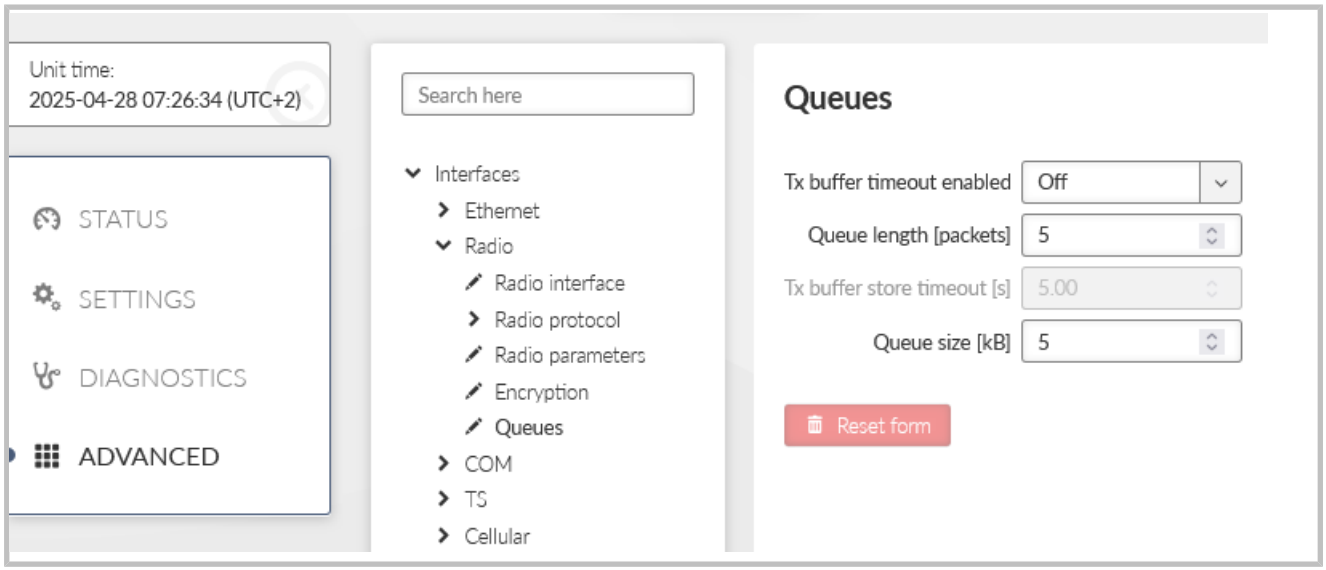


Fig. 7.4: ADVANCED > Interfaces > Radio > Queues

7.1.2.8.4. Flexible protocol - advanced

This settings allows to customize individual length and numbers of slots used for accessing of the radio channel or waiting with retransmissions of an undelivered packet.

The length of the slots has to be same in all radio units within on radio network. It is highly recommended to consult changes of these parameters with our technical support.

7.1.3. COM

Data incoming to the RipEX2 unit from the COM port are received by the Protocol module. The Protocol module behavior depends on the Protocol selected. In case of Transparent protocol (available in Bridge mode only), it is transparently transmitted to the RipEX2 network and sent out through all COM ports with Transparent protocol selected. If any other protocol is selected, the incoming frame from the COM port is processed by the Protocol module, translated into UDP frame, forwarded to the RipEX2 router module and further processed according to router rules. Such UDP frames received by the RipEX2 unit from the RipEX2 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.

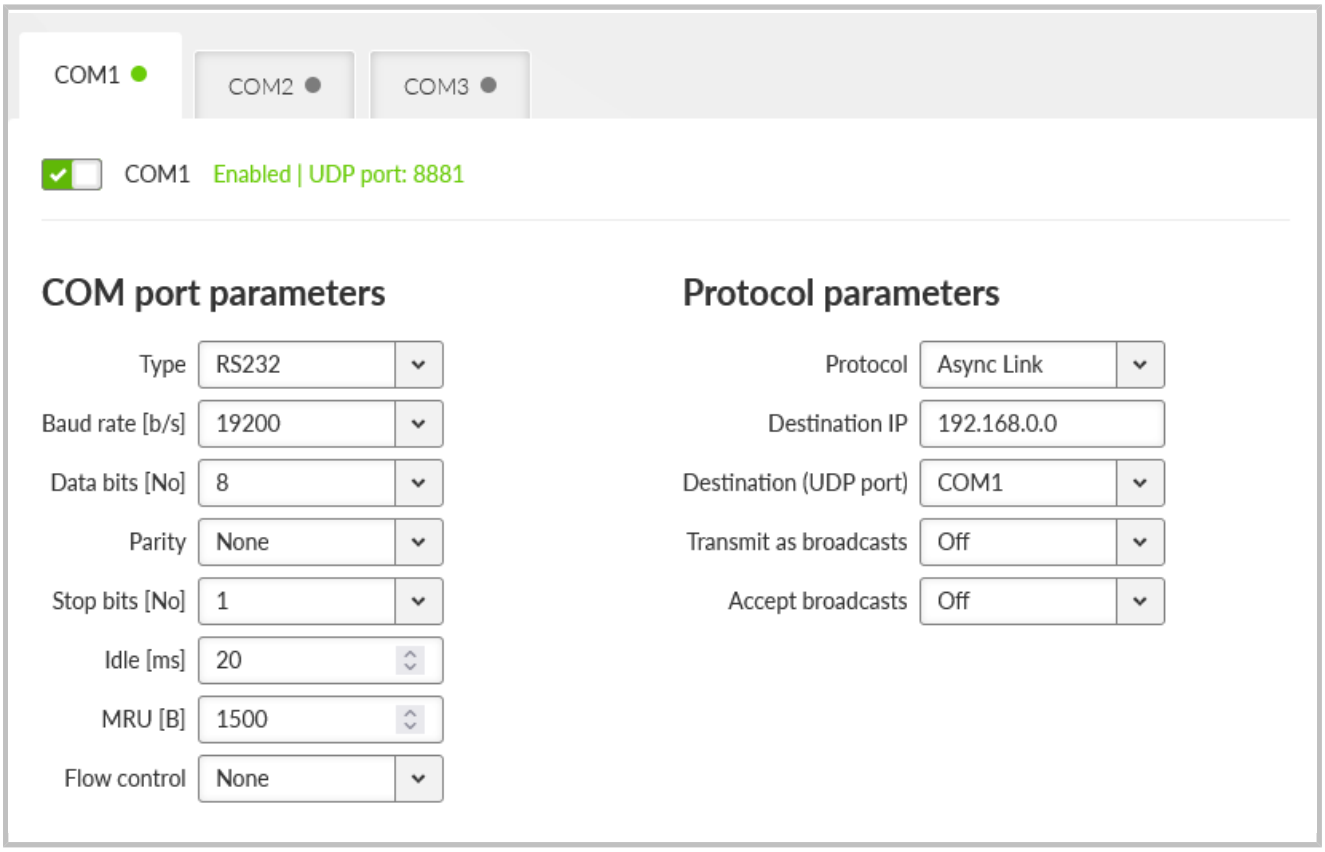


Fig. 7.5: SETTINGS > Interfaces > COM

The menu is divided to two parts:

7.1.3.1. COM port parameters

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



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

1. Very long frames (>800 B) require good signal conditions on the Radio channel and the probability of a collision increases rapidly with the length of the frames. Hence if your application can work with smaller MTU, it is recommended to use values in 200 – 400 bytes range.

Note

2. This MRU and the MTU in Radio 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 RipEX2 (DCE - Data Communications Equipment) can be enabled in order to pause and resume the transmission of data. If RX buffer of RipEX2 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.

7.1.3.2. 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 RipEX2 Radio network. The same settings are valid for Terminal servers as well (for more details about TS see *Section 7.1.4, “Terminal servers”*).



Protocol

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

Transparent protocol can be used when unit operates in Bridge mode only. All the traffic is bridged transparently to RipEX2 network.

Broadcast

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

Some Master SCADA units sends broadcast messages to all Slave units. SCADA application typically uses a specific address for such messages. RipEX2 (Protocol module) converts such message to a customized IP broadcast and broadcasts it to all RipEX2 units resp. to all SCADA units within the network.

Broadcast address

Number {0 – 65535}, default = 255

The protocol address which is treated as broadcast address.

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



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-

tination IP address belongs to a RipEX2 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 RipEX2, the packet is discarded.

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



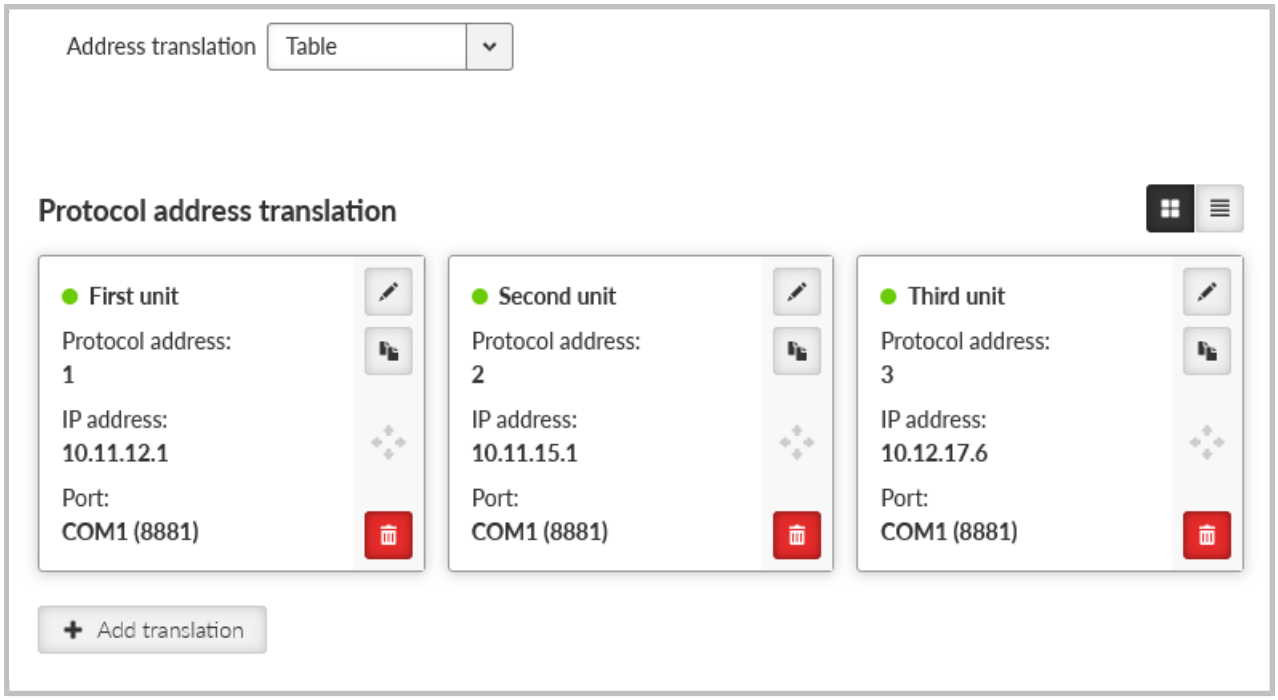
Note
All IP addresses used have to be within the same subnet, which is defined by this Mask
The same UDP port is used for all the SCADA units, which results in the following limitations:

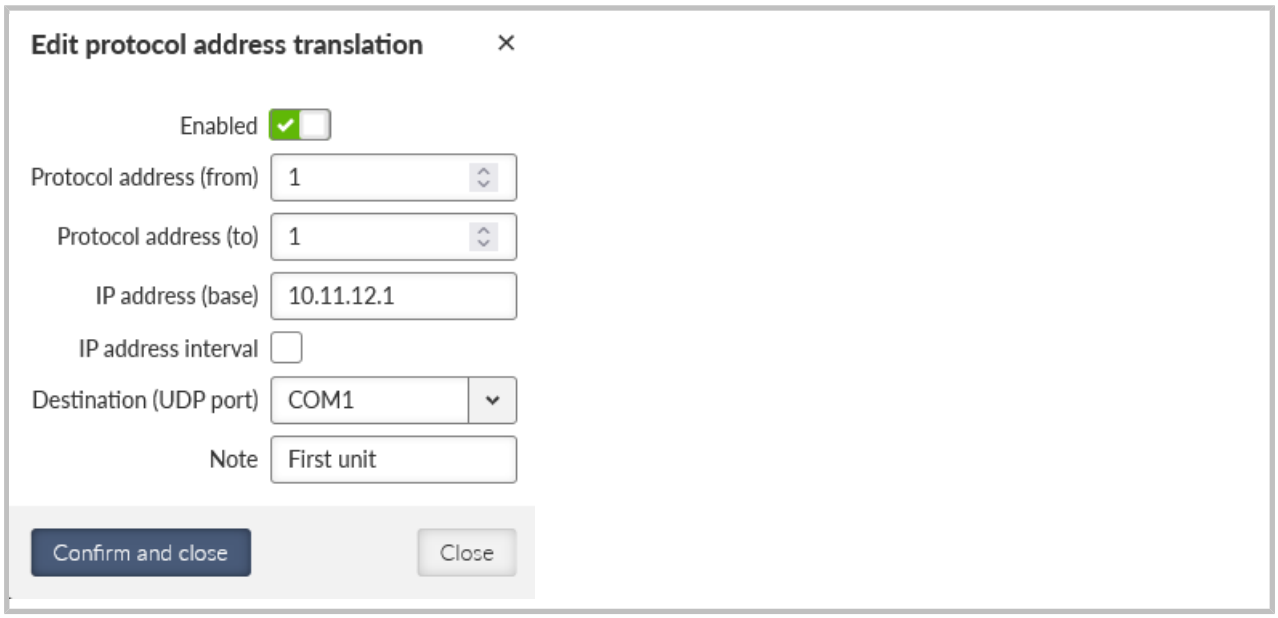
SCADA devices on all sites have to be connected to the same interface

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.





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

7.1.3.3. 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.

7.1.3.3.1. None

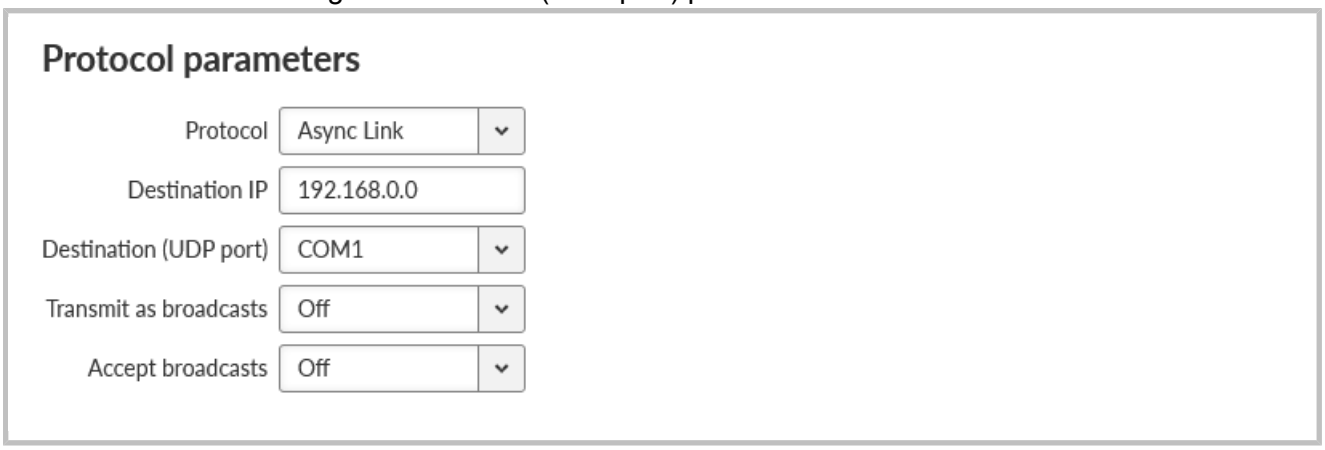
The None protocol switches the COM port off. All incoming data will be thrown away, no data will be sent into the COM interface.

7.1.3.3.2. Transparent protocol

Operates in Bridge mode only. All the traffic is bridged transparently to RipEX2 network (see *Section 5.1, "Bridge mode"* for details).

7.1.3.3.3. Async link

Async link creates an asynchronous link between two COM ports on different RipEX2 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.



Destination IP
Defines destination IP address of RipEX2.

Transmit as broadcasts
List box {On; Off}, default = "Off"
Allows sending of the packets incoming from COM port as broadcast.

Accept broadcasts
List box {On; Off}, default = "Off"
On: Broadcast packets from the radio channel will be send to the COM port.
Off: Only unicast packets will be sent to the COM port.

7.1.3.3.4. COMLI

COMLI is a serial polling-type communication protocol used by Master-Slave application. When RipEX2 radio network in Router mode is used, more COMLI Masters can be employed within one Radio network 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 is not fully compatible on COM port with RipEX and MR modems. RipEX2 implementation is not supporting “Intercharacter tx delay”.

Mode of Connected device: MASTER



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

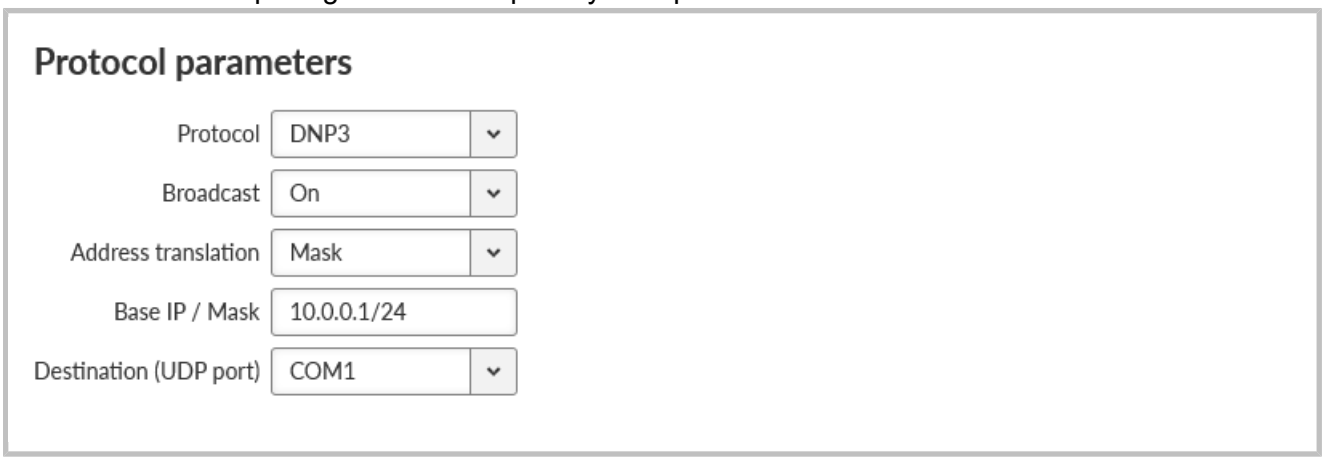


Response timeout [ms]
Number {0 – 16383}, default = 1000
COMLI protocol response timeout is used for waiting on COM port for the response of connected device.

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).

7.1.3.3.5. 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 RipEX2 configuration. The DNP3 allows both Master-Slave polling as well as report-by-exception communication from the remote units.



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

Broadcast
List box {On; OFF}, default = "On"

Note
There is not an option to set the Broadcast address, since DNP3 broadcast messages always have addresses in the range 0xFFFD - 0xFFFF. Hence when Broadcast is On, packets with these destinations are handled as broadcasts.

7.1.3.3.6. 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 RipEX2 configuration.



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

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 nor received.

ACK timeout [ms]

Number {0 – 1683}, default = 1000

Timeout of waiting for ACK.

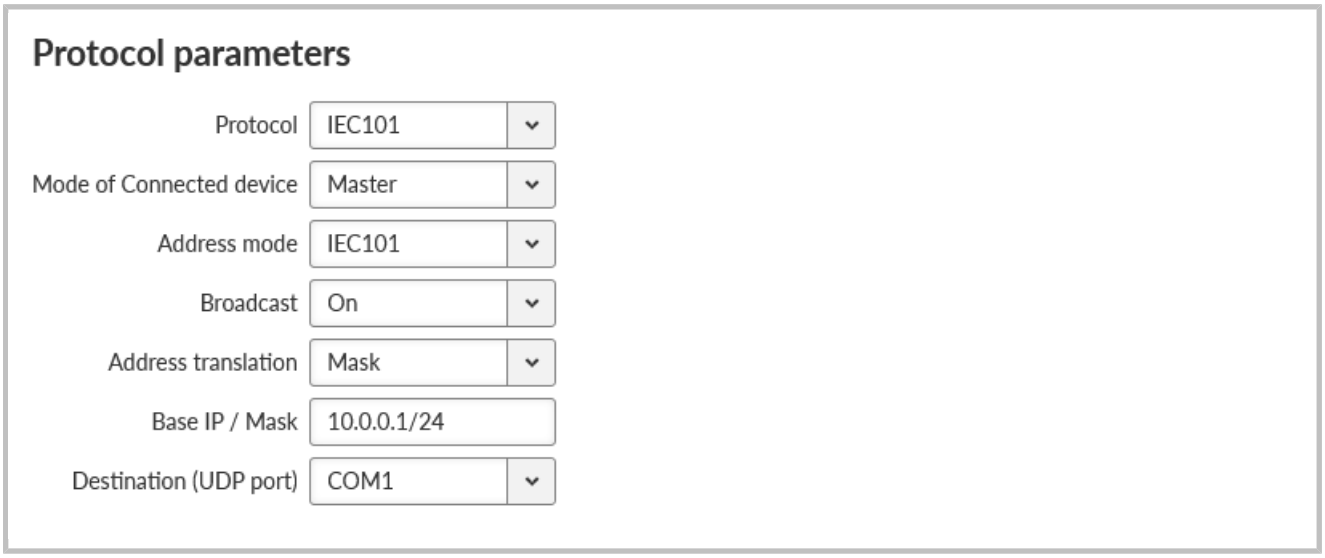
Block control mode

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.

7.1.3.3.7. IEC101



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”

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

7.1.3.3.8. 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

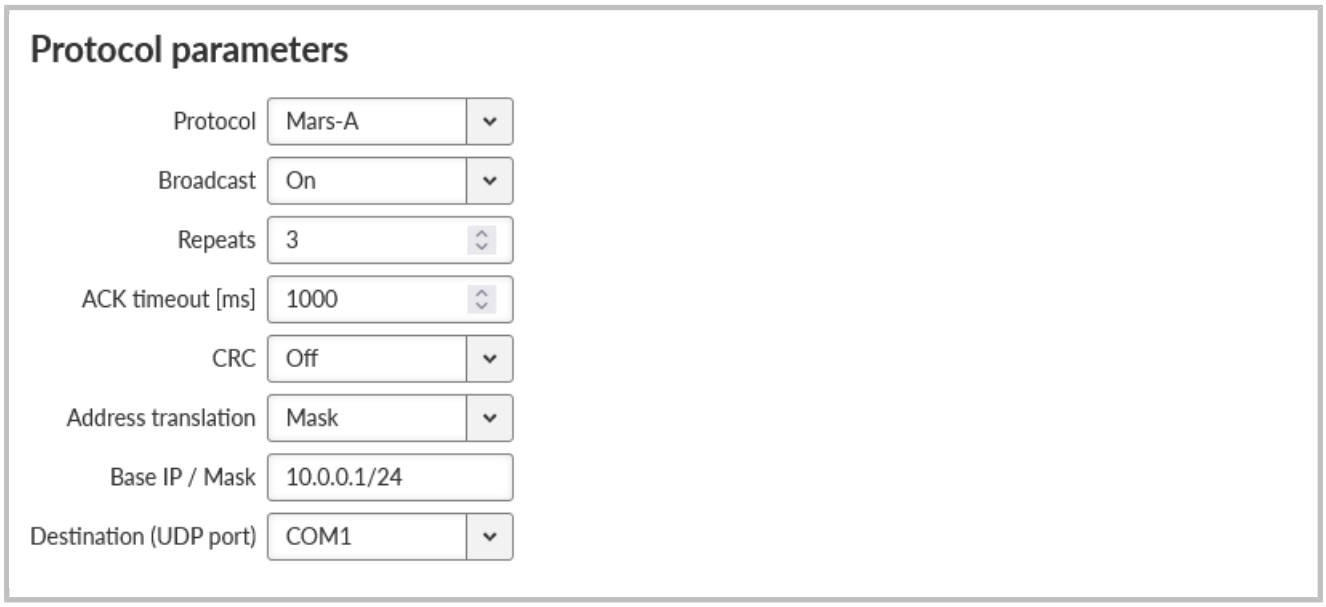
MARS-A was widely used by legacy RACOM radio modems in the MORSE system from the year 1999.

The new implementation of this protocol in RipEX2 or M!DGE3 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.



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.

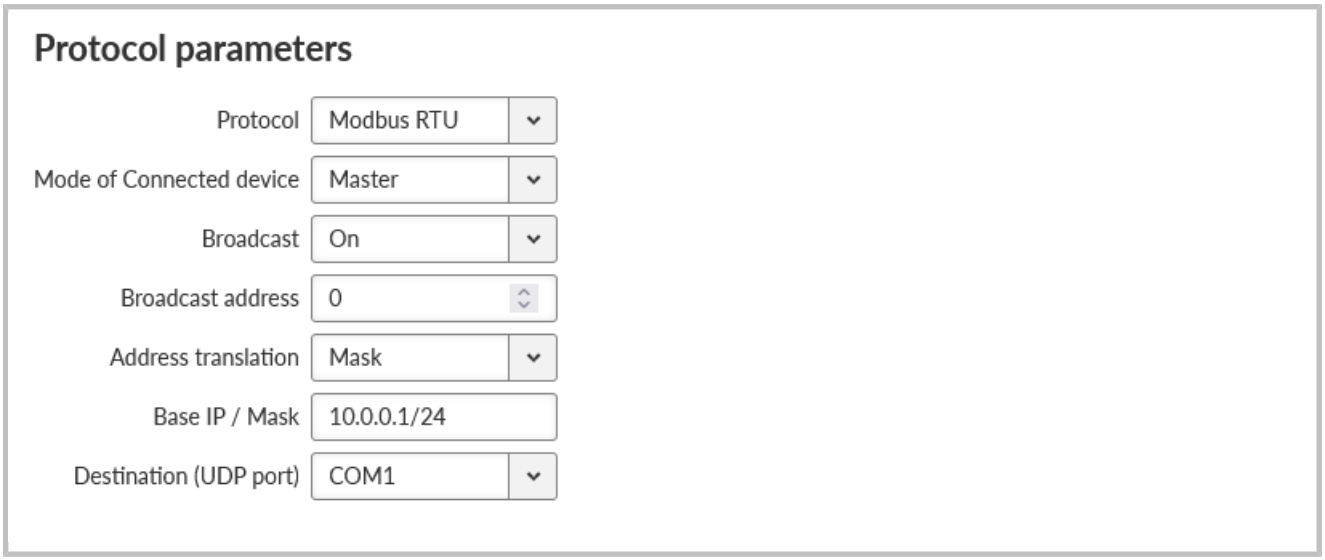
Security bit
List box {On; Off}, default = "Off"
Needed for compatibility with legacy MORSE network implementations. This parameter does not change protocol behavior.

CRC
List box {On; Off}, default = "Off"
Error detection algorithm:
- On - CRC algorithm is used
- Off - XOR algorithm is used

7.1.3.3.9. Modbus RTU

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

When RipEX2 radio network run in Router mode, more Modbus Masters can be used within one Radio network and one Slave can be polled by more Masters.



Mode of Connected device

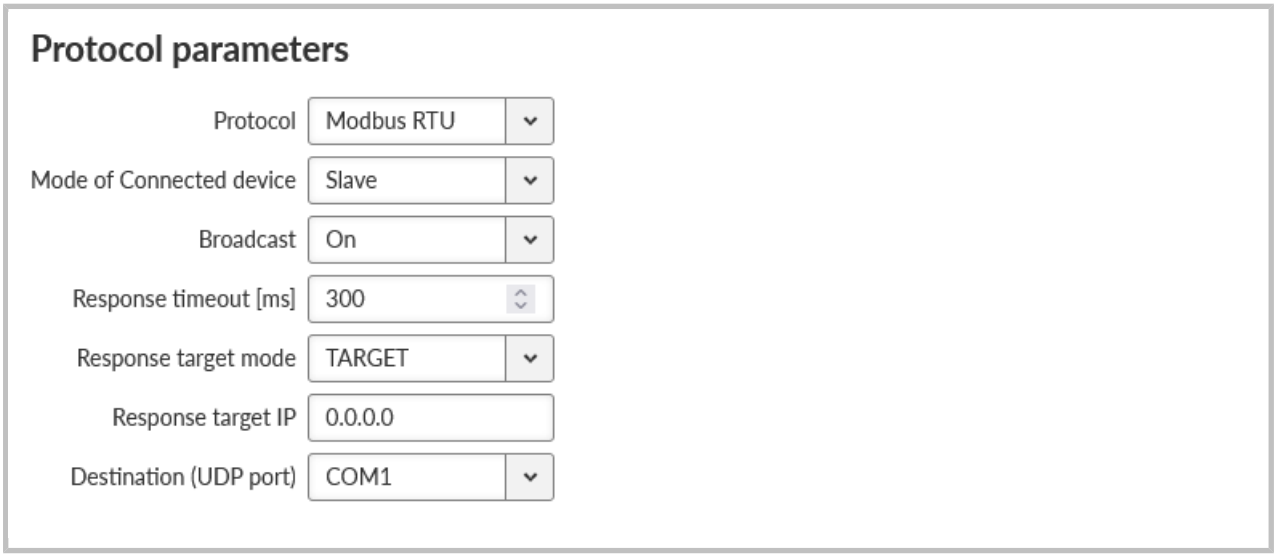
List box {Master; Slave}, default = "Master"

Mode of connected device: MASTER

Broadcast address

It is possible to set address, which will be handled as a broadcast address while Broadcast = "On". Default broadcast address of the Modbus RTU protocol is 0.

Mode of connected device: SLAVE



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 Radio 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.

7.1.3.3.10. PPP protocol

The PPP protocol (Point-to-Point Protocol, specified in RFC 1661) is intended for a direct duplex connection between two network points. It works at the link layer as an extension of the HDLC protocol. Both network points receive a configuration on the basis of which they negotiate connection properties with each other over the serial line. The consequence of a successful negotiation is the creation of network interfaces on both sides. Depending on the selected network protocol, these can be interfaces of different types. In our case, the IPCP protocol (IPV6CP) is used and the resulting interface is of the TUN type (e.g. ppp1). The interface is assigned an IP address according to the configuration and user data are transferred through it. PPP encapsulation is used to encapsulate IP packets into frames transmitted over a serial line (see Frame format, RFC 1662).

7.1.3.3.10.1. Typical course of establishing a connection

Line Parameter Negotiation (LCP)

Basic connection parameters at the serial line level
LCP (Link Control Protocol, RFC 1661)
Negotiated parameters:

- Maximum receive unit (MRU)
- Asynchronous Control Character Map (ACCM)
- Authentication protocol
- Compression of the protocol field in the PPP frame header
- Compression of the address and control fields in the PPP frame header

Authentication

Optional, if negotiated, the appropriate protocol will be used
It can be two-sided, where each side may require a different protocol
Protocols:

- PAP (Password authentication protocol)
- CHAP (Challenge Handshake Authentication Protocol)

Negotiation of data compression parameters (CCP)

Data compression type and parameters
Compression Control Protocol (CCP, RFC 1962)

Network Protocol (NCP) Negotiation

Connection parameters at the network layer level
Network Control Protocol (NCP):

- IPCP (Internet Protocol Control Protocol, RFC 1332)
- IPv6CP (IPv6 Control Protocol, RFC 5072)

7.1.3.3.10.2. Format of frames

The format of PPP frames (RFC 1661, RFC 1662) is based on the HDLC protocol standard.

7.1.3.3.10.3. Common frame format

Flag	Address	Control	Protocol	Information	Padding	FCS	Flag
0x7E	0xFF	0x03	8/16 bits	*	*	16/32 bits	0x7E

7.1.3.3.10.4. Meaning of individual fields

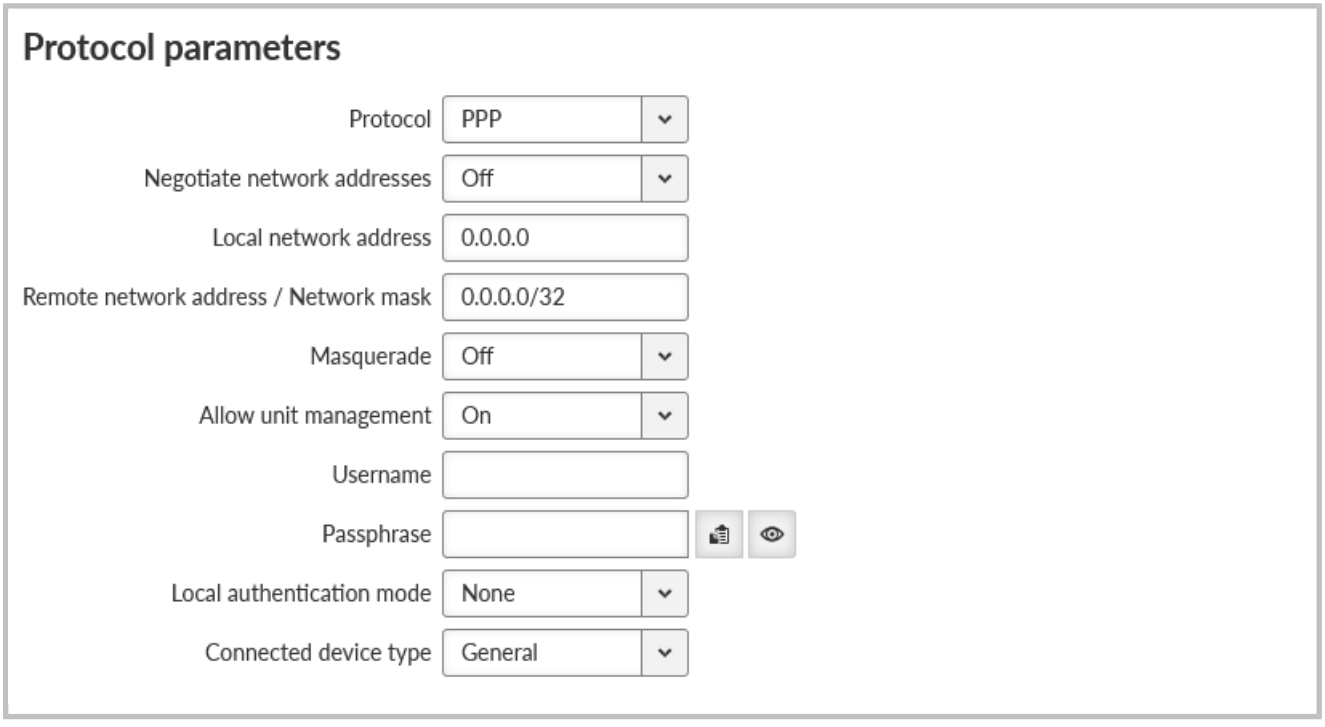
- **Flag**: value 0x7E defined in the protocol specification
- **Address field**: address field, value 0xFF defined in the protocol specification
- **Control field**: control field, value 0x03 defined in the protocol specification
- **Protocol field**: protocol field, indicates the type of data in the Information field
  - Example: 0xC021 for LCP, 0xC023 for PAP
- **Information**: encapsulated data
  - Example: IP packet
- **Padding**
- **Frame Check Sequence (FCS) field**: control sequence for detecting transmission errors

7.1.3.3.10.5. Configuration

Some configuration items are closely related to the native parameters of the pppd daemon. Individual parameters are listed in the text below in bullet points marked "pppd:" and detailed information about them can be found in the daemon's manual pages.

"<NR>" is used to indicate the PPP index (1/2/3).

7.1.3.3.10.6. Protocol parameters



Negotiate network addresses
List box {On; Off}, default = ”Off”
Enables local/remote PPP interface address negotiation.
If disabled Local network address and Remote network address must be set manually.

Local network address
IP address; default = 0.0.0.0
Local IP address of the PPP interface

Remote network address / Network mask

IP address; default = 0.0.0.0/32

Remote IP address and mask of the PPP interface. Address and Mask are used to determine the target range of a rule routing to the PPP interface

Masquerade

List box {On; Off}, default = ”Off”

Enables/disables Source NAT (masquerade) on packets sent over the PPP interface.

With masquerade enabled, packets leaving the station over the PPP interface are rewritten with the source address to the address assigned to that interface

Allow unit management

List box {On; Off}, default = ”On”

Enables unit management access via PPP interface

Username

String {up to 50 char}, default = <empty>

The username to use when authenticating to the counterparty, regardless of the protocol that is required.

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Passphrase

String {up to 50 char}, default = <empty>

The passphrase to use when authenticating to the counterparty, regardless of the protocol that is required.

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Local authentication mode

Selection of the protocol with which the counterparty is to be authenticated when establishing a connection.

For PAP (legacy) and CHAP options, the credentials set by **Local authentication username** and **Local authentication password** are used

Local authentication username

String {up to 50 char}, default = <empty>

The username that the counterparty should use during authentication (see **Local authentication mode**).

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Local authentication password

String {up to 50 char}, default = <empty>

The password that the counterparty should use during authentication (see **Local authentication mode**).

Printable ASCII characters are allowed, with the exception of the prohibited ", `, \, $, ;

Connected device type

List box {General; TETRA terminal (Motorola MTM5x00)}, default = ”General”

Connected device type. Sets the corresponding command sequence to switch the connected device to PPP mode.

Negotiate network addresses must be enabled for TETRA.

Advanced menu parameters:

Asynchronous control character map
Number {0 – 65535}, default = 0
Async-Control-Character-Map (ACCM) settings.
A non-zero value can be used to select control characters that the counterparty should not include in sent PPP packets.

LCP keepalive failure count
Number {0 – 255}, default = 0
A non-zero value means the maximum number of sent LCP echo-request messages before the peer is marked as disconnected and the connection is closed (see **LCP keepalive interval** [s]).
A zero value disables the function.

LCP keepalive interval [s]
Number {0 – 255}, default = 10
Interval of sending LCP echo-request messages, to which the counterparty responds with an LCP echo-reply message in normal state.
Along with that entry **LCP keepalive failure count** can be used to detect if a party is connected
Active if **LCP keepalive failure count** is greater than 0

Idle timeout to reconnect [s]
Number {0 – 65535}, default = 0
Disconnects an inactive connection after a defined period of time

Enable using modem control lines
List box {On; Off}, default = ”Off”
Option to use "modem control lines" (DTR/DSR serial port signals).

Enable control messages logging
List box {On; Off}, default = ”Off”
Option to verbose pppd daemon control messages.
Messages are written to the standard log /var/log/pppd_<NR>/log, which is available in a Diagnostic package.

Compression negotiation mode
List box {Automatic; Manual}, default = ”Automatic”
Mode for selecting configuration parameters related to compression (all remaining items below). When Automatic is selected, the configuration items below are ignored and the pppd daemon uses its default values. When Manual is selected, the configuration items below are active and their values are used by the pppd daemon when negotiating with the counterparty.

Enable address and control field compression
List box {On; Off}, default = ”On”
Choice of whether to negotiate address and control field compression in the PPP frame header (Address/Control field compression, see Frame format), in both directions of data transfer.
Active if **Compression negotiation mode** is Manual.

Enable protocol field compression
List box {On; Off}, default = ”On”
Choice of whether to negotiate protocol field compression in the PPP frame header (Protocol field compression, see Frame format), in both directions of data transfer.
Active if **Compression negotiation mode** is Manual.

Van Jacobson IP header compression max slots
Number {0; 2 – 16}, default = 16

Option of Van Jacobson compression of IP headers.
A non-zero value is a parameter of the compression algorithm (number of connection slots).
A zero value disables the function.
Active if **Compression negotiation mode** is Manual.

Enable compression control protocol
List box {On; Off}, default = ”On”
Option to use CCP (Compression Control Protocol) to negotiate data compression parameters.
The option to disable CCP is provided for compatibility with legacy PPP clients that do not support data compression.
Active if **Compression negotiation mode** is Manual.

BSD data compression receive code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "BSD-Compress" algorithm for data compression in the incoming direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

BSD data compression transmit code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "BSD-Compress" algorithm for data compression in the outgoing direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

Deflate data compression receive code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "Deflate" algorithm for data compression in the incoming direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

Deflate data compression transmit code size
Number {0; 9 – 15}, default = 15
A non-zero value is a parameter of the "Deflate" algorithm for data compression in the outgoing direction.
A zero value disables the function.
Active if **Compression negotiation mode** is Manual and **Enable compression control protocol** is disabled.

7.1.3.3.10.7. Routing

Routing Mode
The listbox is extended with PPP <NR> options
If the routing rule has one of the PPP <NR> options selected, routing is done to the appropriate PPP interface.

Routing Persistent
List box {On; Off}, default = ”Off”

The routing rule is persistent (see Cellular configuration for detailed explanation).

7.1.3.3.10.8. Protocol status

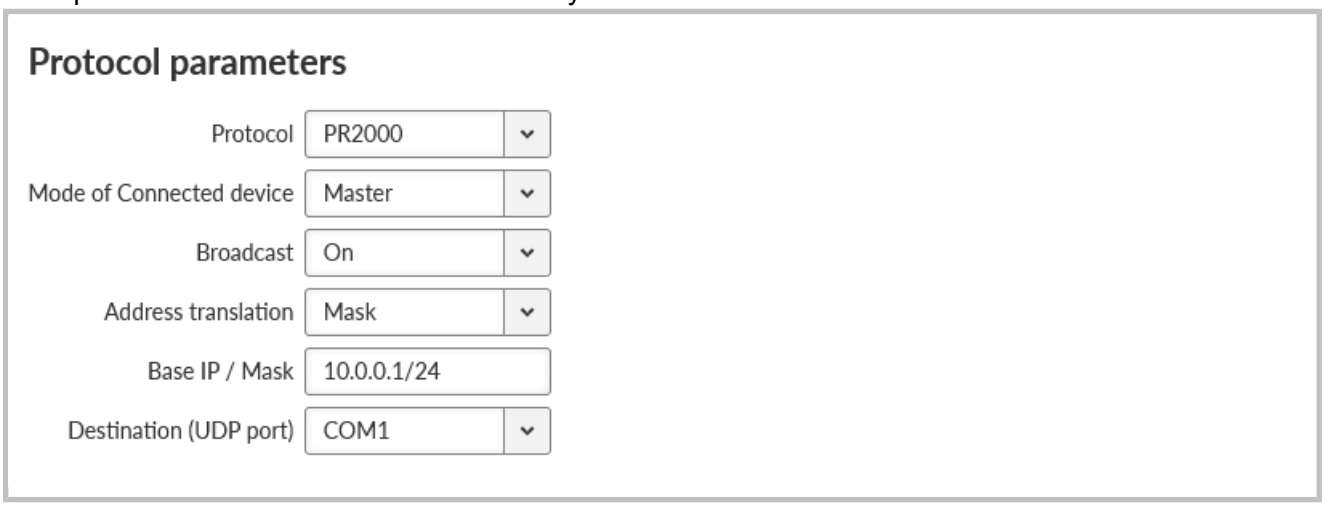
PPP status information is available in the Diagnostics > Information > Interfaces > PPP menu. Status provides following information

- Interface
  - PPP Interface name.
- State
  - Current state of the PPP interface daemon.
- Peer MRU
  - Maximum receive unit (MRU) in bytes requested during negotiation by the counterparty.
- Peer Auth. mode
  - Authentication protocol requested by counterparty.
- Peer ACCM
  - ACCM setting requested by counterparty.
- Negotiated compression options
  - Negotiated options of PPP compression.

7.1.3.3.11. 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 network in their entirety.



7.1.3.3.12. Siemens 3964(R)

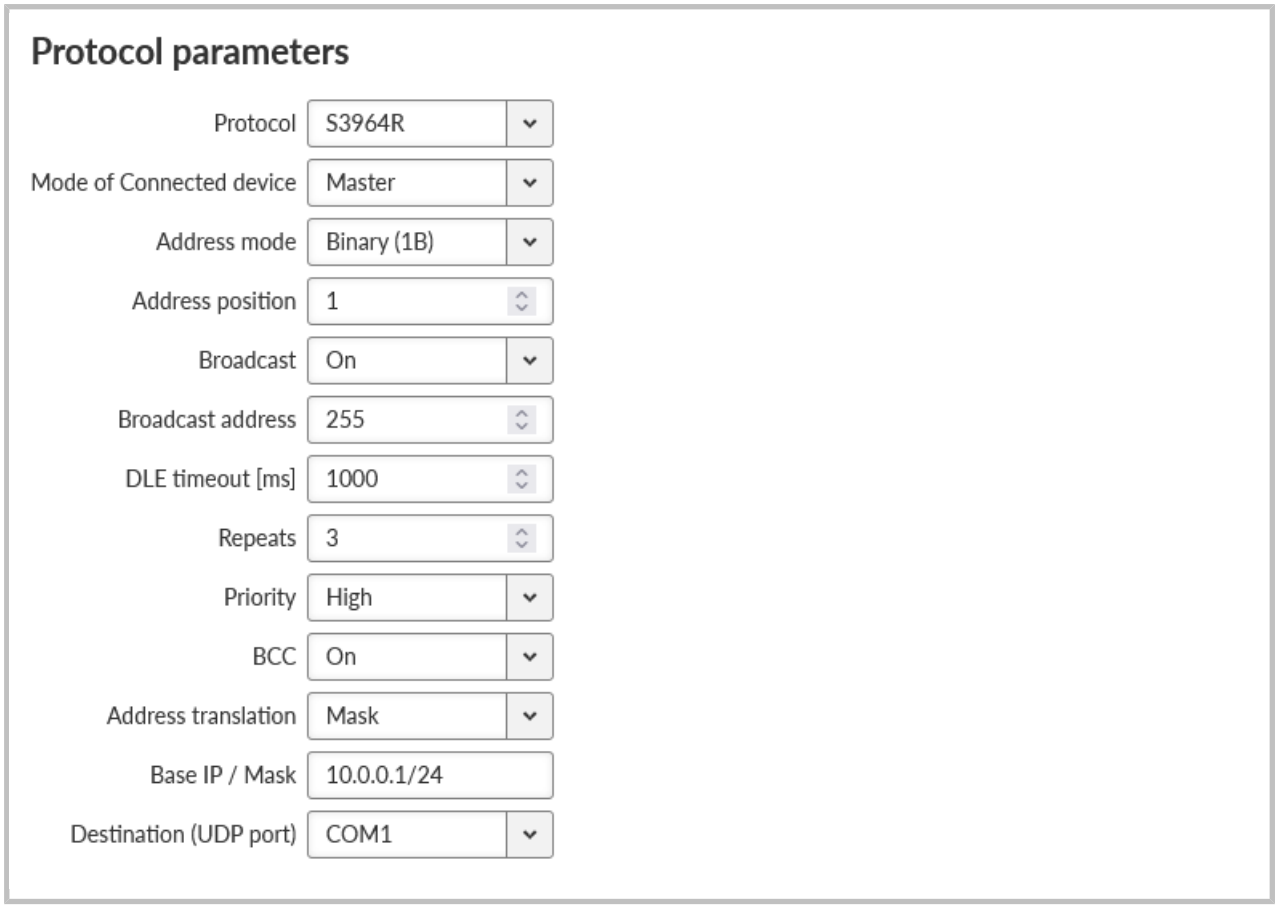
The 3964 protocol is utilized by the Siemens Company as a Point-to-Point connection between two controllers. Meanwhile it has developed into an industry standard that can be found on many devices as a universal communications interface. 3964R is the same as 3964, in addition it only uses BCC (Block Check Character). 3964(R) handles only the link layer (L2 in OSI model), hence RipEX2 uses a similar way to read “SCADA address” as in UNI protocol.

There is a handshake STX(0x02) – DLE(Ox10) on the start of communication and DLE+ETX – DLE on the end. This handshake is performed by RipEX2 locally, it is not transferred over the RipEX2 network.

Communication goes as follows:
LocalRTU −> STX −> Local RipEX2
LocalRipEX −> DLE −> LocalRTU
LocalRTU −> DATA+DLE+ETX+BCC −> Local RipEX2
LocalRipEX −> DATA −> Remote RipEX2*
Local RipEX2 −> DLE −> LocalRTU
Remote RipEX2 −> STX −> RemoteRTU
RemoteRTU −> DLE −> Remote RipEX2
Remote RipEX2 −> DATA+DLE+ETX+BCC −> RemoteRTU
RemoteRTU −> DLE −> RemoteRipEX

* only this packet is transferred over the RipEX2 network, all the other ones are handled locally.

Master



Address mode

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

RipEX2 reads the Protocol address in the format and length set (in Bytes).

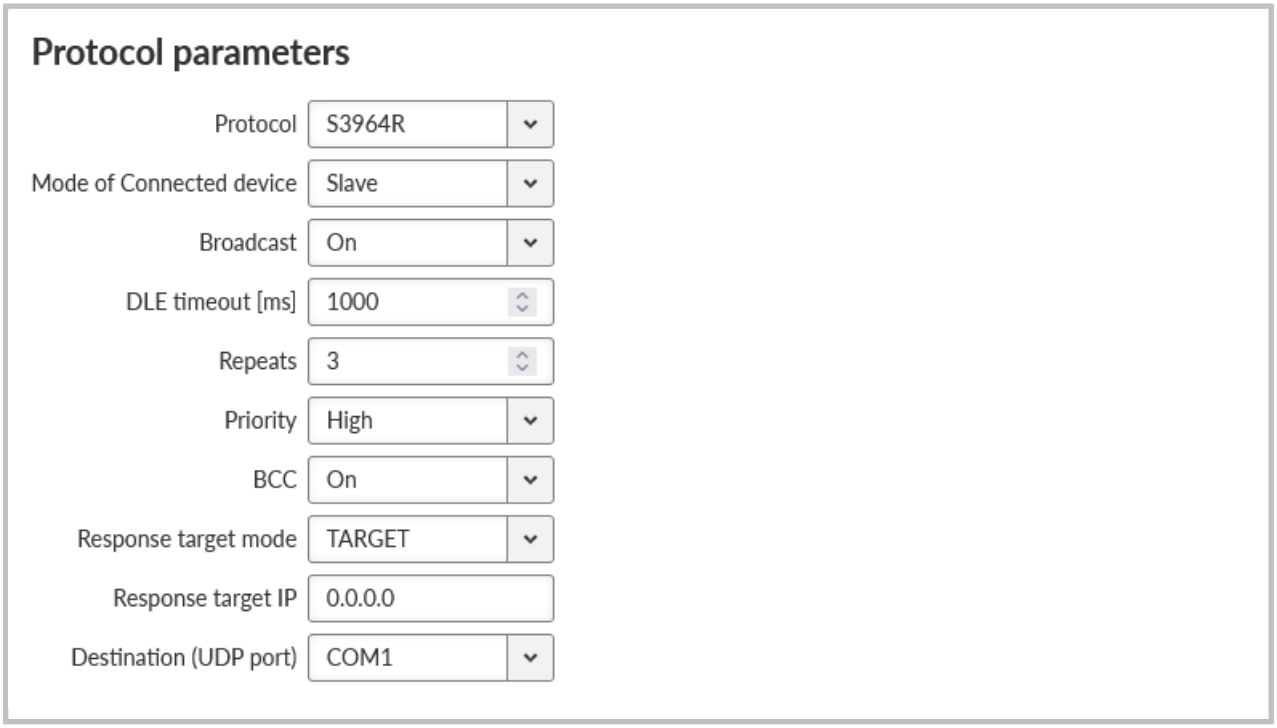
Address position

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



DLE timeout [ms]

Number {300 – 8190}, default = 1000
RipEX2 expects a response (DLE) from the connected device (RTU) within the set timeout. If it is not received, RipEX2 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, RipEX2 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, RipEX2 waits for DLE. When it is Low, RipEX2 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.

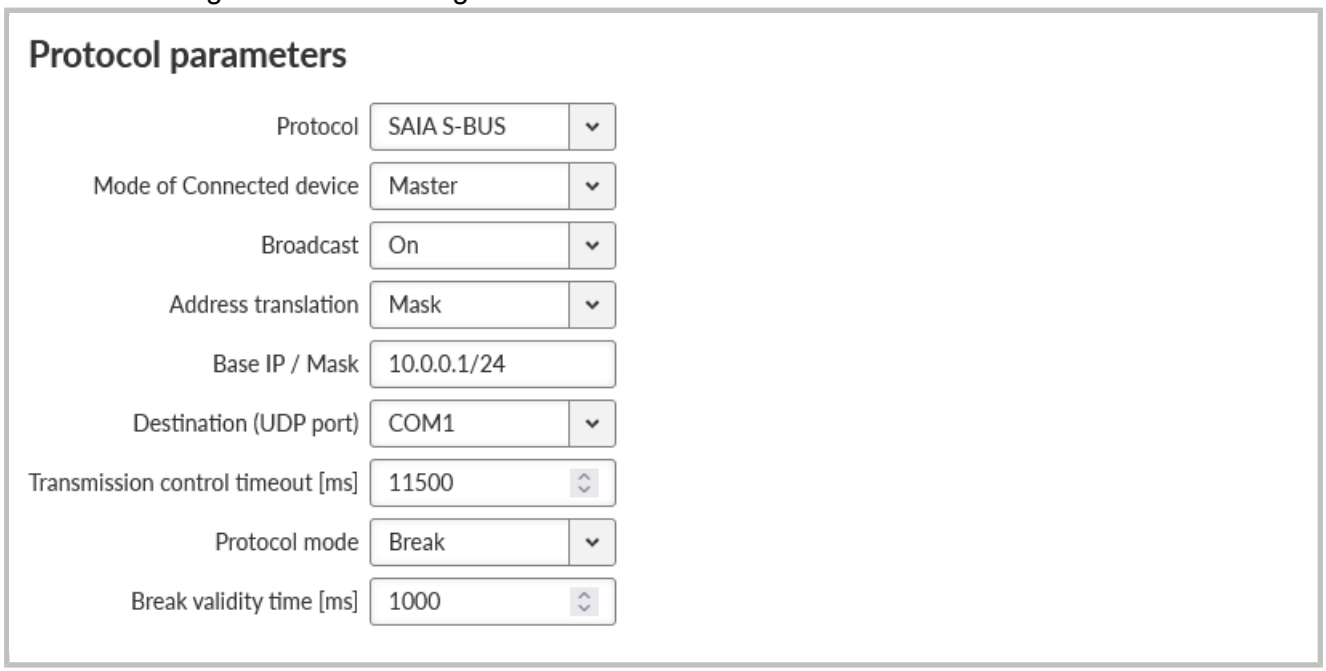
BCC

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.
RipEX2 checks (calculates itself) this byte while receiving a packet on COM. RipEX2 transmits DLE (accepts the frame) only when the check result is OK. BCC byte is not transferred over the RipEX2 network, it is calculated locally in the end RipEX2 and appended to the received data.

7.1.3.3.13. 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 data addressed to 255 is processed as broadcast.

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.



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).

Broadcast

List box {On; Off}, default =”On”

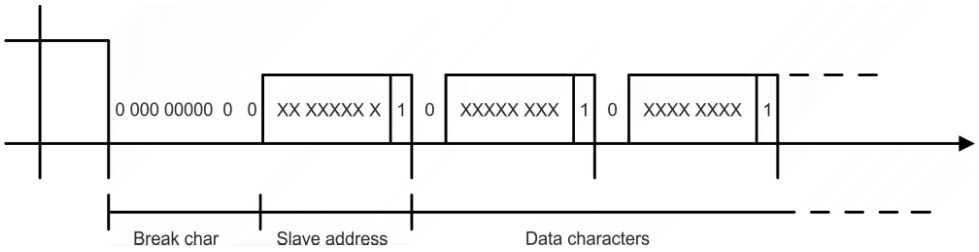
When **On**, the 255 address is treated as a broadcast, When **Off**, the 255 address is ignored.

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.

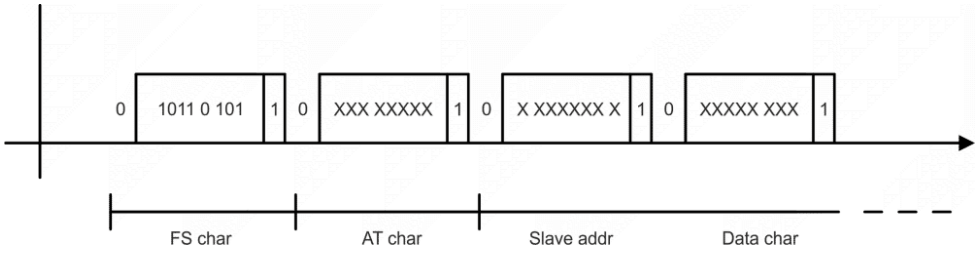


Break mode is available only with COM port, it is not implemented on TS (the break signal is not available there). The Break signal check is very rough (with step of 100 ms) due to Linux kernel limitations.

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* [2]

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

[2] https://www.racom.eu/eng/support/prot/sbus/index.html

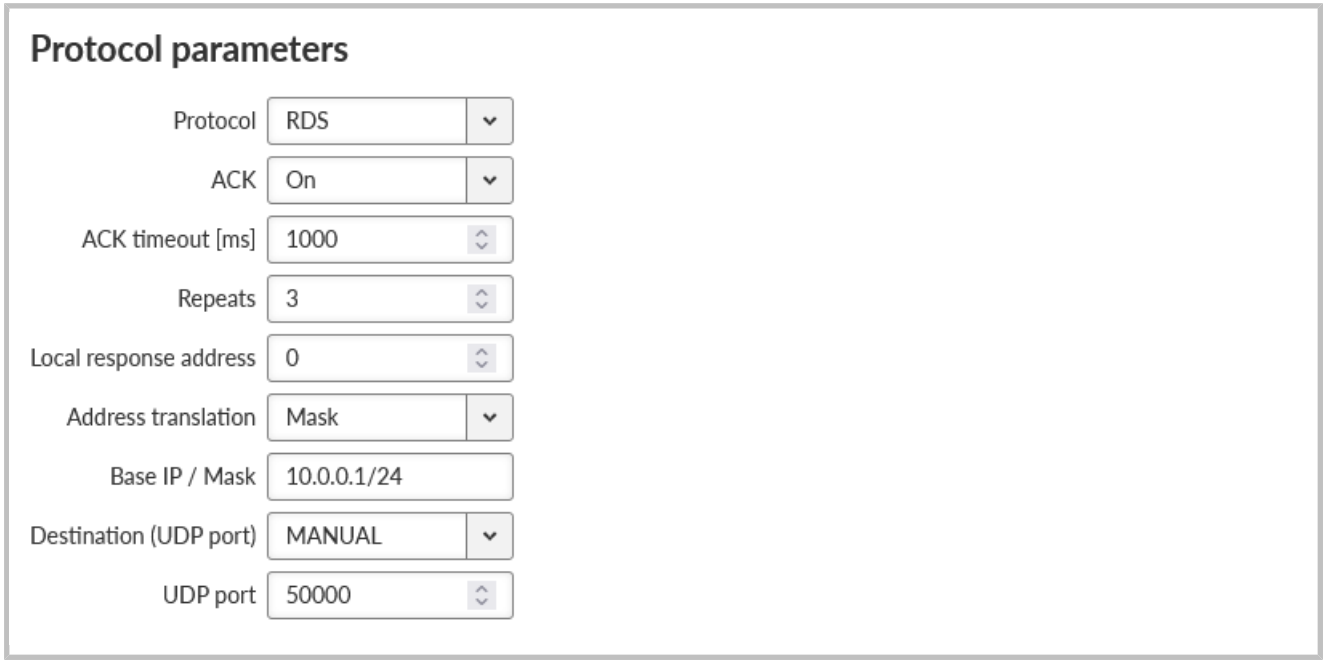
Slave's response timeout - waiting for response, otherwise the reply to master is resent.

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.

7.1.3.3.14. 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 Radio channel and sent to COM1-3 or Terminal server 1-5 according to UDP port settings and vice versa - from wire to Radio channel.



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, RipEX2 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.

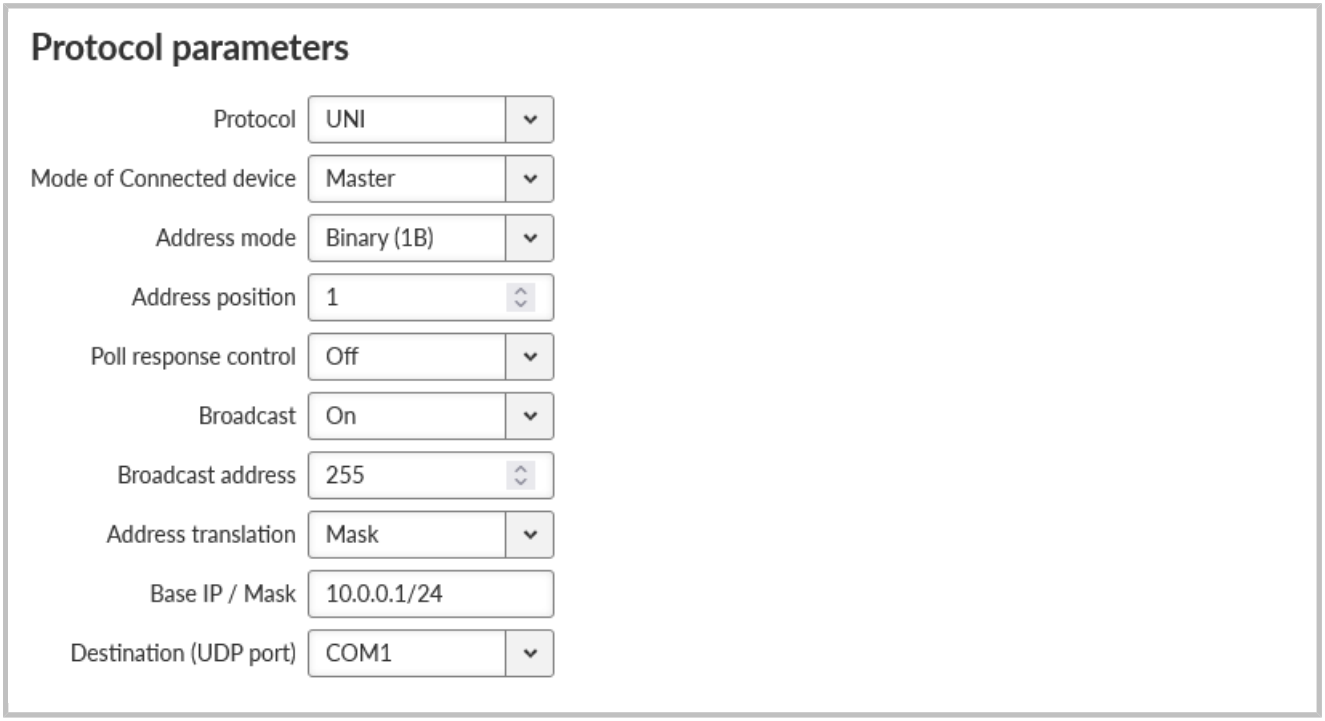
Repeats
Number {0 – 31}, default = 3
Number of frame re-transmissions.

Local response address
Number {0 – 255}, default = 0
This address is used only with status query (0x51). Response of RipEX2 is "0x54 <Local response address> 0x00".

7.1.3.3.15. UNI

UNI is the 'Universal' protocol utility designed for RipEX2. It is supposed to be used when the required application protocol is not available in RipEX2 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.



Mode of Connected device
List box: {Master, Slave}, default = Master

Adress 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 hexa-decimal 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



Accept broadcasts

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

"On" – Broadcast packets received at the radio channel are forwarded to the COM port.

"Off" – Broadcast packets (received at the radio channel) are discarded. Unicast packets are forwarded to the COM port.

7.1.4. Terminal servers

Generally, a Terminal Server (also referred to as a Serial Server) enables connection of devices with serial interface to a RipEX2 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 RipEX2, user data extracted from TCP messages and processed like it comes from a COM port. When data reaches the destination RipEX2, it can be transferred to the RTU either via a serial interface or via TCP (UDP), using the Terminal server again.

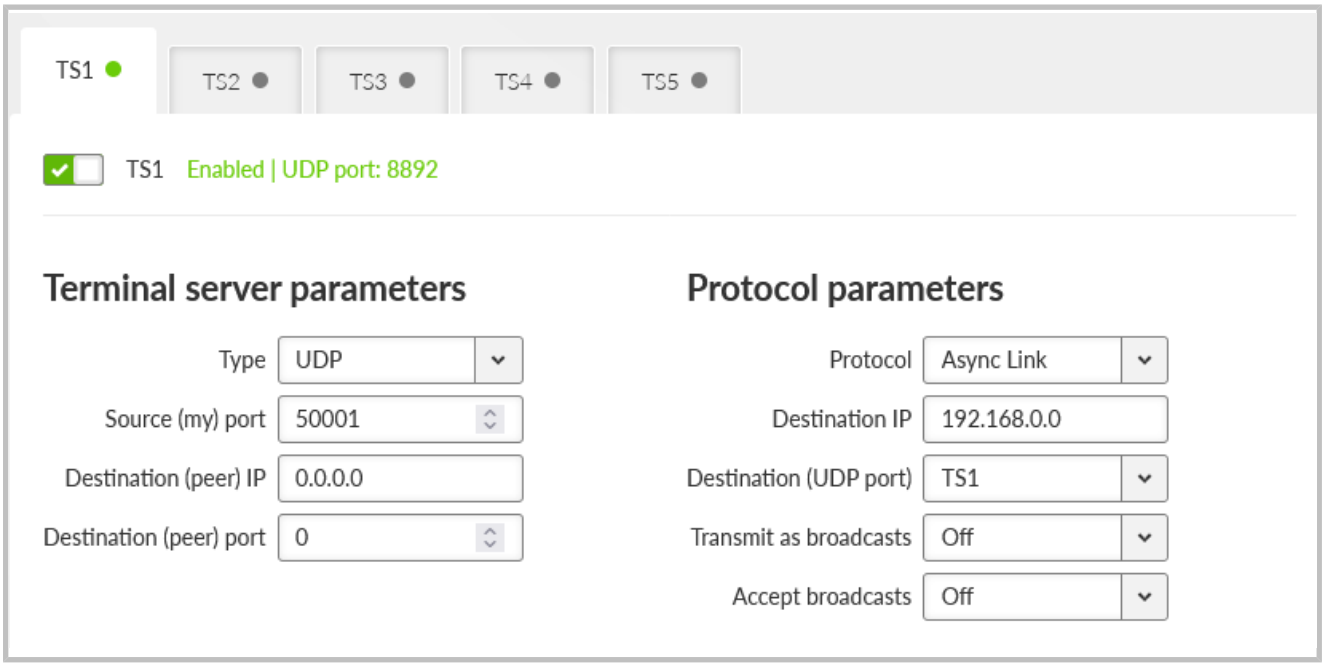


Fig. 7.6: SETTINGS > Interfaces > Terminal servers

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 RipEX2 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 RipEX2 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. RipEX2 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 RipEX2 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 7.1.3.2, "Common Protocol parameters"*.

Note

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

Note

The port ranges 0-1023 and 8800-9823 are reserved and prohibited for Terminal Server. Port 502 is an exception for ModbusTCP.

7.1.5. Cellular

RipEX2 optionally provides cellular WWAN interface using embedded cellular module. Two SIM cards are available, only one can be active at a time.

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

7.1.5.1. EXT

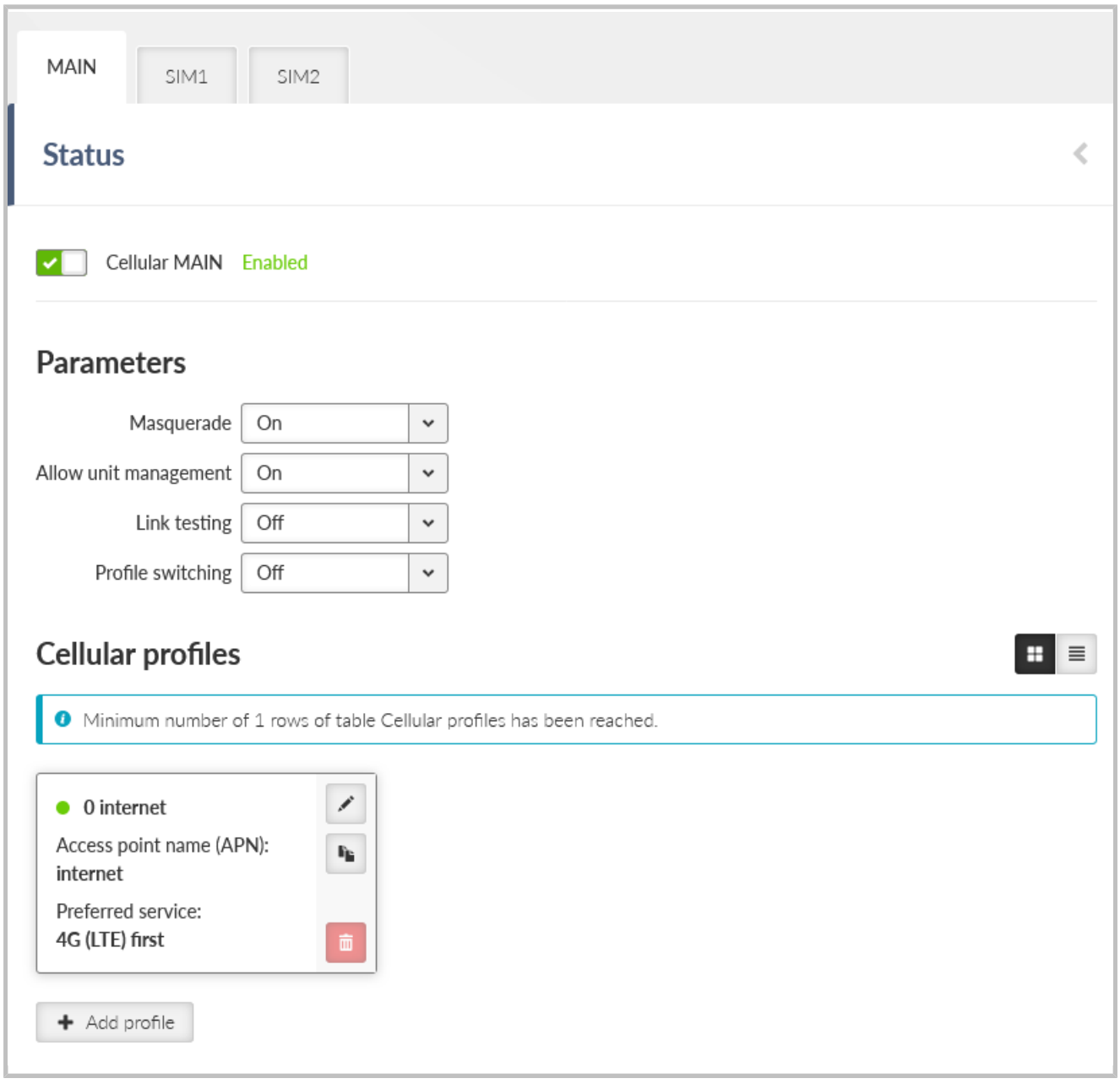


Fig. 7.7: SETTINGS > Interfaces > Cellular

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

Note

Routing **Mode** “WWAN 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 7.7.6, “SMS”*.

7.1.5.1.1. Parameters



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).

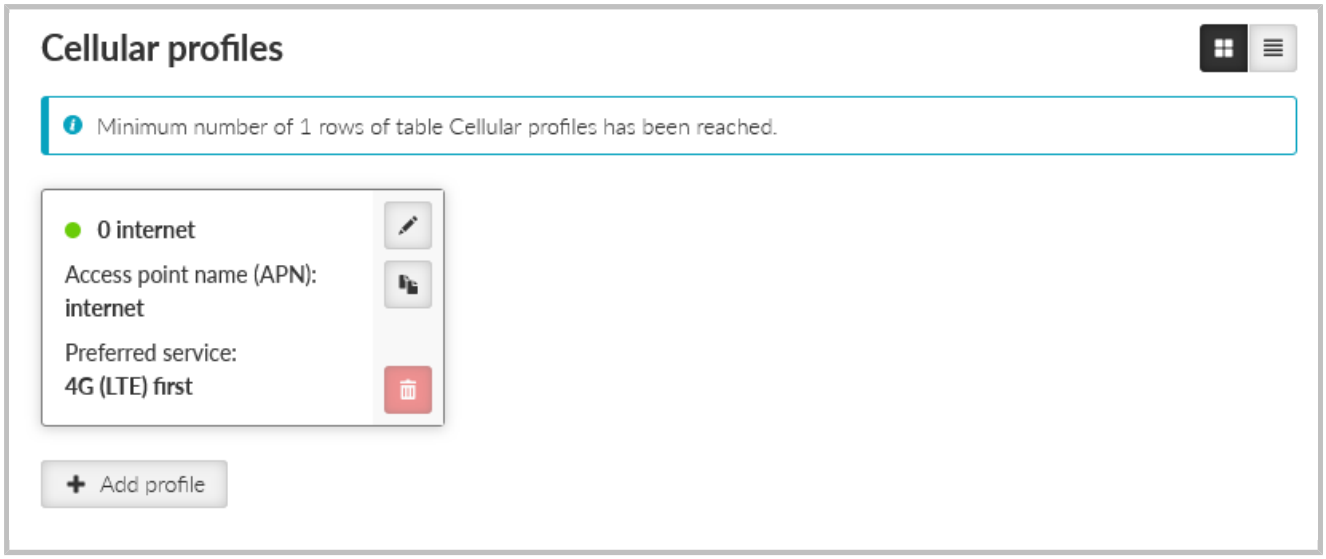
Allow unit management
List box {On; Off}, default = "On"
Allows to manage the unit over WWAN interface.

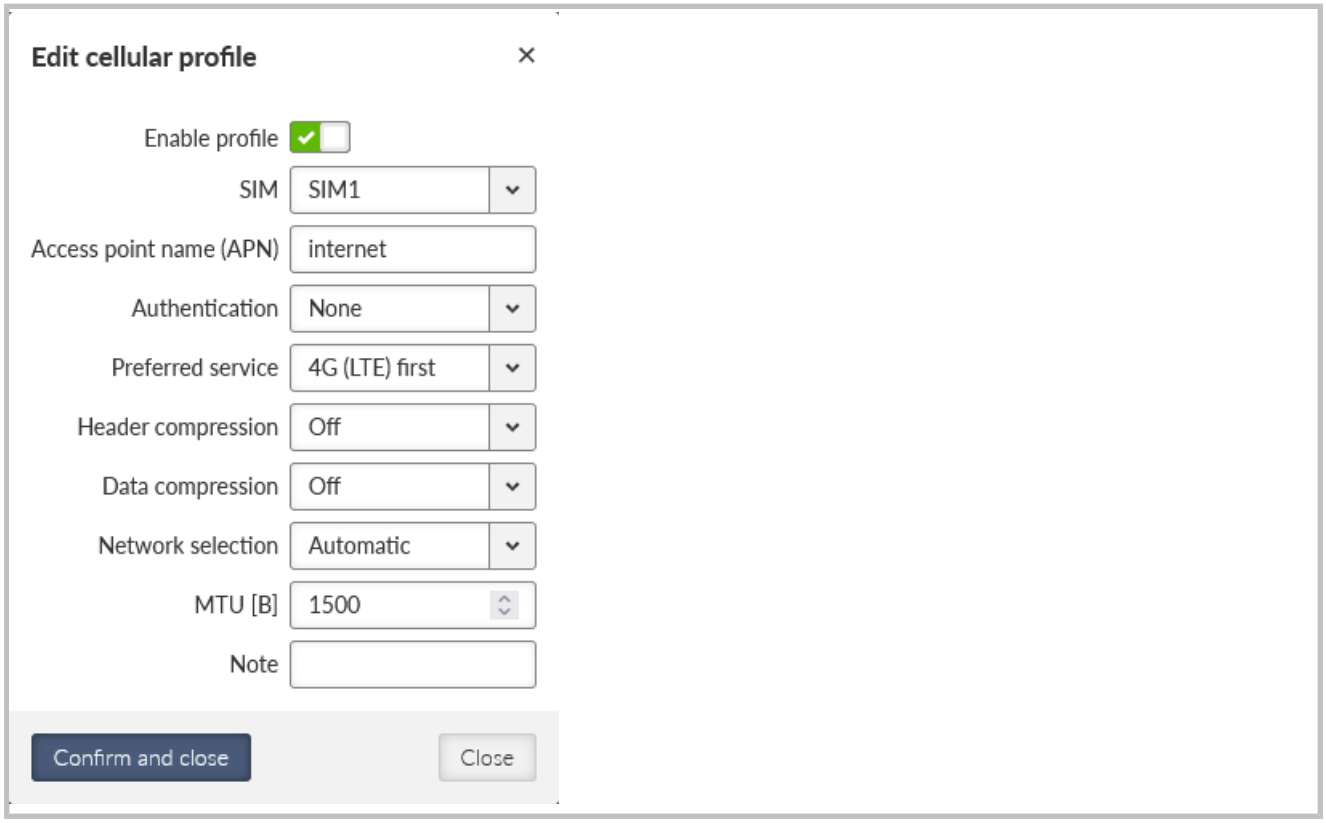
Link testing
List box {On; Off}, default = "Off"
Enables / Disables Link testing.

Profile Switching
List box {On; Off}, default = "Off"
Enables / Disables automatic Profile switching.

7.1.5.1.2. 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).





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.

Note
Default value for cellular module 'R' and 'S' is set to Cat. M1. If the used service is different, you have to change it manually.

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".

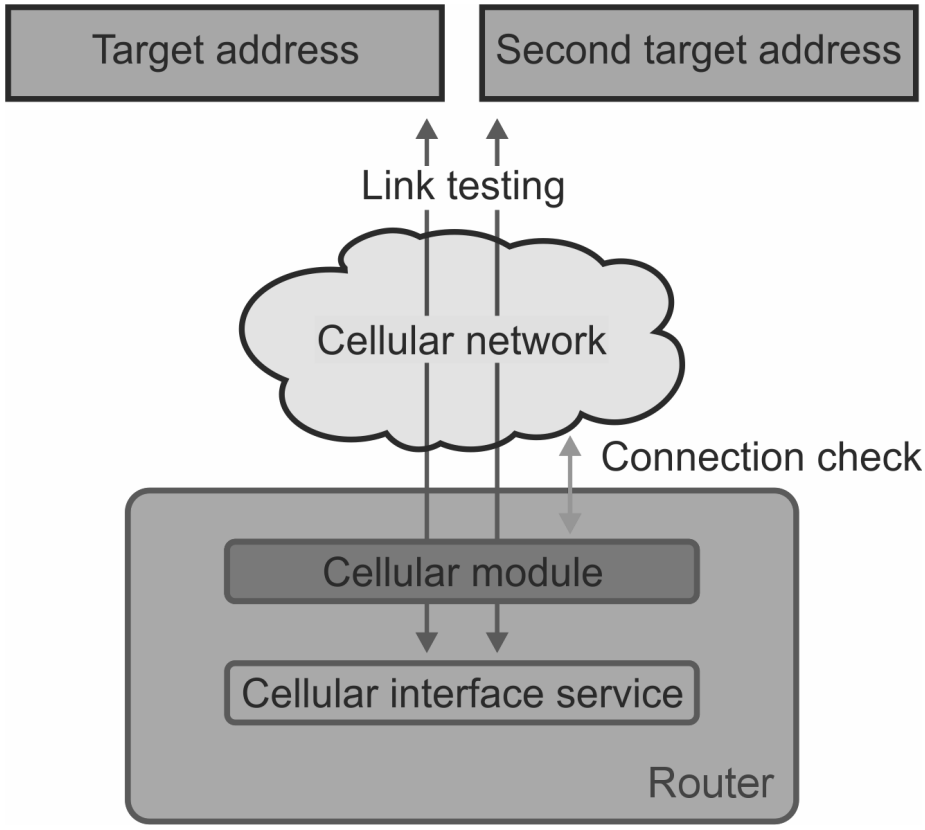
MTU [B]
Number {70 – 1500}, default = 1430

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.

7.1.5.1.3. Link testing

To enable continuous checking of the functional connection via the Cellular interface, Link testing can be activated. This service (Link testing) adds to the basic testing of the connection to the cellular network (Connection check) a test of the end-to-end connectivity through the entire network up to the specified target address(es). The test is carried out by sending an ICMP ping to the defined address(es) and waiting for a response.It is possible to test against one or two target addresses.



The test result is indicated by the link status:

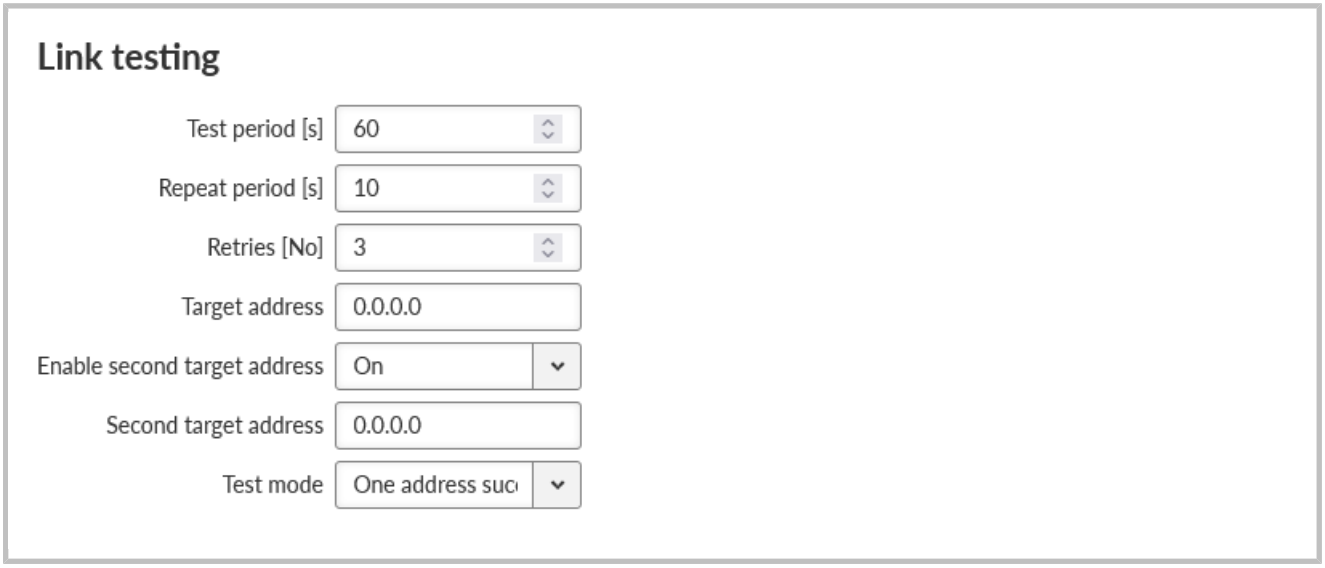
- START - initial status before the start of testing
- RUNNING - the test succeeded, the link is considered to be OK, the test is performed with a Test period
- SUSPECT - the test began to fail, the test is performed with a Repeat period
- FAILED - the link is inoperative, the test is performed with a Repeat period

In a situation where the link is declared inoperative (test in FAILED status), the following actions are performed:

- If Profile switching is disabled, a disconnection and re-login to the Cellular network is initiated.

- If Profile switching is enabled, the switch to the next Profile is initiated.

Settings of Link testing for MAIN (EXT):



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:

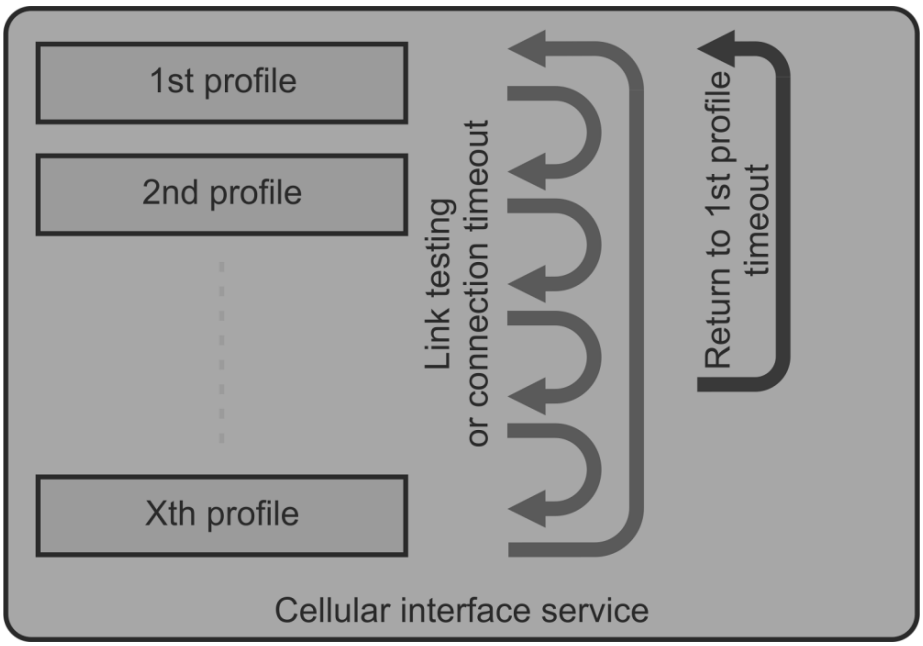
- One address succeeds - only one address is enough to pass the test.
- Both addresses succeeds - both addresses must pass the test.

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.

7.1.5.1.4. 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".





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.

7.1.5.2. 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.

7.1.5.3. 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).

Hot standby
WWAN is activated only in active mode (disabled in passive). In passive mode, the module is disconnected from the mobile network.

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.

7.1.5.4. Status

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

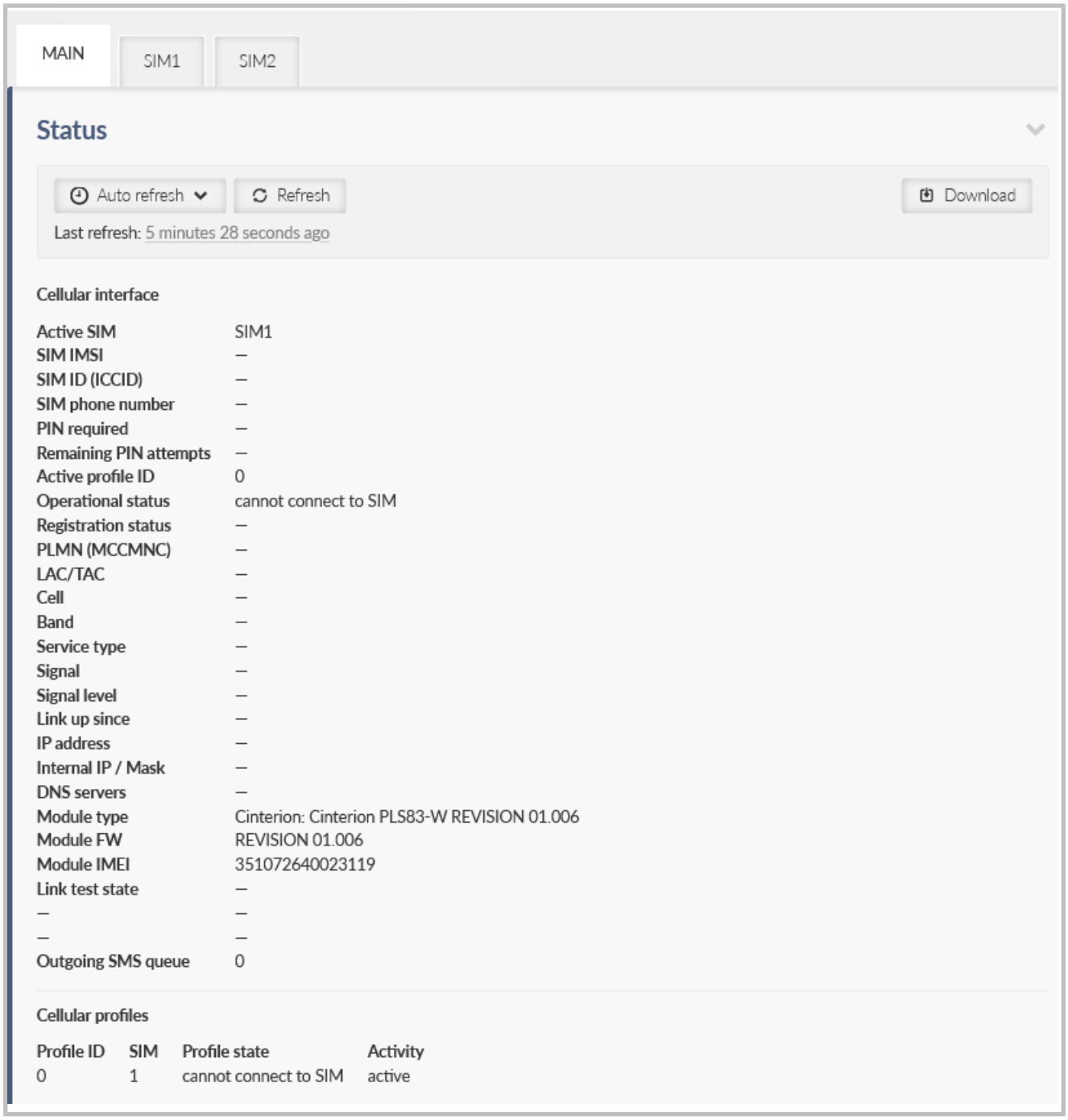


Fig. 7.8: SETTINGS > Interfaces > Cellular > Status

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

Signal level	LED color	2G: RSSI	3G: RSCP	4G: RSRP
Medium	Orange	-95 to -84 dBm	-100 to -89 dBm	-100 to -80 dBm
Good	Green	-84 dBm <=	-89 dBm <=	-80 dBm <=

7.1.6. PPPoE client

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol that encapsulates PPP frames within Ethernet frames. The PPP protocol itself is already described among *serial protocols*. With PPPoE, we distinguish between two basic phases: "Discovery" and "PPP Session".

Discovery phase

The primary goal of the PPPoE Discovery Phase is to acquire essential information for establishing the PPP Session Phase. This information includes the MAC address of the peer device and the PPPoE session ID.

PPP Session phase

The primary goal of the PPP Session Phase is to establish and maintain a connection between the client and the server. This phase utilizes standard PPP frames for data exchange. All frames within this phase carry an ETHER_TYPE value of 0x8864 and are considered Ethernet unicasts.

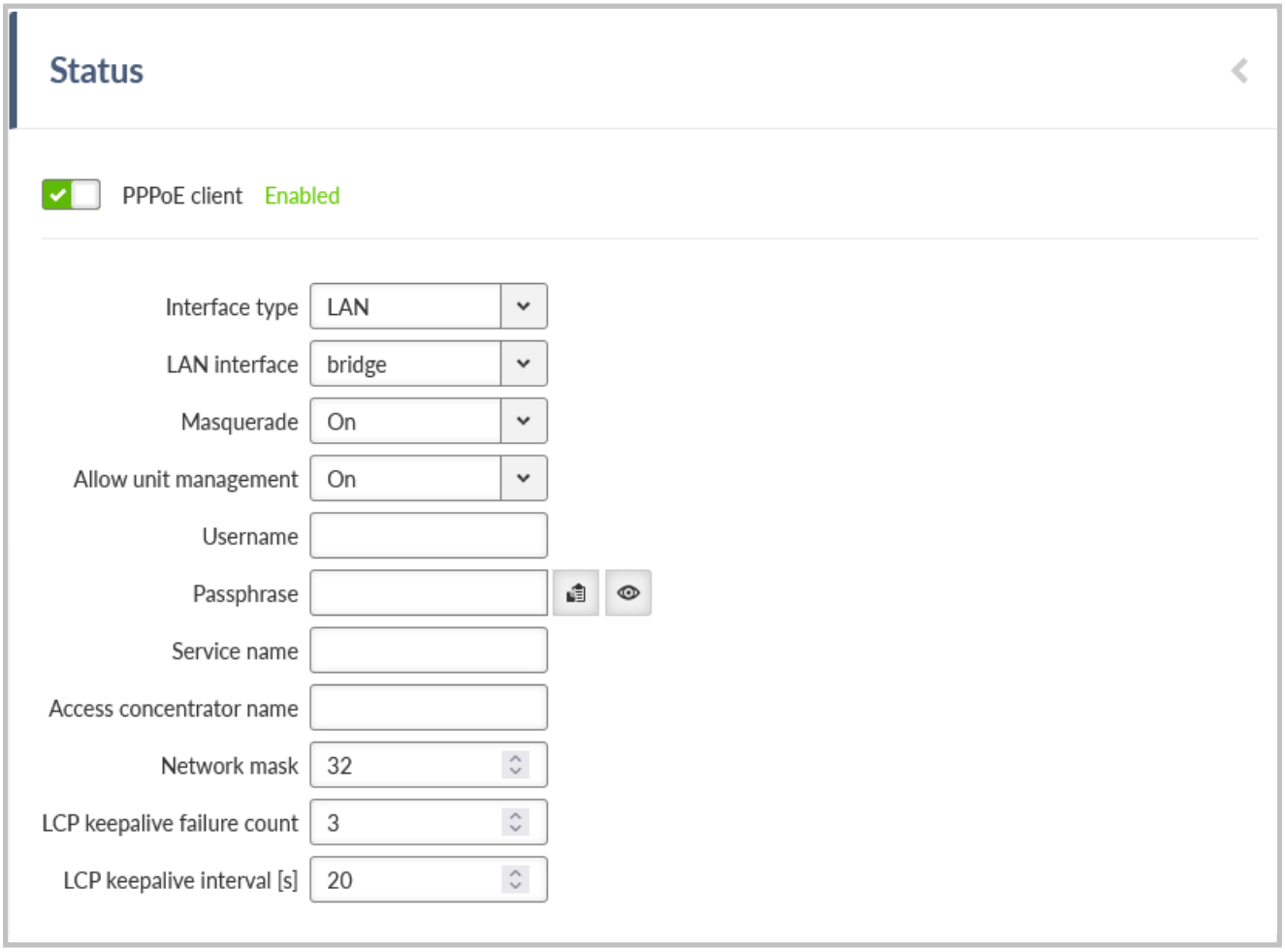


Fig. 7.9: SETTINGS > Interfaces > PPPoE client

Interface type
List box {LAN; VLAN}, default = "LAN"
This parameter specifies from which table the interface will be selected using a name.

- LAN - The name of the LAN interface to be used for PPPoE connection establishment.
- VLAN - The name of the VLAN interface to be used for PPPoE connection establishment.

Masquarade
List box {On; Off}, default = "On"
Enables/disables SNAT (masquerade) on packets sent over the PPP interface.
With masquerade, outgoing packets from the station over the PPP interface have their source address rewritten to the address assigned to this interface. Returning packets are then correctly routed back through the station.

Allow unit management
List box {On; Off}, default = "On"
Allows to manage the unit over PPP interface.

Username
String {up to 64 characters}, default = <empty>
The username to be used for authentication with the peer, regardless of the protocol required.

Passphrase
String {up to 64 characters}, default = <empty>
The passphrase to be used for authentication with the peer, regardless of the protocol required.

Service name
String {up to 64 characters}, default = <empty>
The service name to be used when searching for the server to connect to.

Access concentrator name
String {up to 64 characters}, default = <empty>
The name of the server to connect to.

Network mask
Number {0 – 32}, default = 0
Used together with the peer's IP address to determine the destination range of the routing rule pointing to the PPP interface.

LCP keepalive failure count
Number {0 – 255}, default = 3 (disabled if 0)
A non-zero value specifies the maximum number of LCP request messages sent before the peer is considered disconnected and the connection is terminated.

LCP keepalive interval
Number {0 – 255}, default = 10
The interval for sending LCP request messages, to which the peer normally responds with an LCP reply message.
This parameter can be used in conjunction with LCP keepalive failure count to detect whether the peer is connected.
This parameter is active only when LCP keepalive failure count is greater than 0.

7.1.7. Wi-Fi

RipEX2 optionally provides cellular Wi-Fi interface using embedded Wi-Fi module. Wi-Fi interface can be used in **Access point (AP) mode** only. Client mode is not implemented.

7.1.7.1. Settings

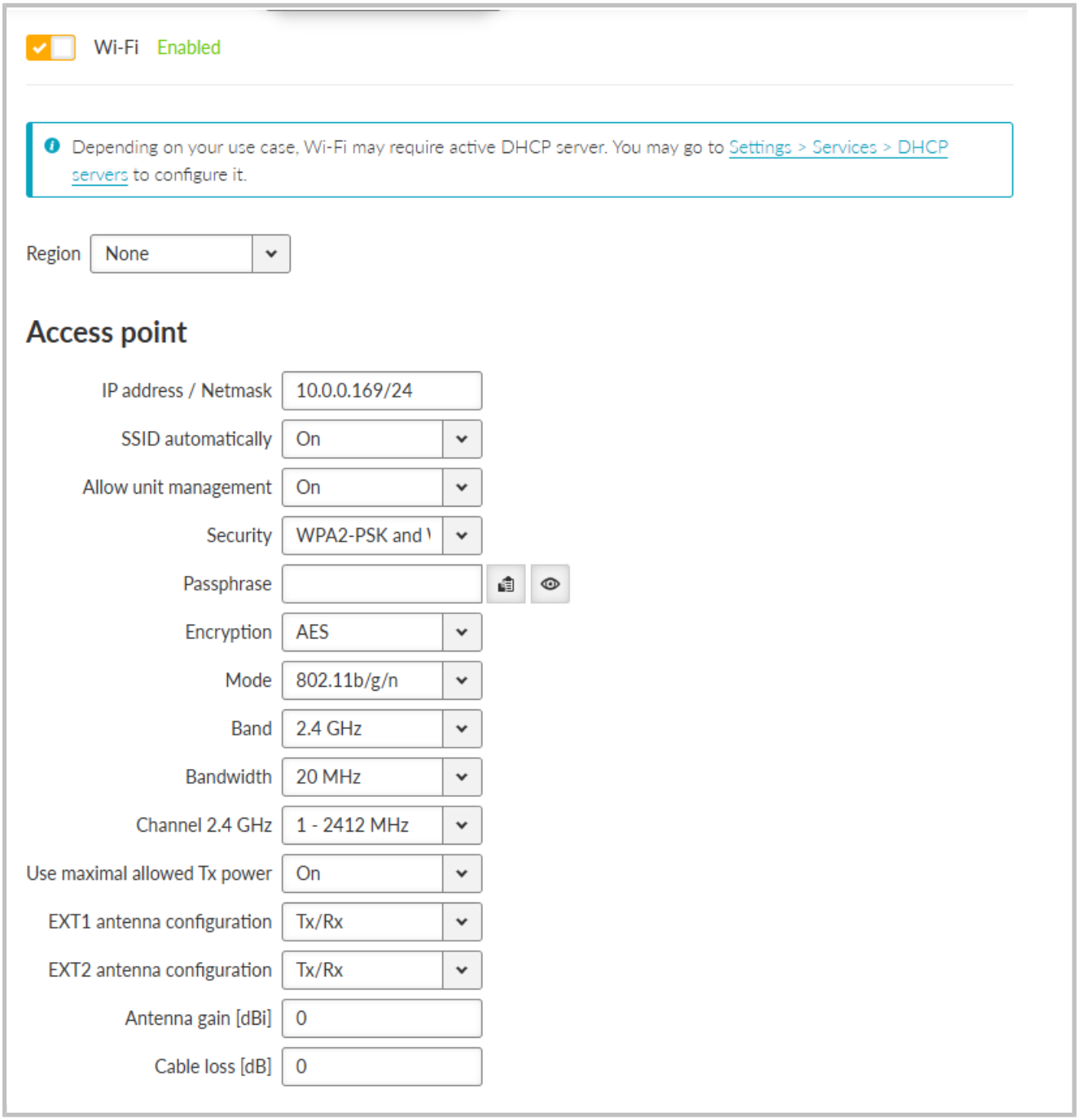


Fig. 7.10: SETTINGS > Interfaces > Wi-Fi

Enable/Disable Wi-Fi
Check box {On; Off}, default = "Off"
Enables / Disables the Wi-Fi.

Region

List box {ISO 3166-1 alpha-2 countries}, default = "None"
Setting the region in which the unit is operated. The purpose is to activate any regional restrictions on transmission power. These restrictions vary by region and by transmission band. The specific value of the maximum allowed EIRP in the selected region can be verified in the Status - the value "Maximum allowed EIRP [dBm]".

IP address / Netmask

IP address, default = "10.0.0.169"
Netmask {0-32}, default = "24"
Wi-Fi interface IP address, must not conflict with another address range.

SSID automatically

List box {On; Off}, default = "On"
When automatic definition of SSID is enabled, the SSID contains unit Serial number.

Hide SSID

List box {On; Off}, default = "Off"
Hides the SSID (network name) of a Wi-Fi AP

Allow unit management

List box {On; Off}, default = "On"
Enables access to unit management through the Wi-Fi interface.

Security

List box {Off, WPA-PSK (legacy), WPA2-PSK, WPA-PSK (legacy) and WPA2-PSK, WPA3-SAE, WPA2-PSK and WPA3-SAE}, default = "WPA2-PSK and WPA3-SAE"
Wi-Fi network security.

Note
802.1w (PMF) is enabled automatically with the mode set to any of "802.11a, 802.11b/g/n, 802.11a/n, 802.11a/n/ac" && security set to any of "WPA, WPA2, WPA3-SAE". Otherwise, it is not enabled.

Passphrase

String {up to 63 characters}, default = <empty>
Passphrase to connect to Wi-Fi Access Point.

Encryption

List box {TKIP (legacy), AES (default), TKIP (legacy) and AES}, default = AES
Wi-Fi network encryption.

Mode

List box {802.11a, 802.11b, 802.11b/g, 802.11b/g/n , 802.11a/n, 802.11a/n/ac}, default = 802.11b/g/n
IEEE 802.11 mode in which the Wi-Fi module will operate.

Band

List box {2.4 GHz, 5 GHz}, default = 2.4 GHz
Band in which the Wi-Fi module will operate.

Bandwitdh

List box {20 MHz ,40 MHz, 80 MHz}, default = 20 MHz
Wi-Fi network bandwidth.

Channel 2.4 GHz

List box {Automatic, 1 - 2412 MHz, 2 - 2417 MHz, 3 - 2422 MHz, 4 - 2427 MHz, 5 - 2432 MHz, 6 - 2437 MHz, 7 - 2442 MHz, 8 - 2447 MHz, 9 - 2452 MHz, 10 - 2457 MHz, 11 - 2462 MHz, 12 - 2467 MHz, 13 - 2472 MHz, 14 - 2484 MHz}, default = "Automatic"
Select your 2.4 GHz Wi-Fi network channel. Includes ACS and automatic channel options, not only manual configuration. Available options depend on your Wi-Fi bandwidth settings.

Channel 5 GHz

List box {Automatic, 36 - 5180 MHz, 40 - 5200 MHz, 44 - 5220 MHz, 48 - 5240 MHz, 52 - 5260 MHz, 56 - 5280 MHz, 60 - 5300 MHz, 64 - 5320 MHz, 100 - 5500 MHz, 104 - 5520 MHz, 108 - 5540 MHz, 112 - 5560 MHz, 116 - 5580 MHz, 120 - 5600 MHz, 124 - 5620 MHz, 128 - 5640 MHz, 132 - 5660 MHz, 136 - 5680 MHz, 140 - 5700 MHz, 144 - 5720 MHz, 149 - 5745 MHz, 153 - 5765 MHz, 157 - 5785 MHz, 161 - 5805 MHz, 165 - 5825 MHz}, default = "Automatic"
Select your 5 GHz Wi-Fi network channel. Includes ACS and automatic channel options, not only manual configuration. Available options depend on your Wi-Fi bandwidth settings.

Note
Channels that require DFS cannot be used.

Use maximal allowed Tx power

List box {On; Off}, default = "On"
Automatic selection of the transmitting power of the Wi-Fi module.
If the option is disabled:

Maximal Tx power

Full number {0-16}, default = "16" [dBm]
Transmitting power of the Wi-Fi module.

EXT1 antenna configuration

List box {Off, Tx, Rx, Tx/Rx}, default = "Tx/Rx"
Determines the functionality of the antenna connected to the Wi-Fi module via EXT1 port.

EXT2 antenna configuration

List box {Off, Tx, Rx, Tx/Rx}, default = "Tx/Rx"
Determines the functionality of the antenna connected to the Wi-Fi module via EXT2 port.

Antenna gain

Full number {0-30}, default = "0" [dBi]
Gain of the antenna connected to the Wi-Fi module.
Used in the calculation of the transmit power of the Wi-Fi module with a positive sign.

Cable loss

Full number {0-30}, default = "0" [dB]
Used in the calculation of the transmit power of the Wi-Fi module with a negative sign.

7.1.7.2. Access control

The Access Control table allows you to control client access based on their MAC addresses.

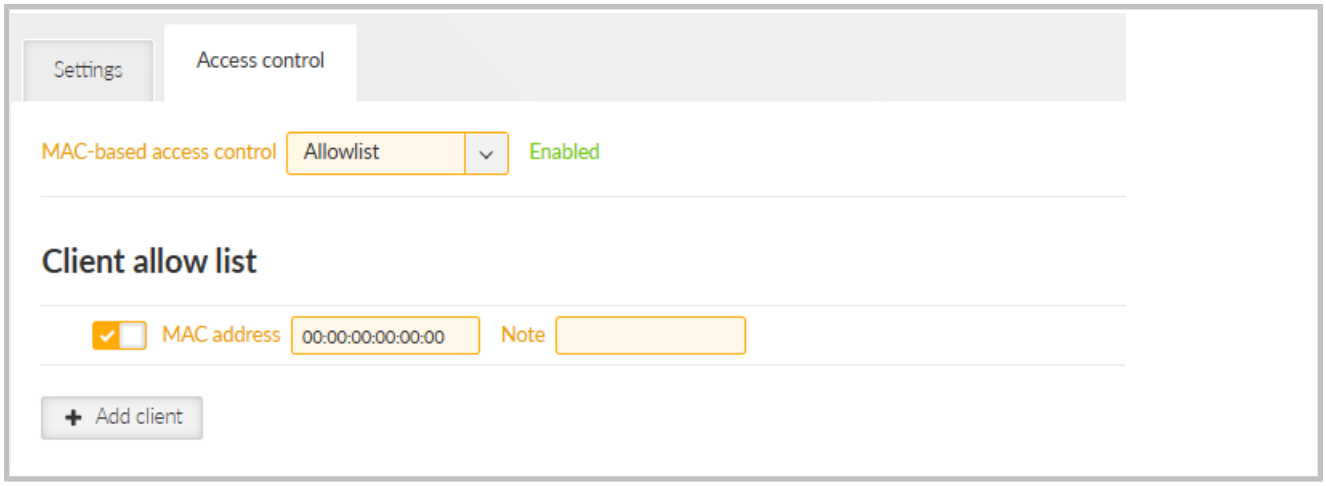


Fig. 7.11: SETTINGS > Interfaces > Wi-Fi > Access control

MAC-based access control
List box {Off, Allowlist, Blocklist}, default = "Off"
Manage client access by MAC address.

Allowlist
Alows only clients with MAC addresses in the list, others are blocked.

Blocklist
Blocks clients with MAC addresses in the list, others are allowed

Enable/Disable client
List box {On; Off}, default = "On"
Activates a rule for a given MAC address.

MAC address MAC address , default = 00:00:00:00:00:00

MAC address of the client

7.1.7.3. Cooperation with other services

DHCP server
It is possible to run a DHCP server over the Wi-Fi interface.
The DHCP server must be configured to allocate IP addresses from the address range specified by the configuration **IP address / Netmask** in the Wi-Fi interface.

Events
Connection and disconnection of clients to the Wi-Fi AP is reported by events "Wi-Fi AP (EXT) reports client connected" and "Wi-Fi AP (EXT) reports client disconnected"

Firewall L3
The firewall can filter traffic coming from the Wi-Fi interface by using the "EXT" option in the I/O interface settings.

Hot standby
Wi-Fi is deactivated in passive mode and activated in active mode.
In passive mode, the module's power supply is active, but the Wi-Fi interface is not active.

Link manager

The Wi-Fi interface can be used in Link Manager as a WWAN (EXT) interface when configuring the link.

NAT

SNAT and DNAT rules can modify traffic passing through the Wi-Fi interface by using the "EXT" option in the I/O interface settings.
The Wi-Fi interface name can be used when setting the manual I/O interface name ("Other"), but only if Wi-Fi (EXT) is active.

Sleep mode

When sleep mode is active, it is possible to delay putting the device to sleep if user traffic is detected on the Wi-Fi interface.

7.2. Routing

RipEX2 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 RipEX2 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.



Note

Due to static internal routing to clients, OpenVPN L3 is incompatible with dynamic routing protocols. Dynamic routing over the OpenVPN L3 interface will not function.



Note

M!DGE3e not supports Dynamic routing functionalities (Link management, Babel, OSPF, BGP).

7.2.1. Static

RipEX2 works as a standard IP router with multiple independent interfaces: Radio interface, Network interfaces (bridging physical Ethernet interfaces), COM ports, Terminal servers, optional 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 either IP of a Network interface (bridging Ethernet interfaces) or IP of Radio interface. The IP address source of outgoing packets from COM ports is equal to IP address of interface (either Radio or 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.



Fig. 7.12: SETTINGS > Routing > Static

Active

{On / Off}
Switches the rule on / off.

Destination IP / mask

IP address, default = 0.0.0.0/0
Each IP packet, received by RipEX2 through any interface (Radio, ETH, COM, ...), has got a destination IP address. RipEX2 (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
Networks defined by IP and Mask for Radio and other interfaces must not overlap.

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

Mode

List box {Static; WWAN (MAIN); WWAN (EXT); PPP1; PPP2; PPP3; Link manager; PPPoE Client}, default = Static

- Static - Used for static IP routing rules. If the next hop on the specific route is over the radio channel, the Radio IP is used as a **Gateway**. If Base driven protocol is used and the destination Remote is behind a Repeater, the destination Remote Radio IP is used as a Gateway (not the Repeater address).
- WWAN (MAIN); WWAN (EXT) - Routing rule to the primary/secondary WWAN, which has a dynamically assigned address. The next hop will be directed through the "wwan" interface when it is open.

- PPP1; PPP2; PPP3 - Routing rule to the PPP interface associated with the COM protocol. The interface may have a dynamically assigned address. Can only be set if the corresponding COM port is enabled and with the PPP protocol.
- Link manager - Routing rule via active link selected by the Link manager. The rule will be dynamically switched in case of a link change or loss. It can be set if the Link manager is enabled.
- PPPoE Client - Routing rule to the PPP interface created by the PPPoE client. The interface has a dynamically assigned address. It can only be set if the PPPoE client is active.

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 RipEX2 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 some of the following interfaces: Radio interface, 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 (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 RipEX2, 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.



Fig. 7.13: ADVANCED > Interfaces > Loopback

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

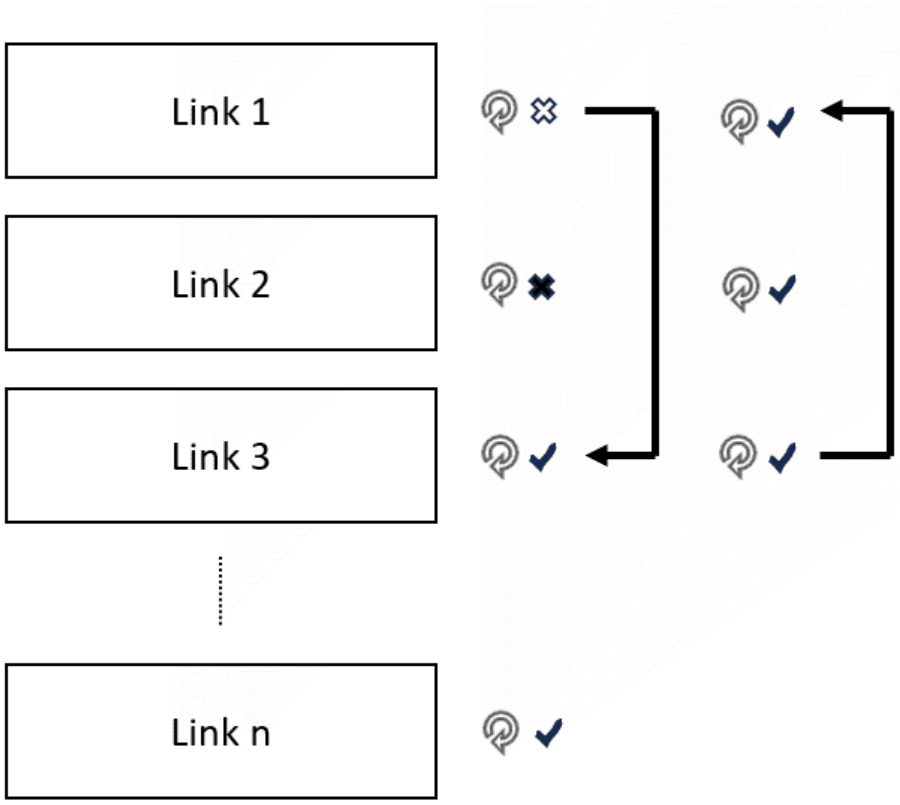
Note
Optional comment.

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. Link management

Link manager is a mechanism providing switching of several pre-configured alternative links (alternative routes). Link switch is triggered in case of the active link failure. Link failure can be detected passively – by checking link interface status (see **Watched interface** parameter) and actively by ICMP ping (see **Link testing** parameter).

Link testing is active on currently active link and all higher priority links (to detect when they are available again). Lower priority links can also be tested (see **Test backup link** parameter). When the current link fails, link manager switches to the next functional lower priority link. If the link is not being checked (Test backup link parameter is disabled), it is assumed to be functional. Routing rules are updated automatically on link switchover.


Link 1
Link 2
Link 3
Link n

7.2.2.1. Parameters

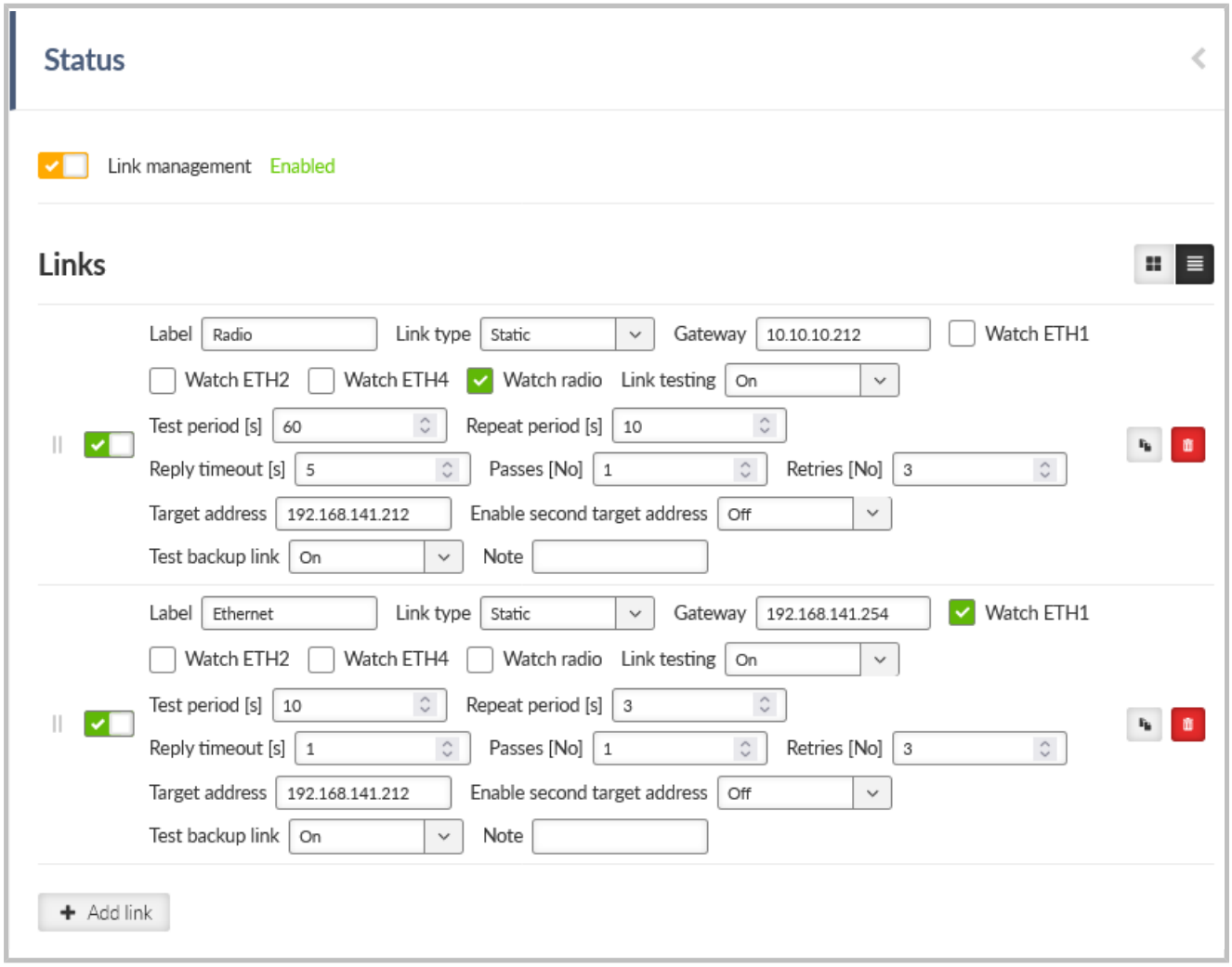


Fig. 7.14: SETTINGS > Routing > Link management

Enable Link manager

Enables/disables the Link manager

IPsec control

List box {Off; On}, default = “Off”

Enables / disables binding between a link and particular IPsec tunnel. This option is available only when IPsec is enabled and configured. Configuration parameter: SETTINGS > VPN > IPsec > IPsec associations > **Management mode** provides two options:

Link manager (Master)

One of the IPsec associations is declared as **Master**. Traffic selectors (CHILD SA) define the traffic to be encrypted.

Link manager (Slave)

All other associations are declared as **Slave**. No Traffic selectors are defined for such a tunnel. The Master’s traffic selectors are used.

7.2.2.2. Links

Every alternative link is configured separately. The priority of individual links is determined by their order. Maximal number of links is 16.

Possible link states:

- **down**: link is not present
- **untested**: link is present, no Link test result is available yet
- **up**: link is present and functional. Should the Link test be activated, the test result is successful
- **test failed**: link is present, the Link test failed

Possible link roles:

- **active**: link is selected as the active one. Only one of the links can be active
- **backup**: link has a lower priority compared to the active link
- **rejected**: link has a higher priority compared to the active link, but can not be used

Enable link

Enables / disables individual link

Label

String {a..z A..Z 0..9 @ _ -}, max 42 char, default = “LINK”
Name of the link that's used in the Status info and System logs

Link type

List box {Static; WWAN (MAIN); WWAN (EXT)}, default = “Static”

- Static – LAN, GRE or radio interfaces
  Gateway needs to be configured. Watched interfaces can be selected.

- WWAN (both MAIN or EXT)
  The cellular interface status is checked automatically (incl. Cellular Link tester – when enabled). The link state is up in case the Cellular interface is enabled and the link test succeeded. The gateway IP is not configured manually - IP address assigned by the cellular network is used.

Gateway

IP address, default = 0.0.0.0
Next-hop (gateway) address for the Static type of the link

Watched interface (ETH1 .. ETH5, Radio)

Enables / Disables checking of individual interface.
When all checked interfaces are down, the link state is **down**
ETHx Link status is checked for ETH1-ETH5 options. Successful establishment of Radio interface is checked for the Radio option

IPsec association

List box {list of available Peer IDs}, default = first Peer ID
When **IPsec control** is On, the individual link is paired with an individual IPsec tunnel defined by its **Peer ID**. In such a case the individual IPsec tunnel is activated/deactivated together with the respective link. It is automatically switched back to the higher priority link once it is restored..

Link testing

List box {Off; On}, default = “Off”
Enables active link testing. Links are tested using ICMP echo packets

Test period [s]
Number {3 – 3600}, default = 60
Testing period of a link that is in the **up** state

Repeat period [s]
Number {3 – 3600}, default = 10
Testing period of a link that has to be tested (above the active link) and it is normally not tested or the test failed

Reply timeout [s]
Number {1 – 60}, default = 5
ICMP ping reply timeout

Passes [No]
Number {1 – 20}, default = 1
Uninterrupted number of successful tests (pings) after which the link status is up

Retries [No]
Number {1 – 20}, default = 3
Uninterrupted number of failed tests (pings) after which the link status is **test failed**

Target address
IP address, default = 0.0.0.0
Primary tested IP address

Enable second target address
List box {Off; On}, default = "Off"
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 succeed}, default = "One address succeeds"

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

Test backup link
List box {Off; On}, default = "Off"
Enables active link testing of a link having lower priority compared to **active** link

Note
String {0–42 char}, default = <empty>

NOTE: Link manager is not a full featured dynamic routing protocol (as Babel, OSPF or BGP). Dynamic routing protocols provide synchronization of alternative packet routes across the whole network. Link manager works locally – there is no synchronization of the selected link (route) with other units across the network. Keep in mind this fact when planning Link manager configuration across your network and preserve symmetrical behaviour. One effect of the fact that each Link manager instance in the network operates independently is the occasional asymmetric traffic when switching alternate routes.

NOTE: Link test packets (ICMP echo to test addresses) must actually test the individual link (be routed through it). In combination with IPsec control, it must not happen that the IPsec tunnel captures and encrypts these packets. Otherwise, non-standard behaviour may occur (oscillation, test never succeeds, stuck on broken link).

7.2.2.3. Status

Status info area provides list of all enabled link. Link state and Link role (see description above) provide information about individual status of each link and which of the links is the active one.

7.2.3. 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 *RFC 6126*[3]).

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.

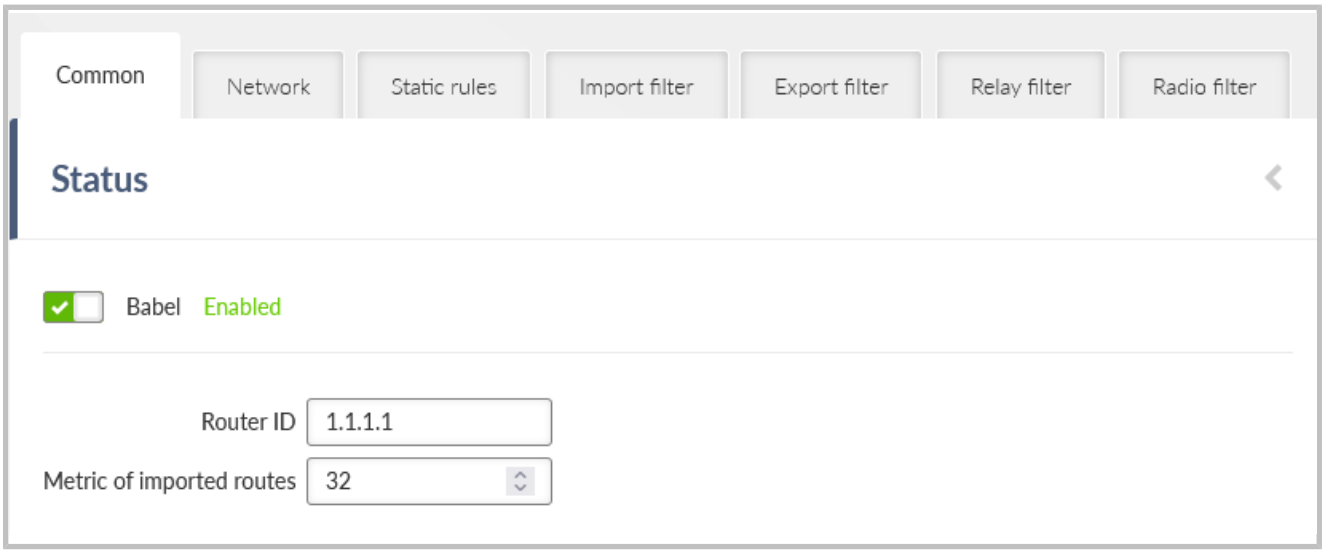


Fig. 7.15: SETTINGS > Routing > Babel

Configuration parameters are described in the following chapters. Several use case scenarios and configuration examples are described in the *Babel Application note*[4].

[3] https://datatracker.ietf.org/doc/html/rfc6126.html#section-1.1
[4] https://www.racom.eu/download/hw/ripex/free/eng/1_application/ripex2-app-bab-en.pdf

7.2.3.1. 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”:

- 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 witch 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:

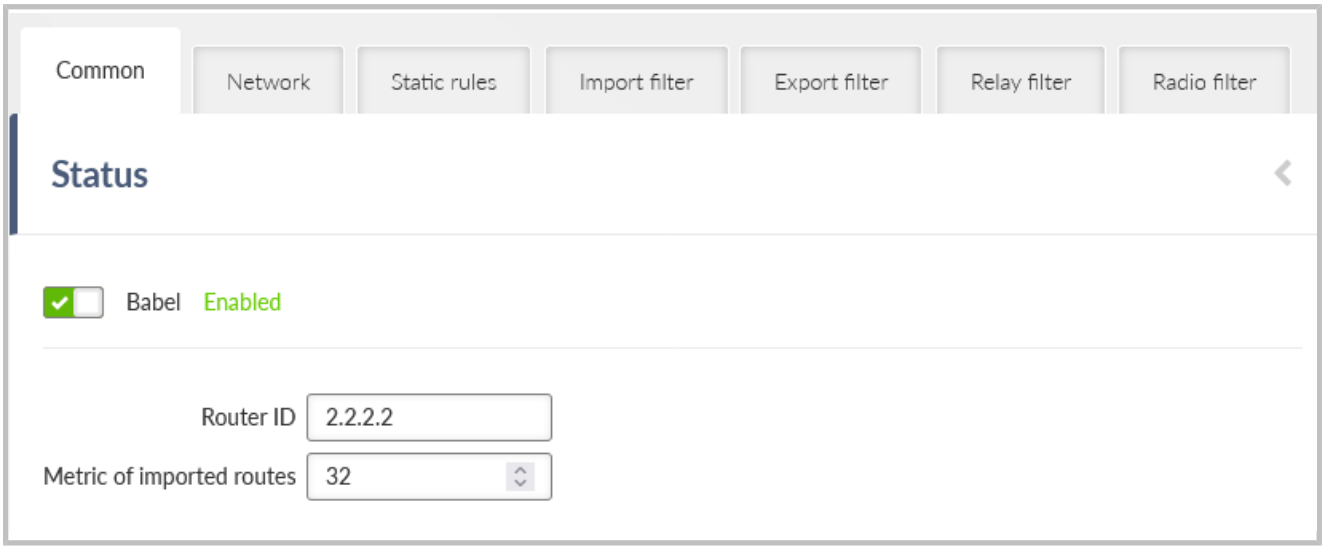
- SETTINGS > Routing > Static routes rule: 0.0.0.0/0 → 10.10.1.11
- Dynamic rule: 192.168.1.0/24 → 192.168.11.1 metric 32
- Packet with DST 192.168.1.42 will be routed to 192.168.11.1 because the dynamic rule has a narrower mask.

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.

7.2.3.2. Common - Common settings



Router ID

IP address, default = 0.0.0.0

RipEX2 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"

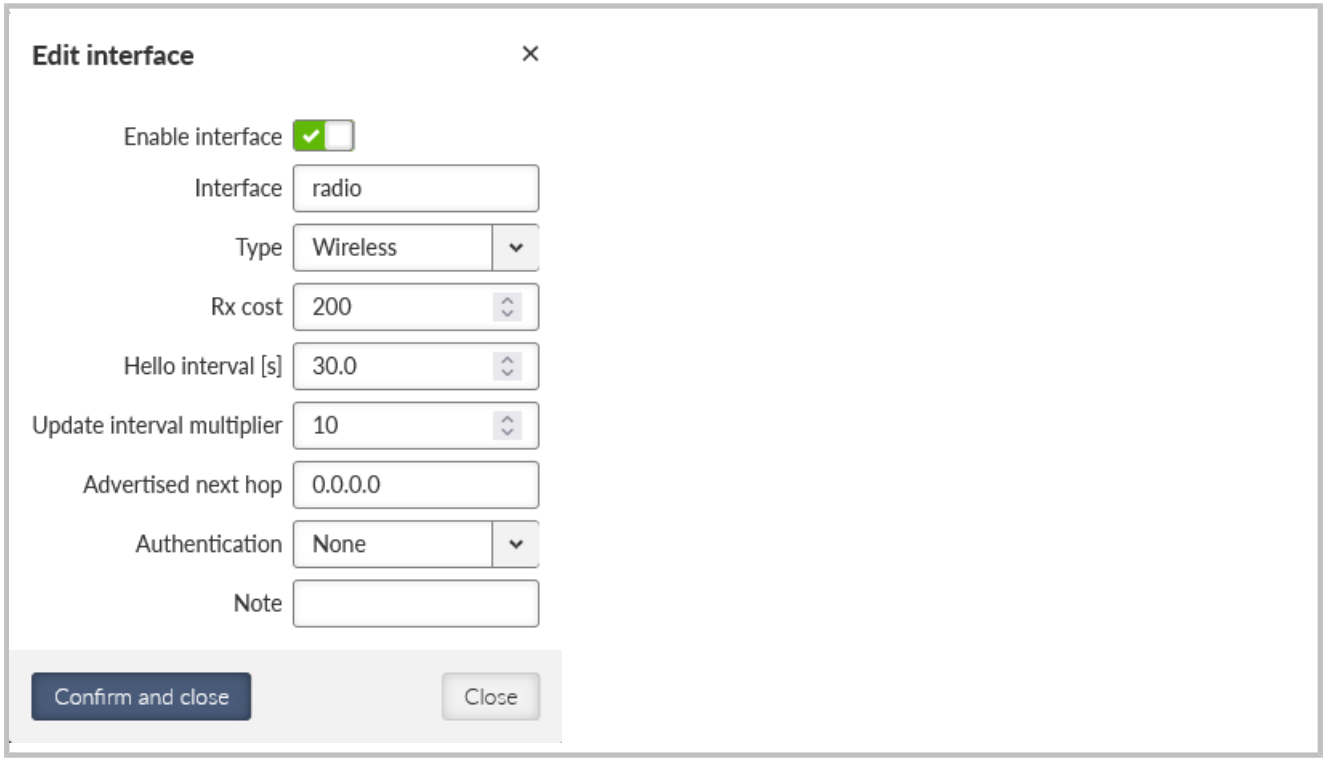
Advanced feature: Enables randomization of the upper 4 Bytes of the router identification. The lower 4 Bytes are set by a **Router ID** parameter. This feature might be used in a case the Babel node is often restarted resulting in refusing its messages by its neighbors.

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.

7.2.3.3. Network - Interfaces



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”

Radio – “radio”

Hot standby – “hstdby”

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

Cellular – “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 is 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.

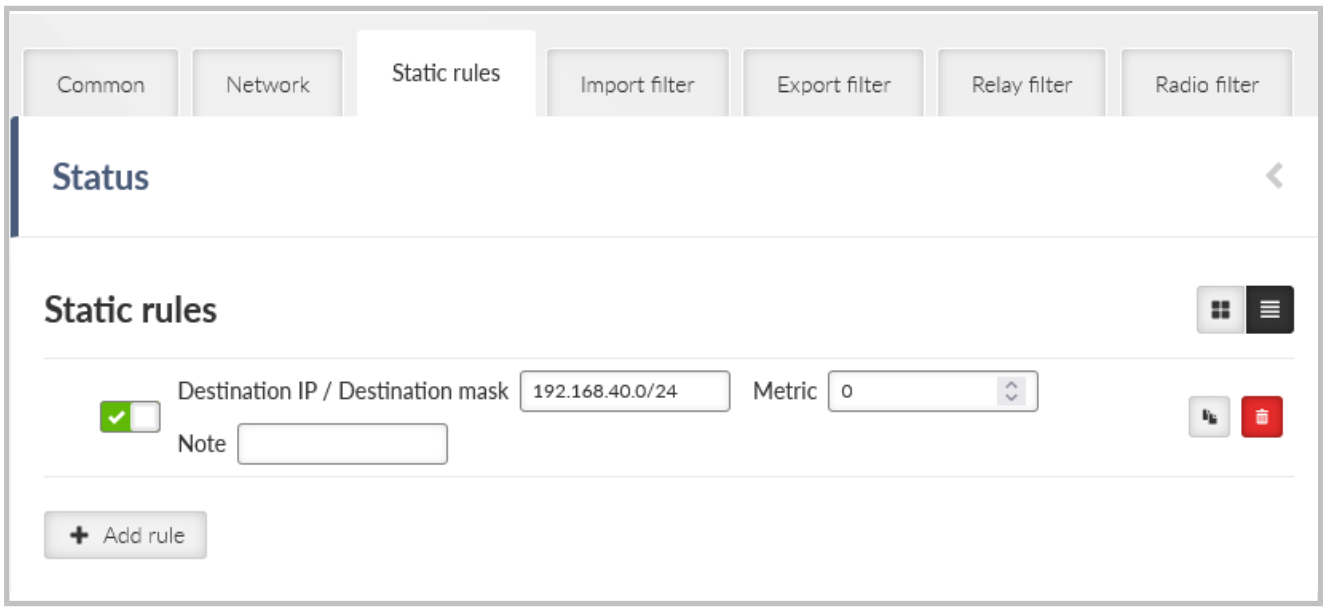
- Full - packets are signed during transfer and the signature is validated when receiving incoming packets. Packets with invalid signature are reported to the log and thrown away.
- Only sign - Packets are signed during transfer and the signature is validated when receiving incoming packets. Packets 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 passphrase 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

Passphrase
String {up to 128 char}
Defines the passphrase for packets authentication.

Note
Optional comment.

7.2.3.4. Static rules



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

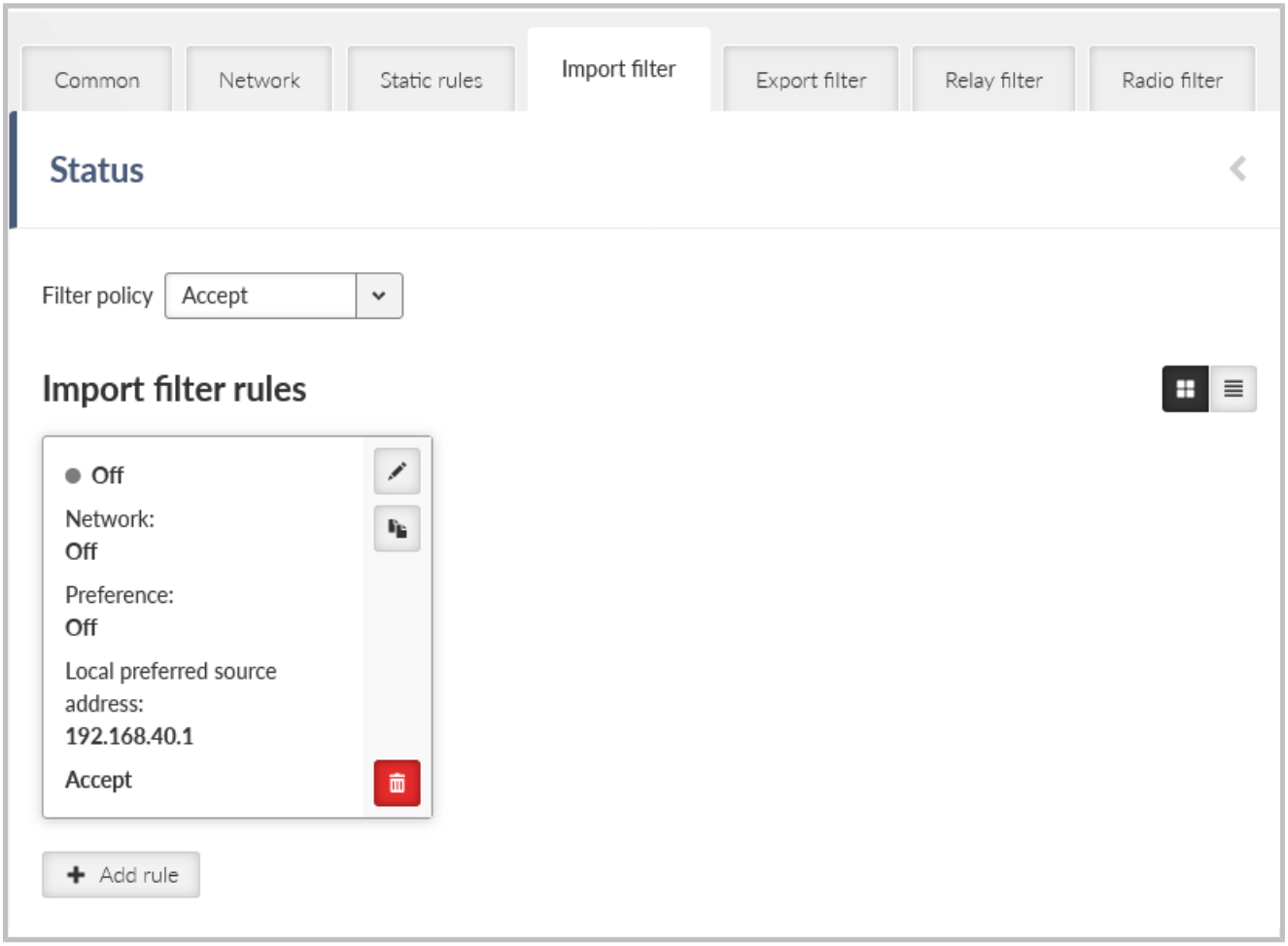
Active
List box {On; Off}, default = "On"
Enables / disables the static routing rule.

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.

7.2.3.5. Import filter



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.

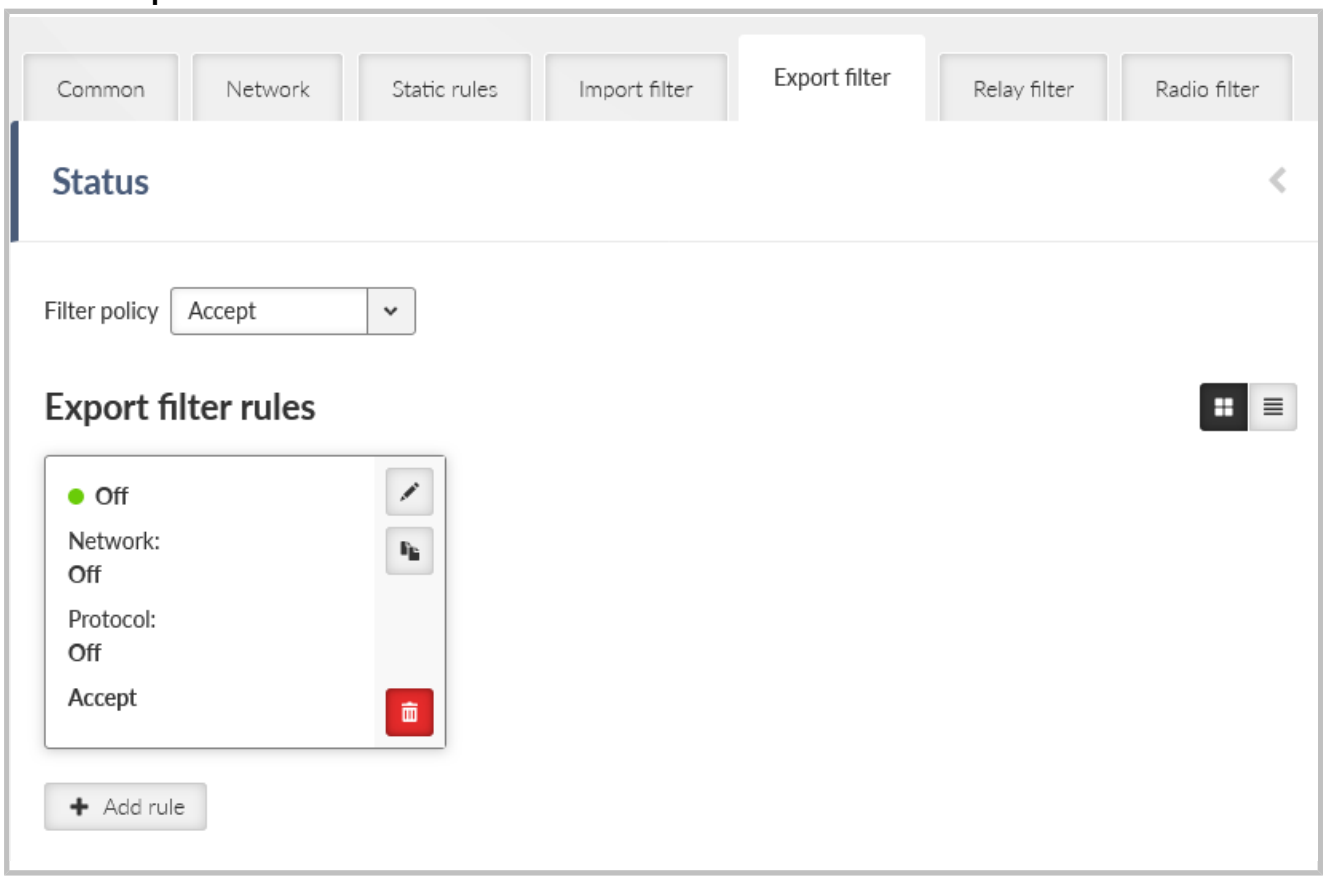
Local preferred source address

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.

7.2.3.6. Export filter



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^{32}-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.

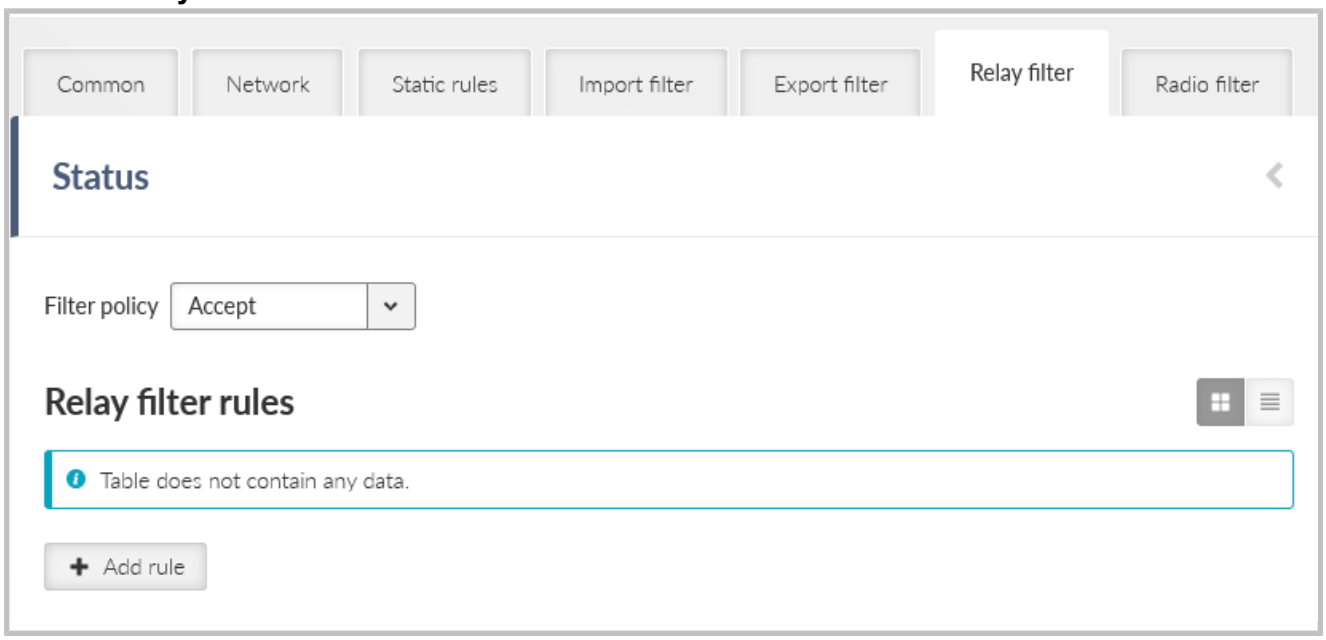
OSPF metric 2: Metric of OSPF type 2. If the rule does not have a metric value filled in, the static Metric value is used.

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.

7.2.3.7. Relay filter



Relay filter selects what happens to a rule received from another Babel instance that were not captured in the filter. When disabled, the rules will not be forwarded to other routers and this station will act as a terminal where paths begin and end in the Babel network, but do not pass through it.

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

Enable rule
Check box {On; Off}, default = "On"

Activates/disables the rule

Filter network
List box {Off; Match; Not match}, default = "Off"
Selects a way to compare the target range of the rule

Network IP/Network mask	IP address / mask, default = 0.0.0.0/0
	Compares network prefix
Mask from	Number {0 – 32}, default = 0
	Defines the allowed mask length range of the compared rule
Mask to	Number {0 – 32}, default = 32
	Defines the allowed mask length range of the compared rule

Action
List box {Accept; Reject; Pass}, default = "Accept"
Chooses what to do with the rule

Filter metric
List box {Off; <; <=; >=; >}, default = "Off"
Selects a way to compare Babel metrics rules

Metric value	Number {0 – 65534}, default = 0
	The compared value of the rule metric

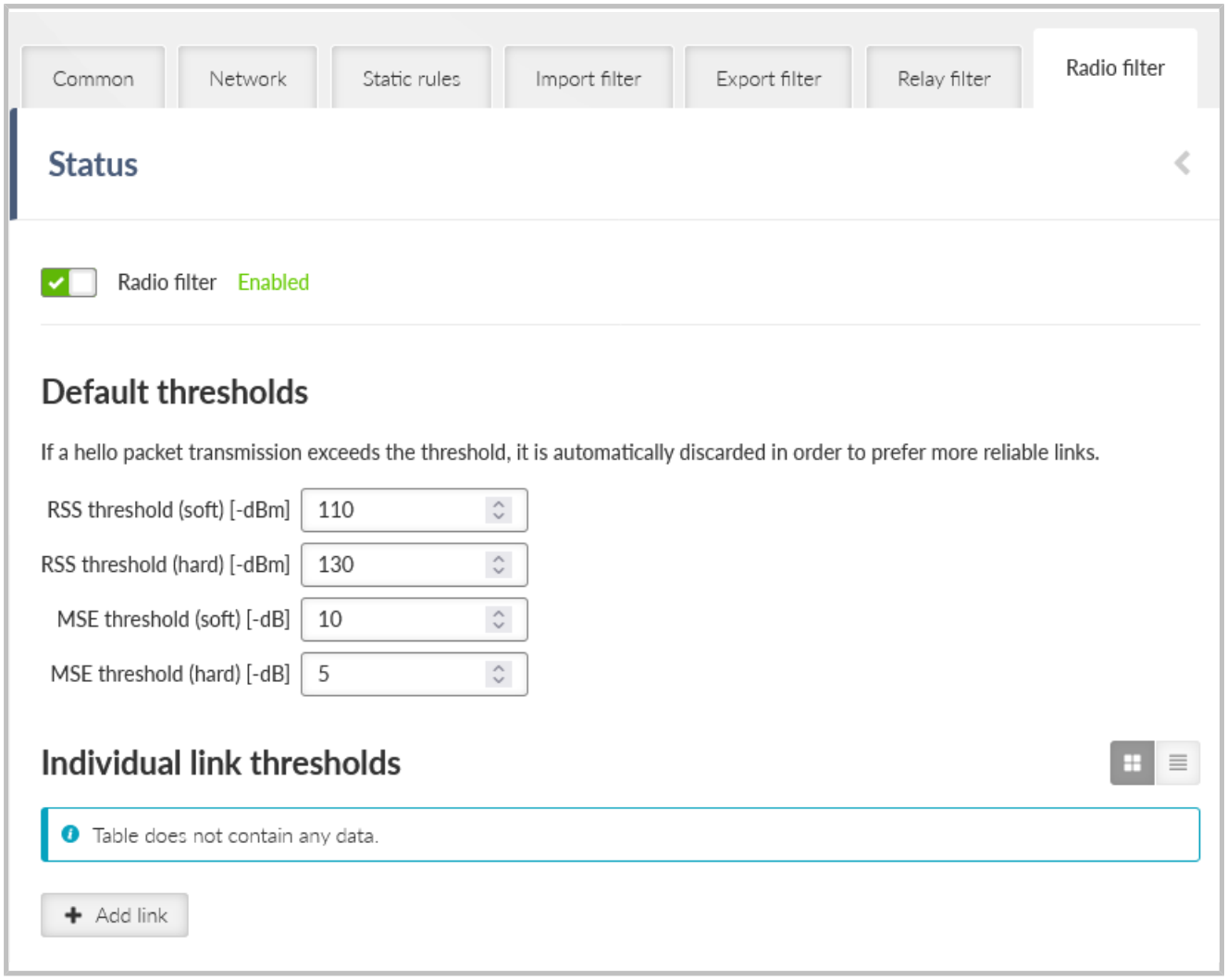
Increase metric
List box {Off; On}, default = "Off"
Enables incrementing Babel rule metrics on forwarding. It is used to penalize paths through this router. Only when Action is Accept or Pass.

Added metric	Number {1 – 65534}, default = 1
	Value added to the rule metric

7.2.3.8. Radio filter

The Radio Filter is a function designed to improve the reliability of Babel, by ensuring user traffic is only routed over high-quality radio links. The filter excludes links with weak signals or poor quality. This prevents routing via unreliable links when signal is strong enough to transmit/receive short Babel Hello packets (Babel overhead/logic), but too weak for regular user traffic.

The filter operates by applying configurable **Soft** and **Hard** thresholds to Received Signal Strength (RSS) and Mean Square Error (MSE) in received Babel Hello packets. Packets exceeding the **Hard** limit are always discarded; packets falling between the thresholds are discarded with a probability that increases linearly as quality degrades; and only packets meeting the **Soft** threshold are always accepted.



The Default thresholds contain settings for filtering Babel Hello packets based on the quality metrics of the received signal, these settings are applied to all links unless specific individual thresholds are configured.

RSS threshold (soft)
Number {50 – 150}, default = 110
RSS level limits [-dBm] of the received Hello packet
Soft limit is the worst value below which the packet is not discarded

RSS threshold (hard)
Number {50 – 150}, default = 130
RSS level limits [-dBm] of the received Hello packet
Hard limit is the best value to always discard the packet

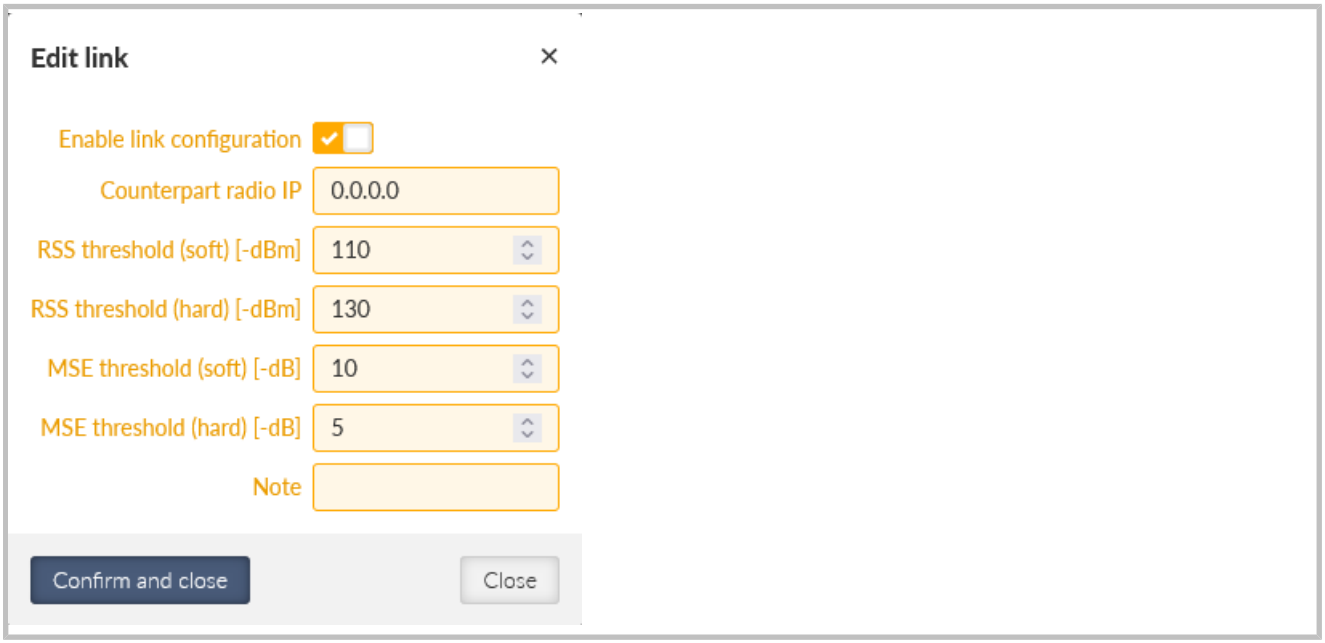
Note
Must be Soft threshold <= Hard threshold

MSE threshold (soft)
Number {0 – 60}, default = 10
MSE data level limits [-dB] of the received Hello packet
Soft limit is the worst value below which the packet is not discarded

MSE threshold (hard)
Number {0 – 60}, default = 5
MSE data level limits [-dB] of the received Hello packet
Hard limit is the best value to always discard the packet

Note
Must be Soft threshold >= Hard threshold

7.2.3.8.1. Indiviual link threshhold



Individual link thresholds contain settings for filtering Babel Hello packets with specific remote based on the source link address.

Enable link configuration
List box {Off; On}, default = "On"
Activates individual settings

Counterpart radio IP
IP address, default = 0.0.0.0
Radio IP address of the Hello packet source for which the individual filter setting applies

Note
Optional note

Advanced settings

Filter poisoned routes
List box {Off; On}, default = "Off"
Enables filtering of poisoned route rules (which arise, for example, when a routing rule is revoked) when importing from the Babel protocol to the babel_ipv4 table (and thus to other tables). It does not affect their retranslation (special behavior of the Babel protocol).

Filter routes with high metric
List box {Off; On}, default = "Off"

Enables filtering of rules with metrics higher than the set metric when importing from the Babel protocol to the babel_ipv4 table. These rules cannot be used for routing in the station or propagated to other stations. They serve to limit the size of routing tables, but if set incorrectly, they can result in remote network stations having no valid path between them.

Maximal accepted route metric
Number {1 - 65534}, default = 1000
The highest value of the imported routing rule metric that will still be accepted.

7.2.4. 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 RipEX2 router. OSPF provides Layer 2 dynamic routing. In the context of RipEX2 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 passphrase.
- 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 RipEX2 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.

7.2.4.1. 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
RipEX2 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).

7.2.4.2. OSPF Network - Areas and interfaces

7.2.4.2.1. Areas and interfaces

OSPF areas RipEX2 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. Of ‘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”
- Radio – “radio”
- Hot standby – “hstdby”
- GRE L3 – “gre_tunX” where ‘X’ is the tunnel number, starting from zero
- Cellular – “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 NMBA 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, Passphrase
List box {None; Keyed MD5 (OSPFv2); HMAC SHA256; HMAC SHA384; HMAC SHA512}, default = "None"
Selection of a method to authenticate the OSPF messages. Passphrase is used as a secret key for the selected hash function. Maximum length of the passphrase 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).

7.2.4.2.2. 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.

7.2.4.2.3. 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.

7.2.4.3. 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.

7.2.4.4. 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^{32}-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.

7.2.4.5. 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.

7.2.5. 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 RipEX2 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

7.2.5.1. 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
RipEX2 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).

7.2.5.2. 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^{32}-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.

Passphrase
String {up to 80 characters}
Passphrase 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^{32}-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 it 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.

7.2.5.3. 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.

7.2.5.4. 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^{32}-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.

7.2.5.5. 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^{32}-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.

7.2.5.6. 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^{32}-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.

7.2.5.7. 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^{32}-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^{32}-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.

7.3. Firewall

A firewall is a critical security tool that monitors and controls network traffic based on predefined rules. It acts as a protective barrier, filtering data packets to prevent unauthorized access, malicious attacks, and other threats.

Firewalls operate at Layer 2 (L2) and Layer 3 (L3) of the OSI model, offering features like packet filtering, traffic inspection, and stateful connection tracking for robust network protection.

7.3.1. Firewall L2

An L2 firewall operates at the data link layer, managing traffic based on MAC addresses and Ethernet frames within the same local network or broadcast domain. It can block or allow traffic based on source and destination MAC addresses, VLAN tags, or specific Ethernet frame types. L2 firewalls are essential for enforcing network segmentation, controlling device access, and optimizing bandwidth in narrowband networks.

7.3.1.1. Blocklist/Allowlist

L2 firewalls enable MAC address filtering to control network access. Administrators can define rules to allow or block traffic from specific devices, enhancing security and isolating compromised endpoints.

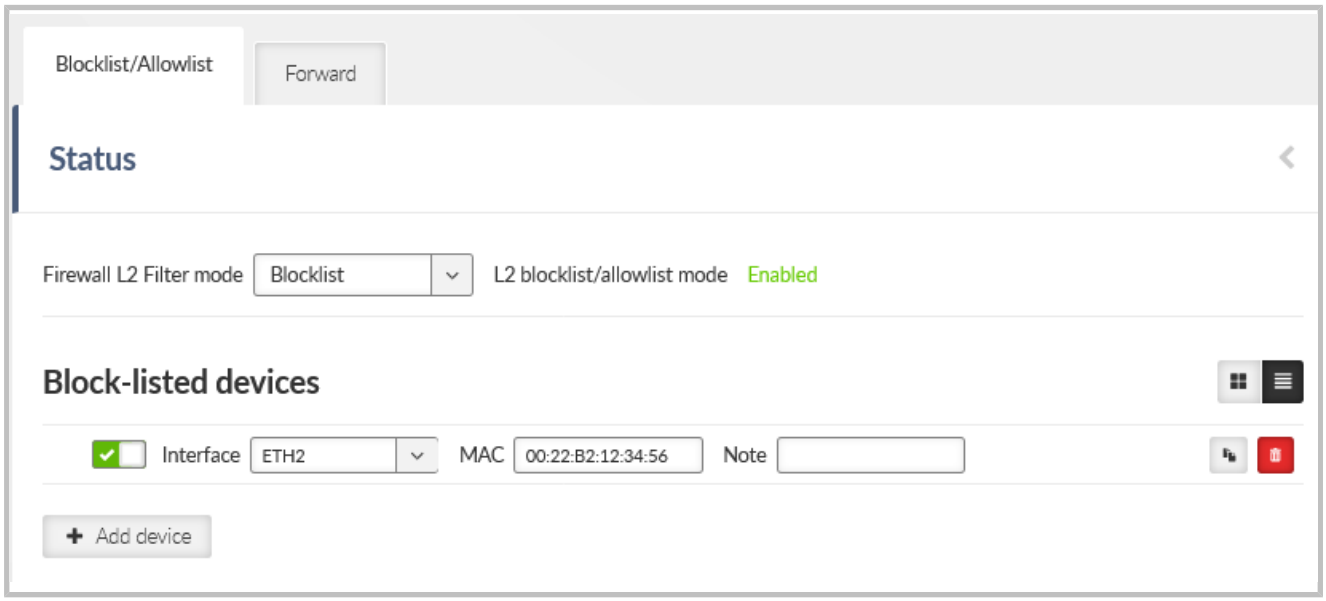


Fig. 7.16: SETTINGS > Firewall > L2

Filter mode

List box {Off; Blocklist; Allowlist}, default = "Off"

Blocklist

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.

Allowlist

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

These parameters are only visible when "Enable blocklist/allowlist rules logging" is checked.

Enable rule logging
List box {On, Off}, default = "On"
Activate logging for your blocklist/allowlist rule.

Rule logging identifier
String matching the regular expression "^[a-zA-Z0-9_-]{0,12}$", default = <empty>
Set an optional identifier for your rule in the log.

Rule logging severity
List box {Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug}, default = "Notice"
Select the log severity level for your rule.



Note

L2 firewall settings do not impact the local ETH access, i.e. settings never deny access to a locally connected RipEX2 (web interface, ping, ...).

7.3.1.2. Forward

Forward rules manage how Ethernet frames are handled within the broadcast domain. These rules control communication paths, enforce segmentation, and filter unwanted traffic. Forward filtering applies to packets traversing a bridge but not to traffic originating from or destined for the station.

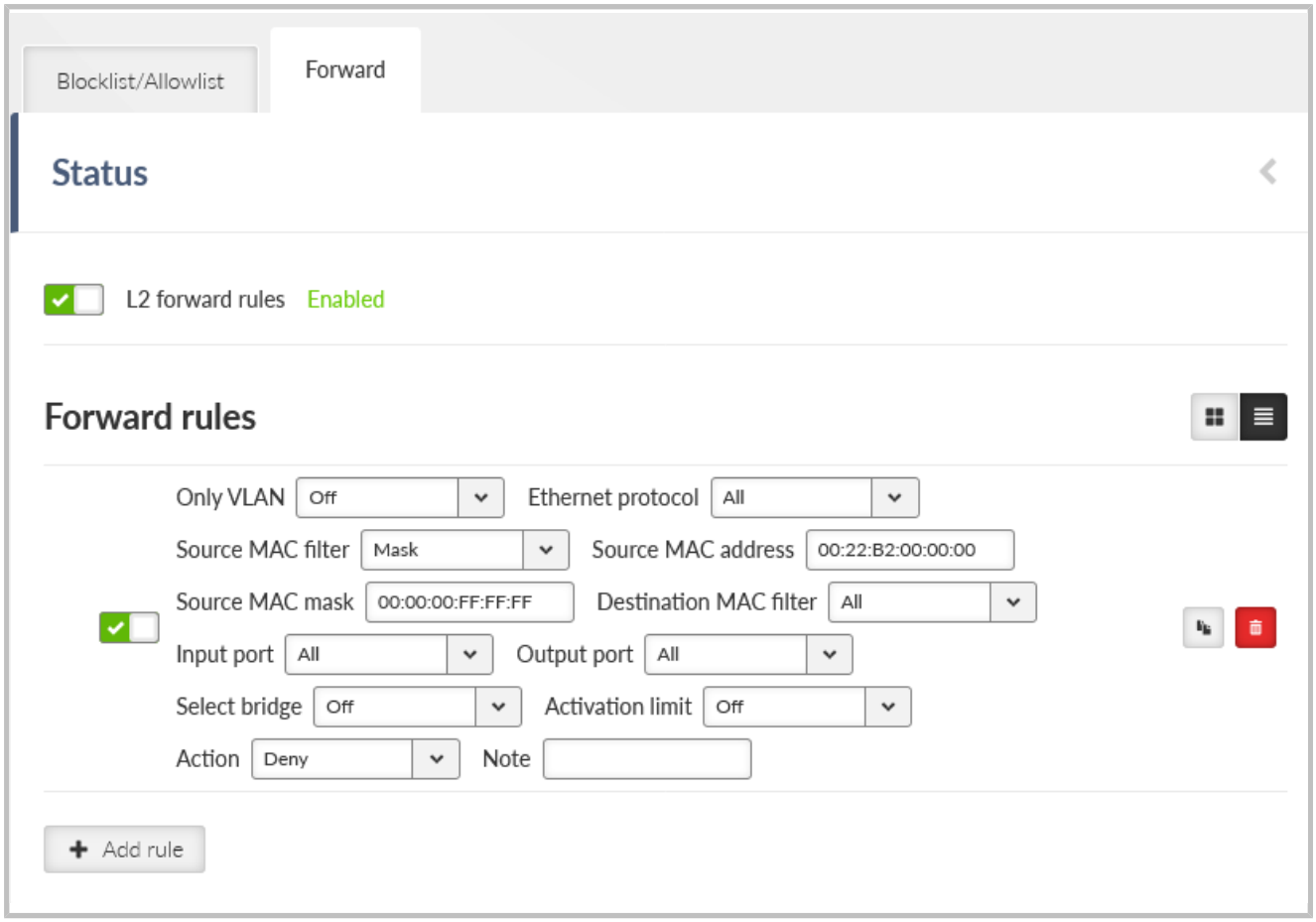


Fig. 7.17: SETTINGS > Firewall > L2 > Forward

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Only VLAN
List box {Off; On}, default = "Off"
Enables packet filtering for a specific VLAN and deep packet inspection.
If enabled:

VLAN
Number (0-4094), default = 1
ID of the filtered VLAN

Ethernet protocol
List box {All; Not VLAN; All VLAN; IPv4; IPv6; ARP; Other}, default = "All"
Filter based on EtherType (protocol carried in the Ethernet frame).

Source MAC filter
List box {All; Mask; Unicasts; Multicasts; Broadcasts}, default = "All"
Enables filtering based on the source MAC address of the packet.
For Mask option:

Source MAC address
Address used to compare against the source MAC address of packets.

Source MAC mask
Mask used to compare against the source MAC address of packets.

Destination MAC filter
List box {All; Mask; Unicasts; Multicasts; Broadcasts}, default = "All"
Enables filtering based on the destination MAC address of the packet.
For Mask option:

Destination MAC address
Address used to compare against the destination MAC address of packets.

Destination MAC mask
Mask used to compare against the destination MAC address of packets.

Input port
List box {All; Radio; All ETH; ETH1; ETH2; ETH3; ETH4; ETH5; GRE L2; OpenVPN L2; Other"}, default = "All"
Filters based on the port that the packet entered the bridge through.
For Other option:

Input port name
String {0–16 char}, default = <empty>
Name of the input port. Must be the name of an existing interface used as a bridge port.

Output port
List box {All; Radio; All ETH; ETH1; ETH2; ETH3; ETH4; ETH5; GRE L2; OpenVPN L2; Other"}, default = "All"
Filters based on the port that the packet exits the bridge through.
For Other option:

Output port name
String {0–16 char}, default = <empty>
Name of the output port. Must be the name of an existing interface used as a bridge port.

Select bridge
List box {Off; On}, default = "Off"
Enables limiting of the rule to a specific bridge. The rule will only be applied to packets that pass through the selected bridge.

Activation limit
List box {Off; On}, default = "Off"
Enables limiting the number of times the rule can be triggered per time unit.
If enabled:

Frame count
Number (1-10000), default = 3
Average packet/activation rate limit per time unit.

Measurement period
List box {Second, Minute, Hour, Day}, default = "Minute"
Time unit for limiting the packet/activation rate.

Burst size
Number (1-10000), default = 3
Initial and maximum number of TBF tokens. After a period of inactivity, TBF allows a burst of traffic to pass through at once. Must be greater than or equal to Frame count.

Action
List box {Deny; Allow}, default = "Deny"
Selects the action to be taken on a packet that matches the configured filter.

These parameters are only visible when "Enable forward rules logging" is checked.

Enable rule logging
List box {On, Off}, default = "On"
Activate logging for your forward rule.

Rule logging identifier
String matching the regular expression "^[a-zA-Z0-9_-]{0,12}$", default = <empty>
Set an optional identifier for your rule in the log.

Rule logging severity
List box {Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug}, default = "Notice"
Select the log severity level for your rule.

7.3.2. Firewall L3

An L3 firewall operates at the network layer, filtering traffic based on IP addresses and protocols. It enables control over data packets as they traverse different networks, allowing administrators to block or permit traffic based on source and destination IPs, port numbers, and protocol types. L3 firewalls are crucial for enforcing inter-network security, managing traffic flow, and protecting against external threats.

7.3.2.1. Forward

Forward rules in an L3 firewall control how IP packets are routed between networks. These rules specify whether traffic should be allowed or blocked as it passes through the router. Packets coming from addresses on the Blocklist are automatically dropped. By applying forward rules, administrators can manage traffic flow, enforce security policies, and prevent unauthorized access between different network segments.

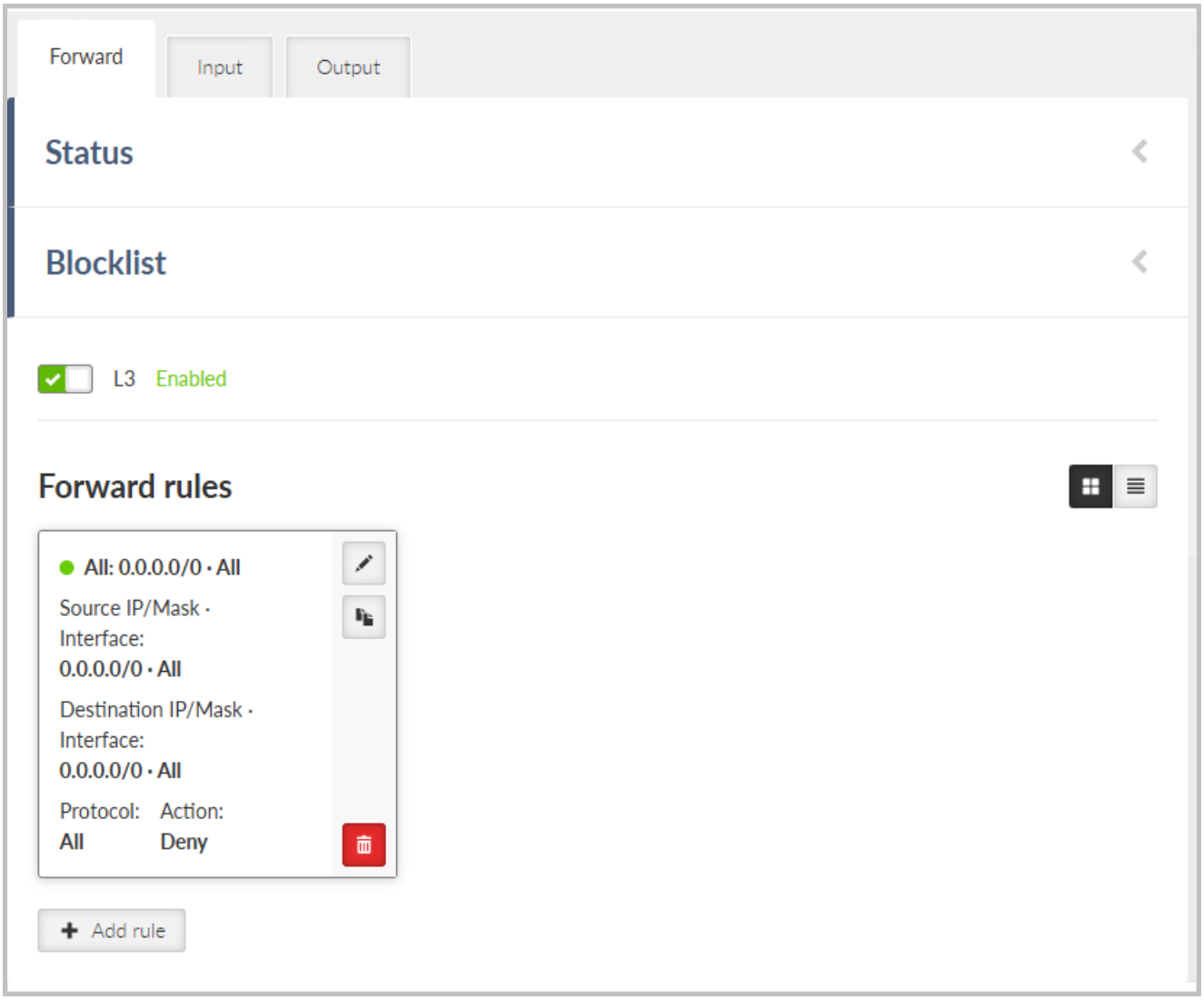


Fig. 7.18: SETTINGS > Firewall > L3

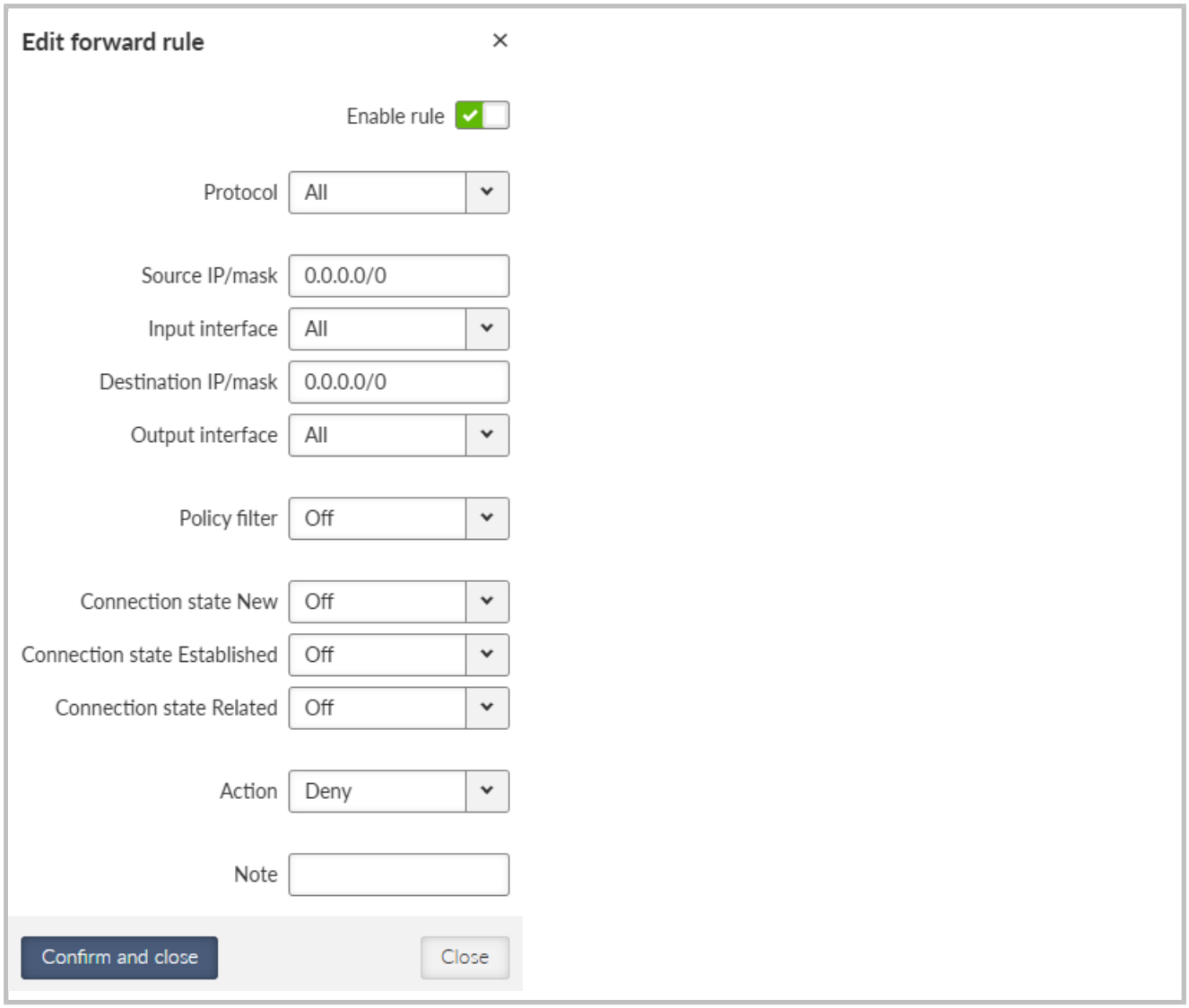


Fig. 7.19: SETTINGS > Firewall > L3 forward

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Select the transport protocol to filter by. The “All” option disables filtering by protocol.

Protocol number
Number (1-255), default = 1
The transport protocol number by which it is filtered. This parameter occurs only when parameter **Protocol** is set to "Other".

Source IP / Mask
IP address, Mask, default = 0.0.0.0/0
Source IP address/Mask of the packet. If mask is set to 0, it is not filtered by source IP address. The rule with narrower mask has higher priority. The rules order does affect priority.

Source port (from) / Source port (to)
Number (0-65536), default = 0
Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Input interface
List box {All; Radio; All ETH; EXT; ETH1..ETH5; All serial PPP; PPPoE client; GRE L2; GRE L3; OpenVPN L2; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the input device (interface, port) from which the packet came.

Input interface name
String (0-16 symbols), default = <empty>
The name of the input interface (or bridge port) of the packet.
This parameter occurs only when parameter Input interface is set to "Other".

Destination IP / Mask
IP address, Mask, default = 0.0.0.0/0
Destination IP address/Mask of the packet. If mask is set to 0, it is not filtered by destination IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Destination port (from) / Destination port (to)
Number (0-65536), default = 0
Interval of destination ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Output interface
List box {All; Radio; All ETH; EXT; All serial PPP; PPPoE client; GRE L3; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the output interface from which the packet leaves. Cannot select the bridge port.

Policy filter
List box {Off; On}, default = "Off"
Enables packet filtering according to the applied policy - IPsec.

Direction
Listbox: {In (Decapsulation), Out (Encapsulation)}, default = "Out (Encapsulation)"
Filters by packet processing direction.

Policy
Listbox: {None, IPsec}, default = "None"
Filters according to the policy applied to the packet:
None - The packet will not be processed by IPsec (decapsulation and encapsulation)
IPsec - The packet will be processed by IPsec

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 RipEX2 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 RipEX2 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 RipEX2 may be lost, when another RipEX2 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 RipEX2 (FORWARD chain).

Action

List box {Deny; Allow}, default = "Deny"
Selects the action to perform on a packet that matches the configured filter.

7.3.2.2. Input

Input rules in an L3 firewall regulate how IP packets destined for the router itself are handled. These rules determine whether traffic should be accepted or dropped based on factors like source IP address, protocol, and port number.

Packets coming from addresses on the Blocklist are automatically dropped. Addresses are added to the Blocklist as a result of an Input firewall rule with the Action set to "Deny, Add to Blocklist."

Additionally, the system creates automatic Input rules based on interface settings:

- Management access is limited on individual interfaces according to the "Allow unit management" setting for that interface.
- Remote access is restricted on individual interfaces based on the "Allow Remote access" setting for that interface.

By configuring input rules and interface settings, administrators can ensure robust protection against unauthorized access and direct attacks targeting the device.

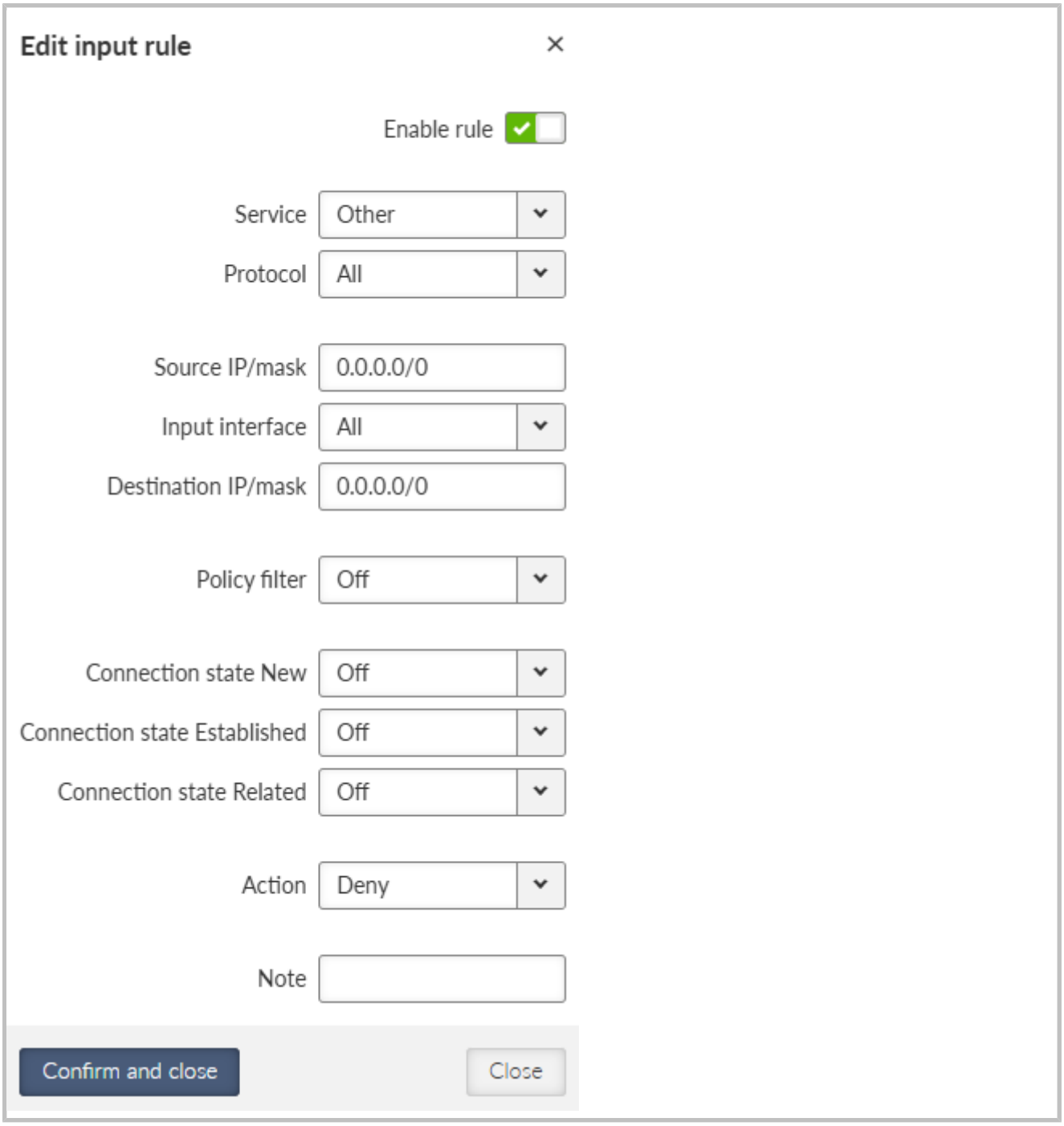


Fig. 7.20: SETTINGS > Firewall > L3 input

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

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

Allows you to select a known service on the station whose protocol and destination port the rule filter will capture.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Select the transport protocol to filter by. The “All” option disables filtering by protocol.

Protocol number
Number (1-255), default = 1
The transport protocol number by which it is filtered. This parameter occurs only when parameter **Protocol** is set to "Other".

Source IP / Mask
IP address, Mask, default = 0.0.0.0/0
Source IP address/Mask of the packet. If mask is set to 0, it is not filtered by source IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Source port (from) / Source port (to)
Number (0-65536), default = 0
Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Input interface
List box {All; Radio; All ETH; EXT; ETH1..ETH5; All serial PPP; PPPoE client; GRE L2; GRE L3; OpenVPN L2; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the input device (interface, port) from which the packet came.

Input interface name
String (0-16 symbols), default = <empty>
The name of the input interface (or bridge port) of the packet.
This parameter occurs only when parameter Input interface is set to "Other".

Destination IP / Mask
IP address, Mask, default = 0.0.0.0/0
Destination IP address/Mask of the packet. If mask is set to 0, it is not filtered by destination IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Destination port (from) / Destination port (to)
Number (0-65536), default = 0
Interval of destination ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Policy filter
List box {Off; On}, default = "Off"
Enables packet filtering according to the applied policy - IPsec.

Policy
Listbox: {None, IPsec}, default = "None"
Filters according to the policy applied to the packet:
None - The packet will not be processed by IPsec (decapsulation)
IPsec - The packet will be processed by IPsec

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 RipEX2 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 RipEX2 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 RipEX2 may be lost, when another RipEX2 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 RipEX2 (FORWARD chain).

Action

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

Selects the action to perform on a packet that matches the configured filter.

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

Output rules in an L3 firewall govern how IP packets originating from the router itself are handled. These rules allow administrators to control traffic sent by the router, specifying whether it should be allowed or blocked based on factors such as destination IP address, protocol, and port number. By configuring output rules, administrators can restrict unnecessary or potentially harmful outbound traffic, enforce security policies, and manage communication initiated by the router.

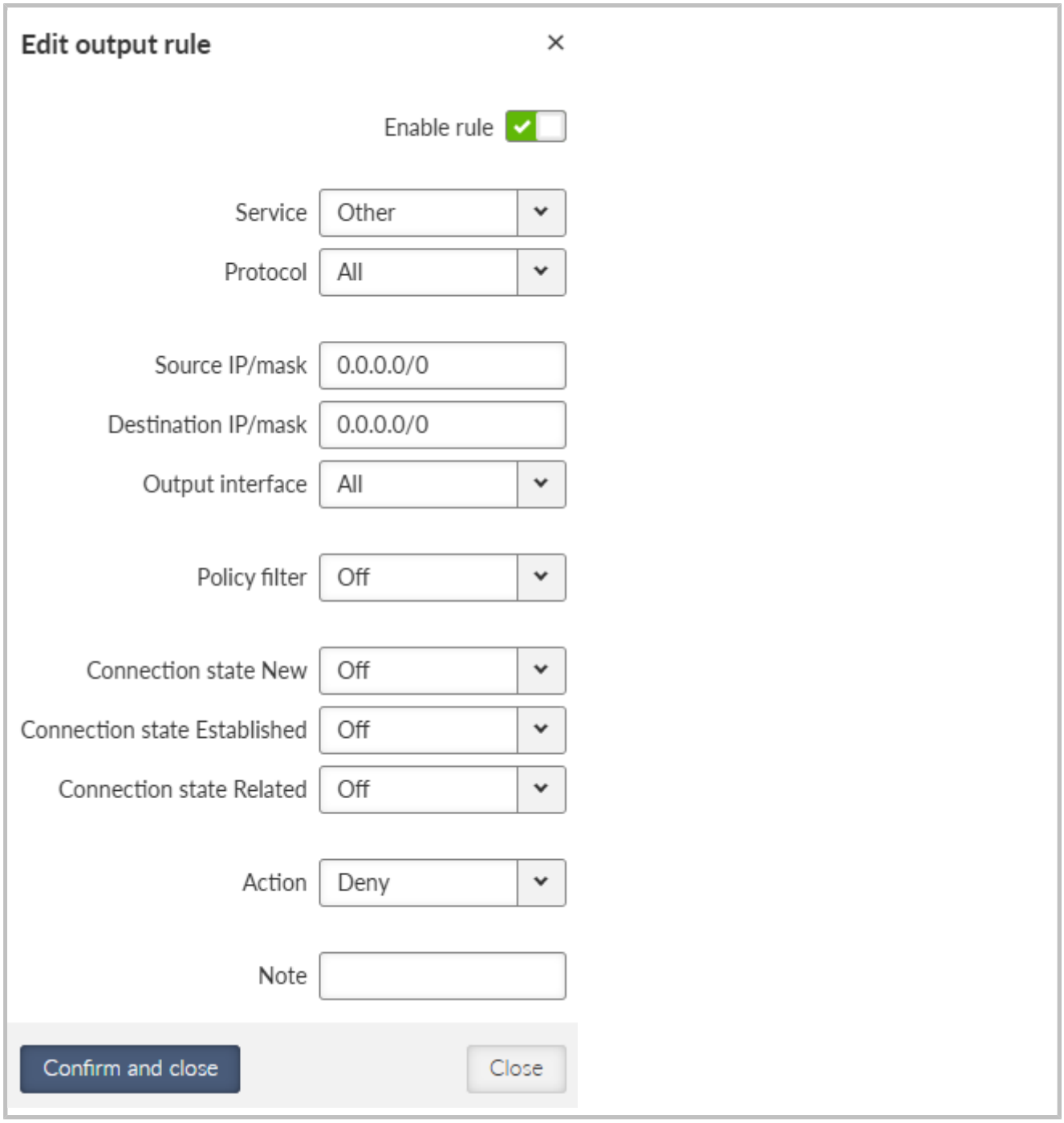


Fig. 7.21: SETTINGS > Firewall > L3 output

Each individual firewall rule is described by following parameters:

Enable rule
Check box {On; Off}, default = "Off"
Enables / disables L3 firewall rule.

Service
List box {Other; COM1; COM2; COM3; TS1; TS2; TS3; TS4; TS5; SSH; HTTP; HTTPS; Remote access; SNMP; NTP}, default = "Other"
Allows you to select a known service on the station whose protocol and destination port the rule filter will capture.

Protocol
List box {All; ICMP; UDP; TCP; GRE; ESP; Other}, default = "All"
Select the transport protocol to filter by. The “All” option disables filtering by protocol.

Protocol number
Number (1-255), default = 1
The transport protocol number by which it is filtered. This parameter occurs only when parameter **Protocol** is set to "Other".

Source IP / Mask
IP address, Mask, default = 0.0.0.0/0
Source IP address/Mask of the packet. If mask is set to 0, it is not filtered by source IP address. The rule with narrower mask has higher priority. The rules order does affect priority.

Source port (from) / Source port (to)
Number (0-65536), default = 0
Interval of source ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Destination IP / Mask
IP address, Mask, default = 0.0.0.0/0
Destionation IP address/Mask of the packet. If mask is set to 0, it is not filtered by destination IP address.
The rule with narrower mask has higher priority. The rules order does affect priority.

Destination port (from) / Destination port (to)
Number (0-65536), default = 0
Interval of destination ports. This parameter occurs only when parameter **Protocol** is set either to "UDP" or "TCP".

Output interface
List box {All; Radio; All ETH; EXT; All serial PPP; PPPoE client; GRE L3; OpenVPN L3; Hot standby; Other}, default = "All"
Selects the output interface from which the packet leaves. Cannot select the bridge port.

Output interface name
String (0-16 symbols), default = <empty>
The name of the output interface of the packet.
This parameter occurs only when parameter Input interface is set either to "Other".

Policy filter
List box {Off; On}, default = "Off"
Enables packet filtering according to the applied policy - IPsec.

Policy
Listbox: {None, IPsec}, default = "None"
Filters according to the policy applied to the packet:
None - The packet will not be processed by IPsec (encapsulation)
IPsec - The packet will be processed by IPsec

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 RipEX2 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 RipEX2 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 RipEX2 may be lost, when another RipEX2 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 RipEX2 (FORWARD chain).

Action

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

Selects the action to perform on a packet that matches the configured filter.

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).

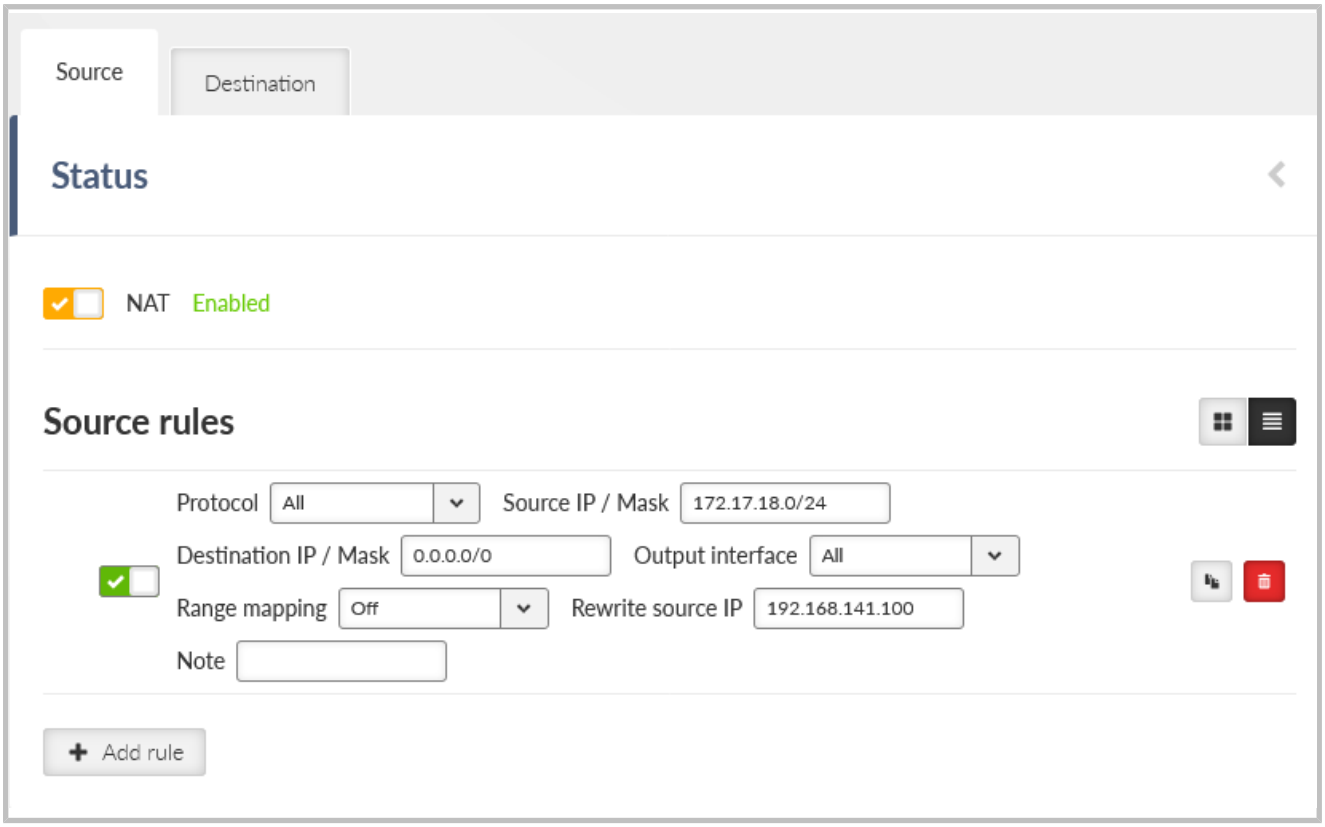


Fig. 7.22: SETTINGS > Firewall > NAT

- 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”.

Each individual NAT rule is described by following parameters:

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

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 "**Procotol**" 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 "**Procotol**" is set to "UDP" or "TCP".

Output Interface
List box {All; Radio; All ETH; EXT; GRE L3; Hot standby; Other}, default = "All"
Filters selected interfaces.

Output interface name
Has to be set as one of existing interfaces ("radio", 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).

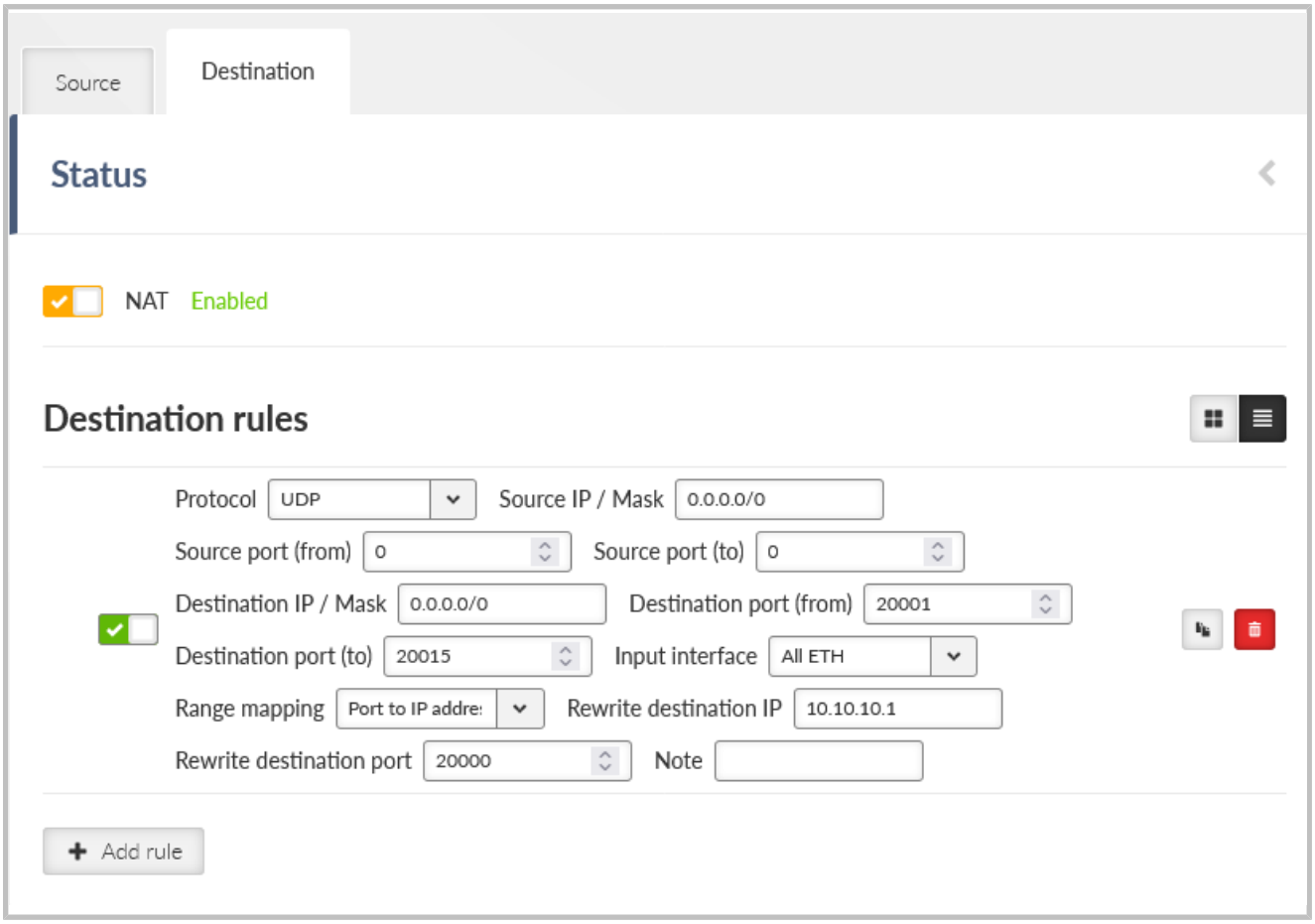


Fig. 7.23: SETTINGS > Firewall > NAT > Destination

- 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”.

Each individual NAT rule is described by following parameters:

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

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 on the same number. These parameters occur only, if parameter "**Procotol**" 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 "**Procotol**" is set to "UDP" or "TCP".

Input interface
List box {All; Radio; All ETH; EXT; GRE3; Hot standby; Other}, default = "All"
Filters selected interfaces.

Input interface name
Has to be set as one of existing interfaces ("radio", 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**".
  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.

Note

FTP connection is a special type of TCP with multiple sessions being opened and internal functionality. If you configure DNAT for the connected FTP server, enable the “FTP connection tracker” parameter and specify a correct port (default is 21). These parameters can only be set in the Advanced menu.

7.3.3.3. Cooperation with other services

- MASQUERADE rule for Cellular connection has lower priority that 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 RipEX2 (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 7.4.1.3.3, “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) changes 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.

Note

OpenVPN and IPsec are not suitable for the narrowband radio networks with the capacity of several kb/s or Mb/s. Both VPN protocols are designed for fast speed Ethernet connections of 100-1000 Mb/s. If you need to encrypt the Radio channel, use its AES256 Encryption option. Utilize OpenVPN or IPsec on Ethernet or cellular interfaces. On the other hand, both VPN options will work on the Radio channel as well, but could slow down the overall network operation.

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.

There are 2 modes of operation, RipEX2 offers both the Tunnel mode and the Transport 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. In Transport mode, only the payload of the original IP packet is encrypted and authenticated. The original IP header remains intact, allowing for direct routing, while the data itself is secured using AH or ESP protocols.

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 RipEX2.

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 RipEX2.

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 RipEX2 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 (passphrase).

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).
- It the re-authentication is not required - only new IKE SA keys are generated and exchanged.

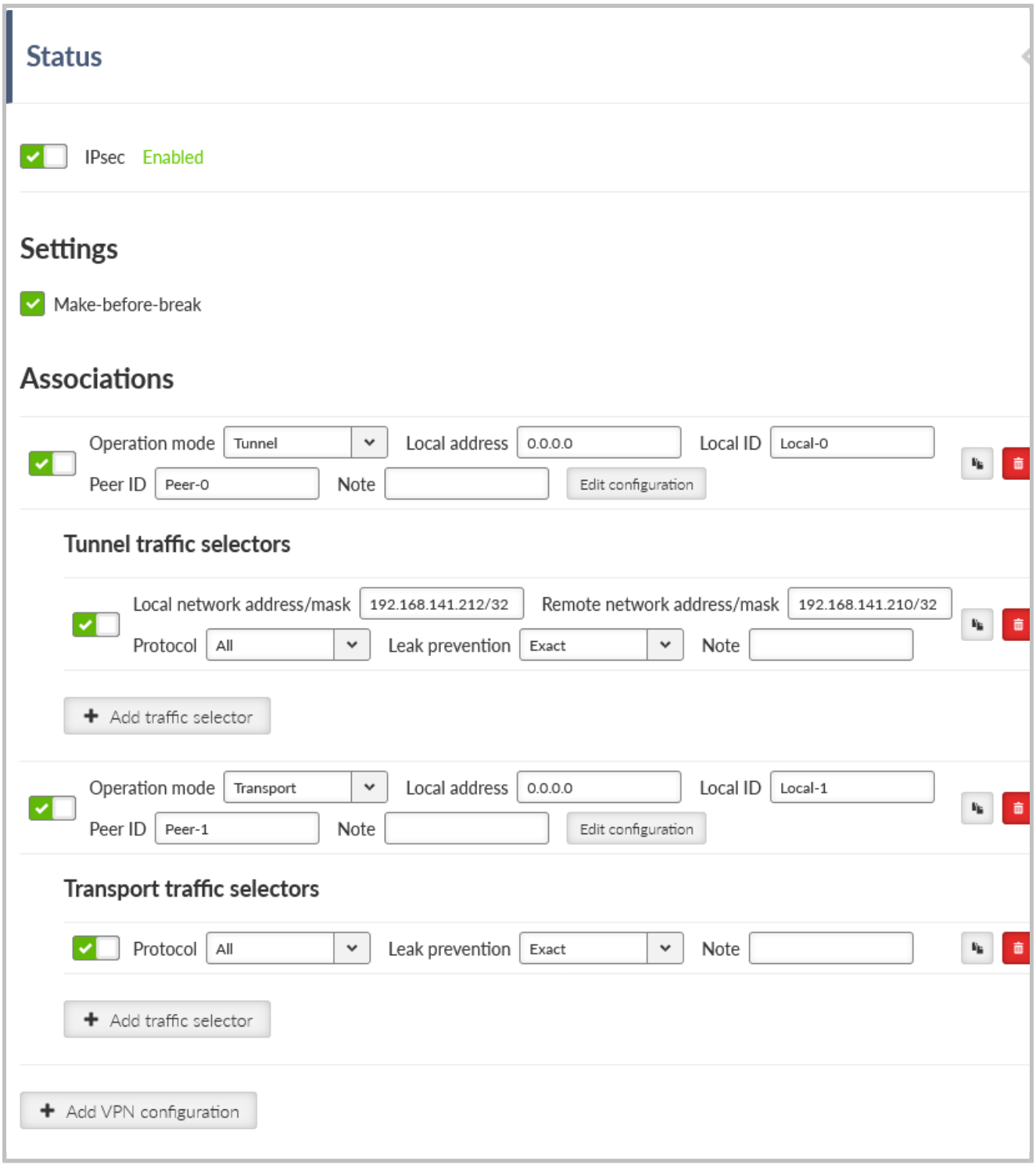


Fig. 7.24: SETTINGS > VPN > IPsec

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.

Operation mode
List box {Tunnel; Transport}, default = "Tunnel"
Selects IPsec mode



Note
The Tunnel mode is usually used for site-to-site and host-to-site connections. The Transport mode is used for host-to-host connection and very often combined with GRE and dynamic routing.

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).



Local address

IP address, default = "0.0.0.0"

IP address used as the source address for IKE negotiation. If specified, must be a valid local address.

When left at 0.0.0.0 the Local address becomes dynamic.

Peer address

IP address, default = "0.0.0.0"

IP address of the peer running the IKE daemon that will be negotiated with. It must not be the same as Local address.

Local ID

IP address or FQDN (Fully Qualified Domain Name), default = "Local-0"

IP address or FQDN 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), default = "Peer-0"

IP address or FQDN 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.

Start state

List box {Passive; On demand; Start}, default = "Passive"

Passive - the connection is not established, it is waiting for the other side.

On Demand - The connection will start to establish when a packet tries to pass through it.

Start - the connection is established immediately.

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 = "Off"
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

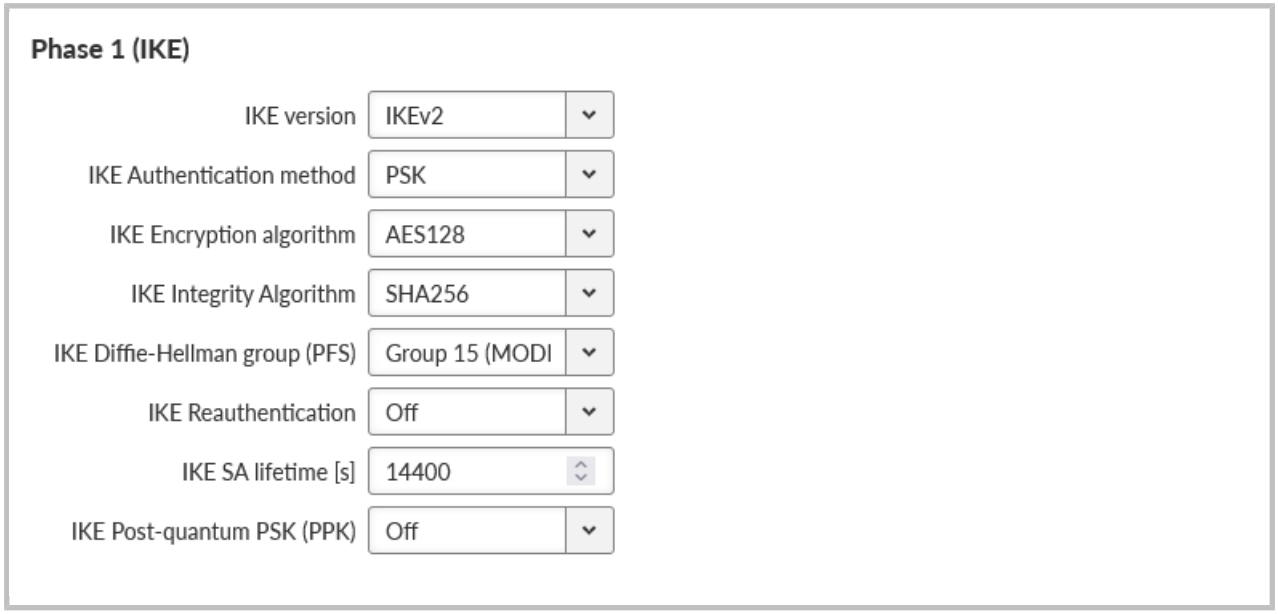
List box {Clear; Hold; Restart}, default = "Hold"
One of three connection states automatically activated when connection loss is detected:
Clear – connection is closed and waiting
Hold – connection is closed. Connection is established when first packet transmission through tunnel is attempted.
Restart – connection is established immediately
This parameter is available only if parameter **Dead Peer Detection** is set to "On".

Management mode

List box {Off; Master; Slave}, default = "Off"
Selects how to manage the IPsec association.
Master - Managed by the Link Manager. Defines the Traffic selector of the tunnel.
Slave - Managed by the Link Manager. Takes over Traffic selectors from the Master Association.
This parameter is available only if parameter **Link management** is set to "On".

Phase 1 IKE

Parameters related to IKE SA (IKE Security Association) provide SA keys exchange with the peer.



IKE version

List box {IKEv2, IKEv1}, default = "IKEv2"
IKE version selection.
Must match the settings on the peer.

IKE Authentication method

List box {PSK}, default = "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.

IKE Encryption algorithm

List box {3DES (legacy); AES128; AES192; AES256; AES128CCM (AEAD); AES192CCM (AEAD); AES256CCM (AEAD); AES128GCM (AEAD); AES192GCM (AEAD); AES256GCM (AEAD); ChaCha20Poly1305 (AEAD)}, default = "AES128"
IKE SA encryption algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

IKE Integrity 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.

IKE 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.

IKE 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.

IKE 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 RipEX2's channel load can affected during the key exchange process.

IKE Post-quantum PSK (PPK)

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

Enables additional protection using PPK when using IKEv2.

IKE PPK ID

String {0–64 char}, default = <empty>

PPK key identifier, which can be an FQDN. It must not be empty or the same as the identifier in another IKE SA. It is used to identify and select the PPK key between peers, and they must have the same identifier.

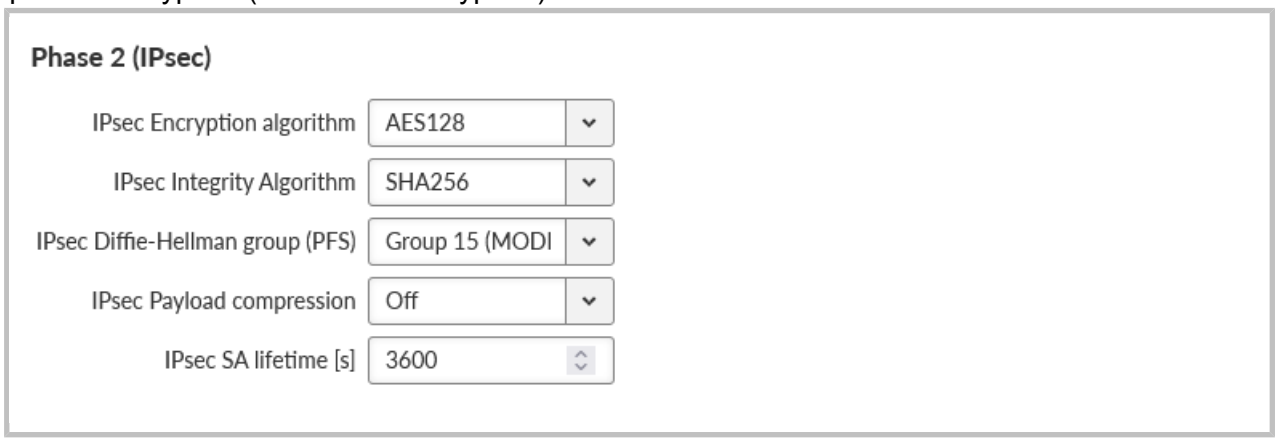
IKE PPK KEY ID

List box {None; Radio Encryption Key}, default = "None"

Key identifier in the keyring. The key must exist and be populated with the type 'psk' and a length of at least 32B (256 bits).

Phase 2 – IPsec

Certain parameters are shared by all subordinate CHILD SA. IPsec Security Association provides packet encryption (user traffic encryption).



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.

IPsec Integrity 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.

IPsec 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

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

This parameter enables payload compression. This takes place before encryption. Peer configuration must match.

IPsec SA lifetime [s]

Number {180 – 86400}, default = 3600

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 RipEX2's channel load can affected during the key exchange process.

PSK

PSK (Pre-shared key) authentication is used for IKE SA authentication. The relevant peer is identified using it's "Peer ID". The key must be the same for both local and peer side of the IPsec.



Mode

List box {Passphrase; Key ID}, default = "Passphrase"

Passphrase

The PSK key is entered as a passphrase. An empty passphrase is not allowed (max. length is 128 characters). Passphrase for the FW version 2.1.1.0 must not contain any unsupported characters. Unsupported characters are: ", `, \, $, ;. The full UTF-8 character set is available since FW 2.1.2.0.

Note

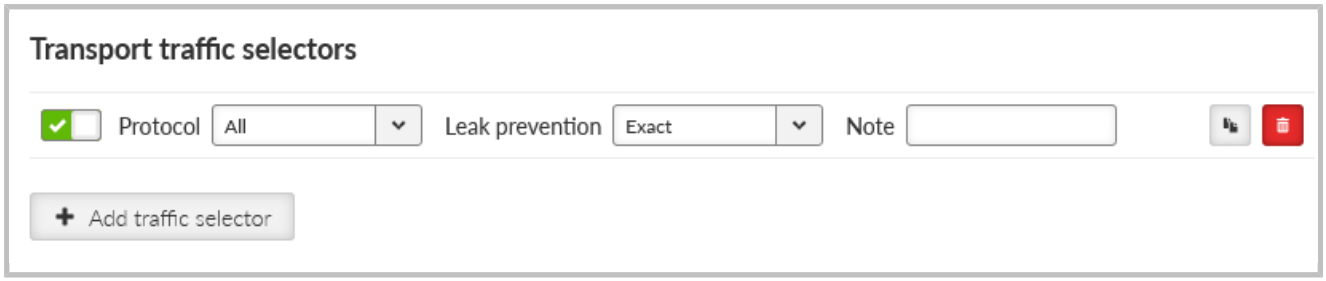
If the passphrase starts with the characters 0x or 0s, then the connection between RipEX2 with FW 2.1.2.0 (and newer) and RipEX2 with FW 2.1.1.0 (and older) will not be established. Likewise, any other device that writes the passphrase into its configuration as a plain string (not 'hexa' or 'base64' encoded).

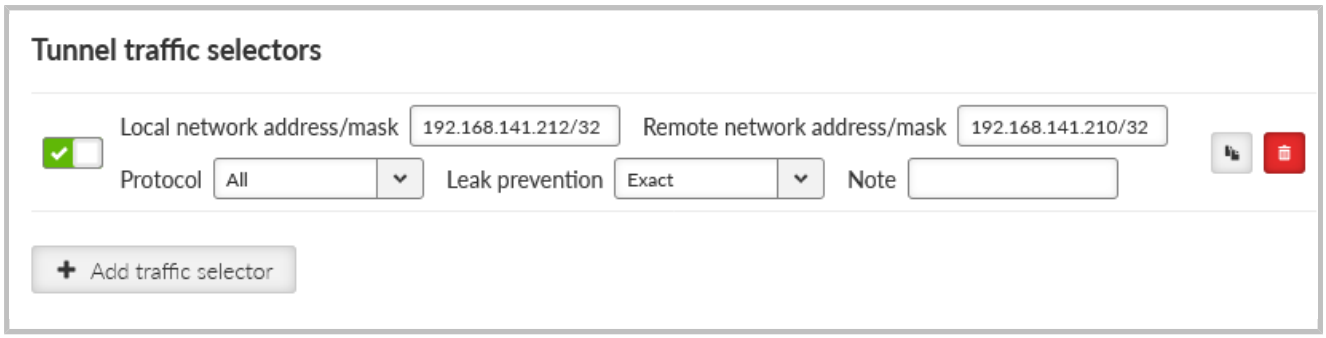
Key

It is possible to set 256 bits long Key instead of Passphrase. This parameter occurs only, if parameter **Mode** is set to "Key".

7.4.1.2.1. Transport/Tunnel Traffic selectors

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.





Local network address / Mask
IP address/Mask, default = "0.0.0.0/32"
Source IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

Remote network address / Mask
IP address/Mask, default = "0.0.0.0/32"
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".

Leak prevention
List box {Off; Exact; Paranoid}, default = "Exact"
The level of automatic protection against leaking or receiving unencrypted traffic.
Off - No automatic protection rules. The user must write his own in the L3 firewall.
Exact - Automatic rules exactly copy the CHILD SA settings.
Paranoid - For input/forward rules it's the same as Exact. For output, the automatic rules are stricter because they do not filter by the source address of the packet.

7.4.1.3. Cooperation with other services

7.4.1.3.1. Automatically generated routing rules

For Tunnel mode, a special IPsec routing table is created to correctly fill in the source IP address of packets sent from the unit over IPsec.

For each traffic selector (CHILD SA), the service tries to find a local IP address that matches the address and mask of the local part of the selector. If such an address exists, an auxiliary routing rule is created in the IPsec table that has the address and mask of the remote part of the selector as the destination and the found local address as the local preferred source address. With this rule, the locally generated packets will have addresses that match the CHILD SA selector and will be encrypted.

At the same time, the existence of a routing rule for the packet is ensured. If the routing rule did not exist, the packet would be dropped before being captured and encrypted by IPSec.

Note

If the selector is limited to a specific protocol, however, a routing rule will not be created because it would cover all protocols, including traffic that the selector does not capture.

User routing is required for Transport mode; without it, the IKE SA association could not be established. This mode does not use the special IPsec routing table.

7.4.1.3.2. Manually created firewall rules

A user-defined firewall filters packets before or after encryption in IPsec. If automatic protection against leakage of unencrypted traffic is disabled, custom protection rules (**Policy filter**) can be applied.

Handwritten protection rules must prevent

Sending traffic to be encrypted as unencrypted (data leakage).
Receiving unencrypted traffic that should have been encrypted (data insertion).

Tunnel mode

INPUT - For each traffic selector (CHILD SA) a rule discarding traffic with **Policy** “None” and with swapped address ranges.
OUTPUT - For each traffic selector (CHILD SA) a rule discarding traffic with **Policy** “None” and with the same address ranges.
FORWARD - For each traffic selector (CHILD SA) 2 rules:
Discarding traffic with **Policy** “None” and **Direction** “Out (Encapsulation)” and with the same address ranges.
Discarding traffic with **Policy** “None” and **Direction** “In (Decapsulation)” and with swapped address ranges.

Transport mode

INPUT - For each traffic selector (CHILD SA), a rule to discard traffic with a **Policy** set to “None” and with a source address of the IPsec peer address and a destination address of the IPsec local address.
OUTPUT - For each traffic selector (CHILD SA), a rule to discard traffic with a **Policy** set to “None” and with a source address of the IPsec local address and a destination address of the IPsec peer address.

7.4.1.3.3. 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

7.4.2.1. 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 RipEX2 IPv4 network.

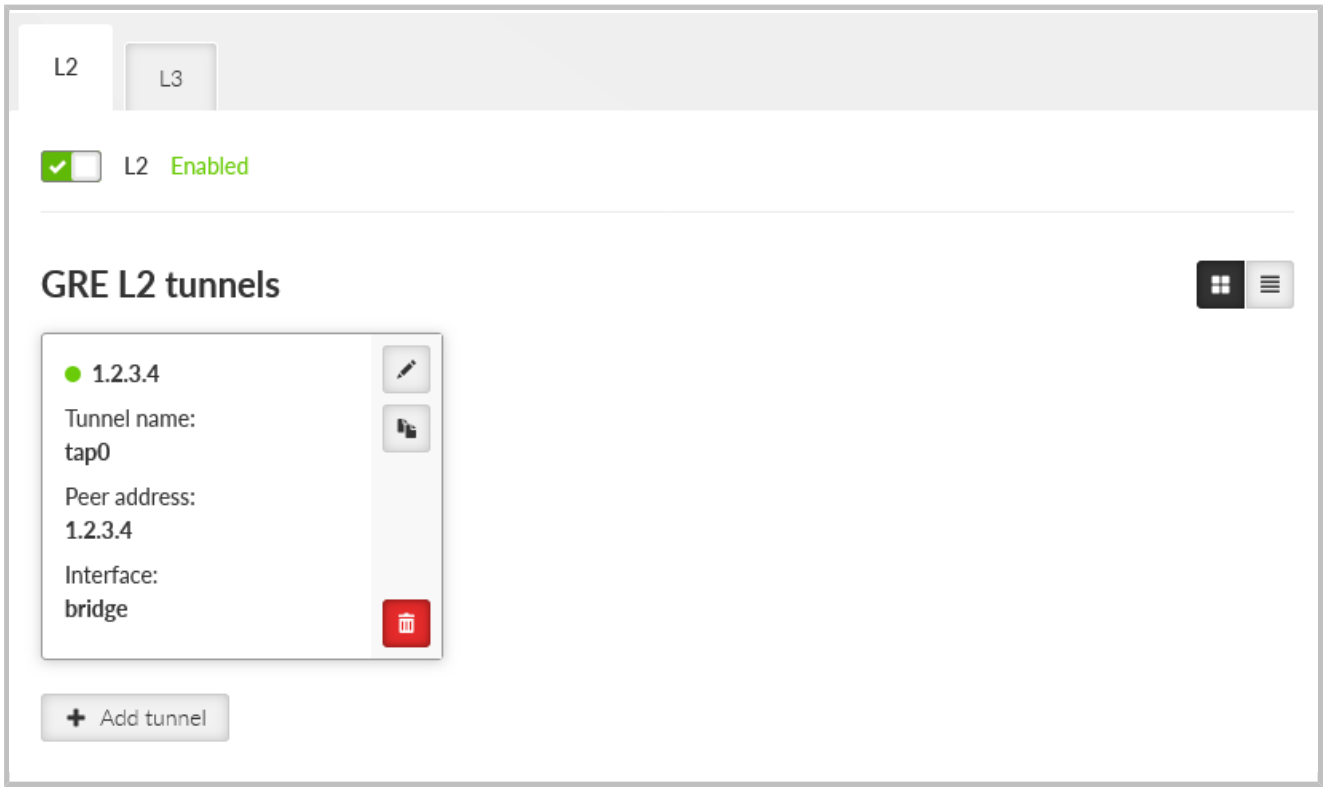
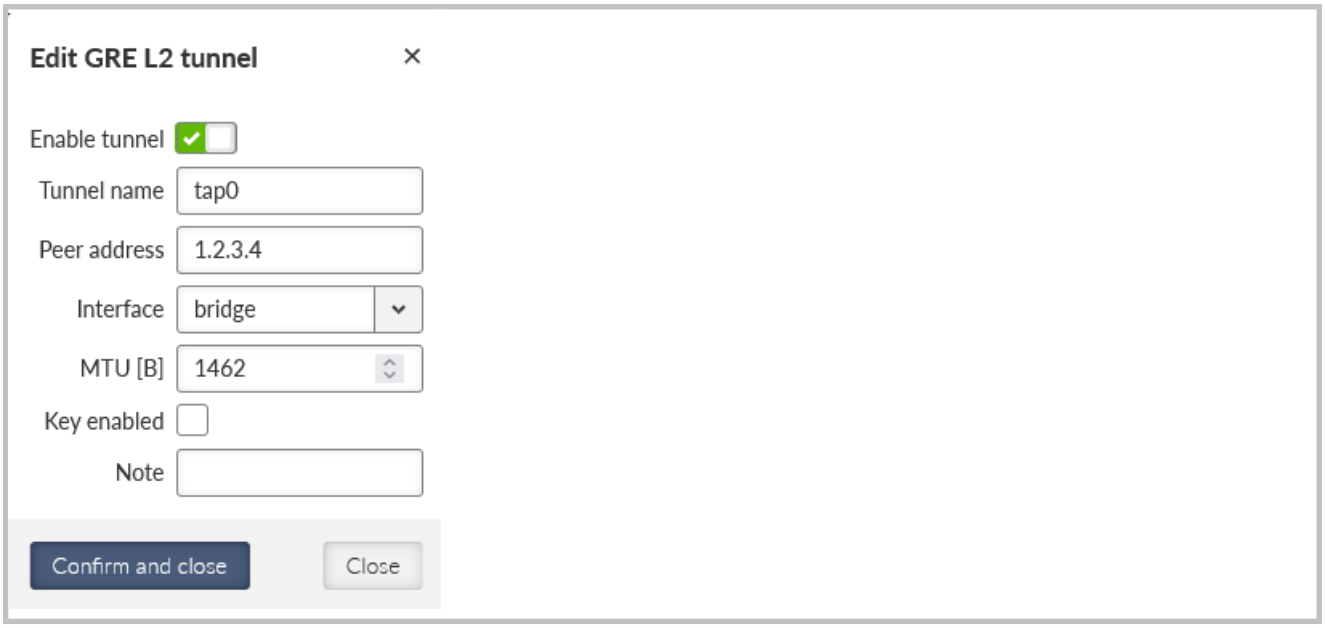


Fig. 7.25: SETTINGS > VPN > GRE

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.

Tunnel name
The base of the tunnel interface name, prefixed with "gre_".

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.

Interface
Has to be set as one of existing bridge's name in SETTING/Interfaces/Ethernet/ Network interface Name.

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 RipEX2 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.

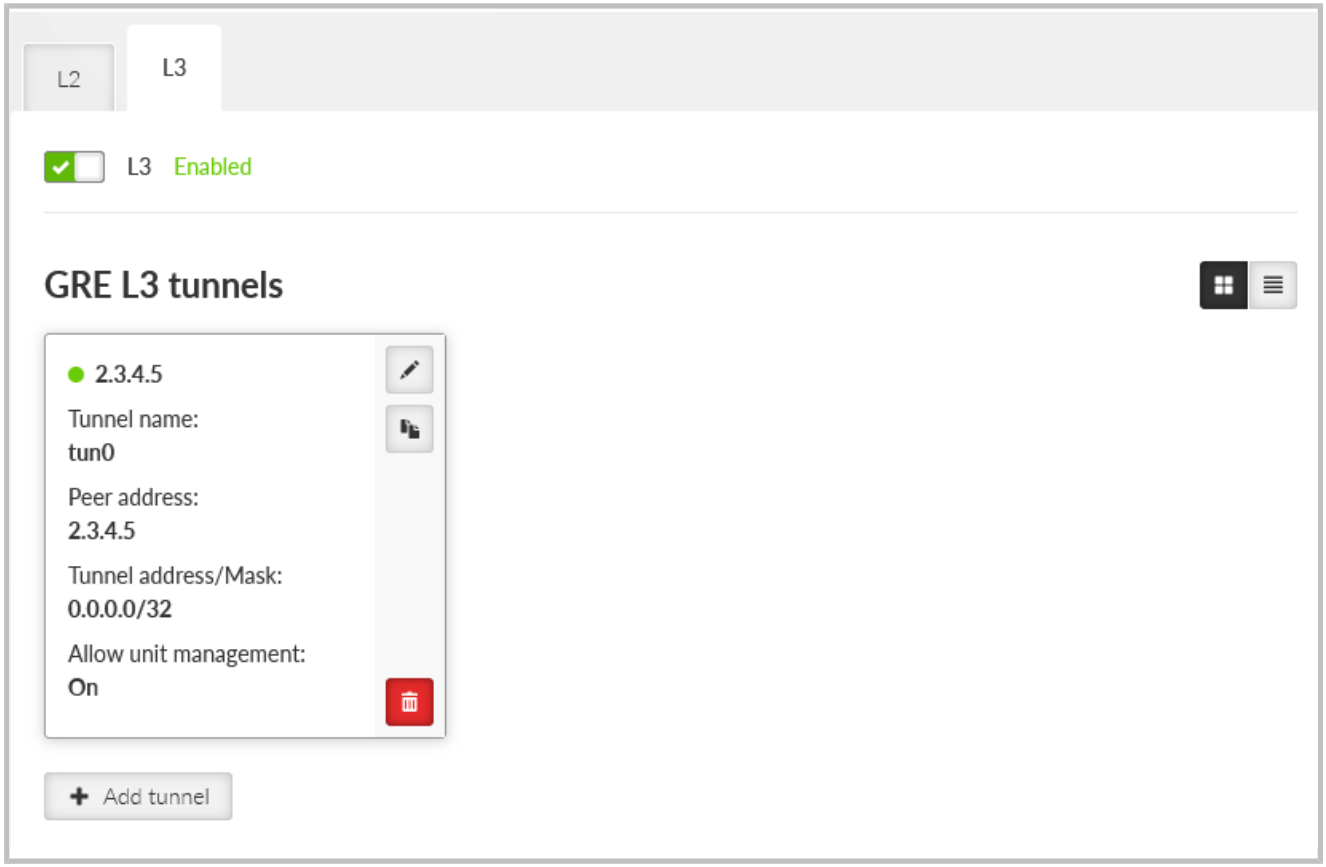
Key enabled
Enables using key identification of the tunnel from/to the same peer.

Key
Identification number of the tunnel Number {0 – 4,294,967,295}, default = 0

Note
Optional comment.

7.4.2.2. 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.

Tunnel name
The base of the tunnel interface name, prefixed with "gre_".

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

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 RipEX2 units = 576 B.

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

Allow unit management
Allows / disables unit management via GRE tunnel.

Note
Optional comment.

7.4.3. OpenVPN

OpenVPN is a virtual private network (VPN) system that allows to create secure encrypted point-to-multipoint connections in routed (TUN) or bridged (TAP) modes. Up to four instances (clients and/or servers) can be used simultaneously in one unit. Each server is capable of establishing connections with several tens of clients.

OpenVPN allows peers to authenticate to each other using pre-shared secret keys and certificates. An OpenVPN server is capable to release an authentication certificate for every client, using signatures and certificate authority (certificates can be generated / uploaded in the SETTINGS>Security>Credentials menu).

A time synchronisation of individual units is required for proper OpenVPN function.

Link for *OpenVPN application note*[5].

[5] https://www.racom.eu/eng/products/m/ripex/app/openvpn/intr.html

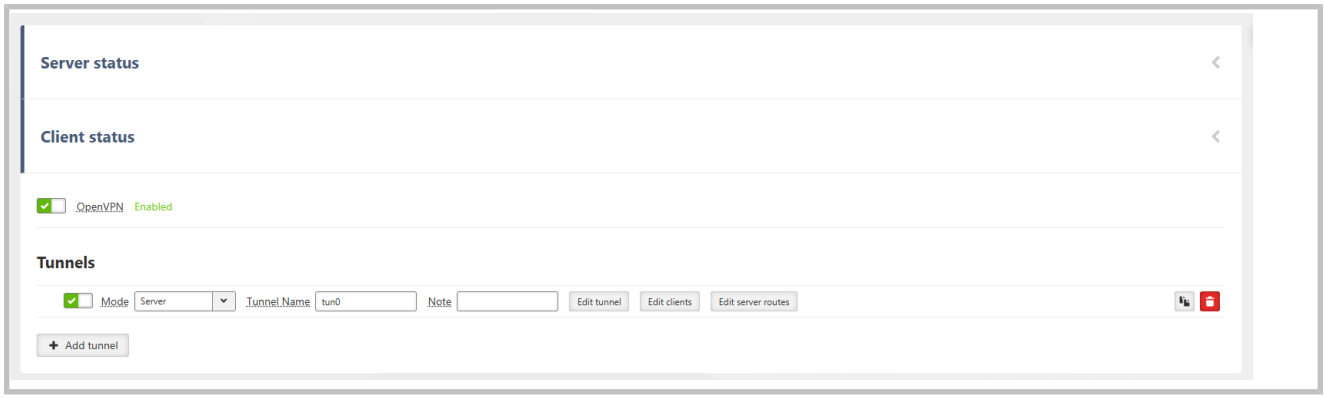


Fig. 7.26: SETTINGS > VPN > OpenVPN

OpenVPN Enable

List box {Off; On}, default = "Off"
Turns on the entire OpenVPN system.

OpenVPN Tunnel Enable

List box {Off; On}, default = "On"
Enables / disables a particular OpenVPN tunnel.

Mode

List box {Client; Server}, default = "Client"
Instance mode selection.
Server: Server passively listens and waits for client connections (one or more), then assigns addresses and sets up routing.
Client: Client actively connects to the server and retrieves part of the configuration.

Tunnel name

String, default = "tun0"
String matching regular expression '^[a-zA-Z0-9_-]{1,10}$'. User part of the OpenVPN tunnel interface name, prefixed with 'ovpn_'. Must be unique among active OpenVPN instances.

Note

Optional comment.

7.4.3.1. OpenVPN tunnel

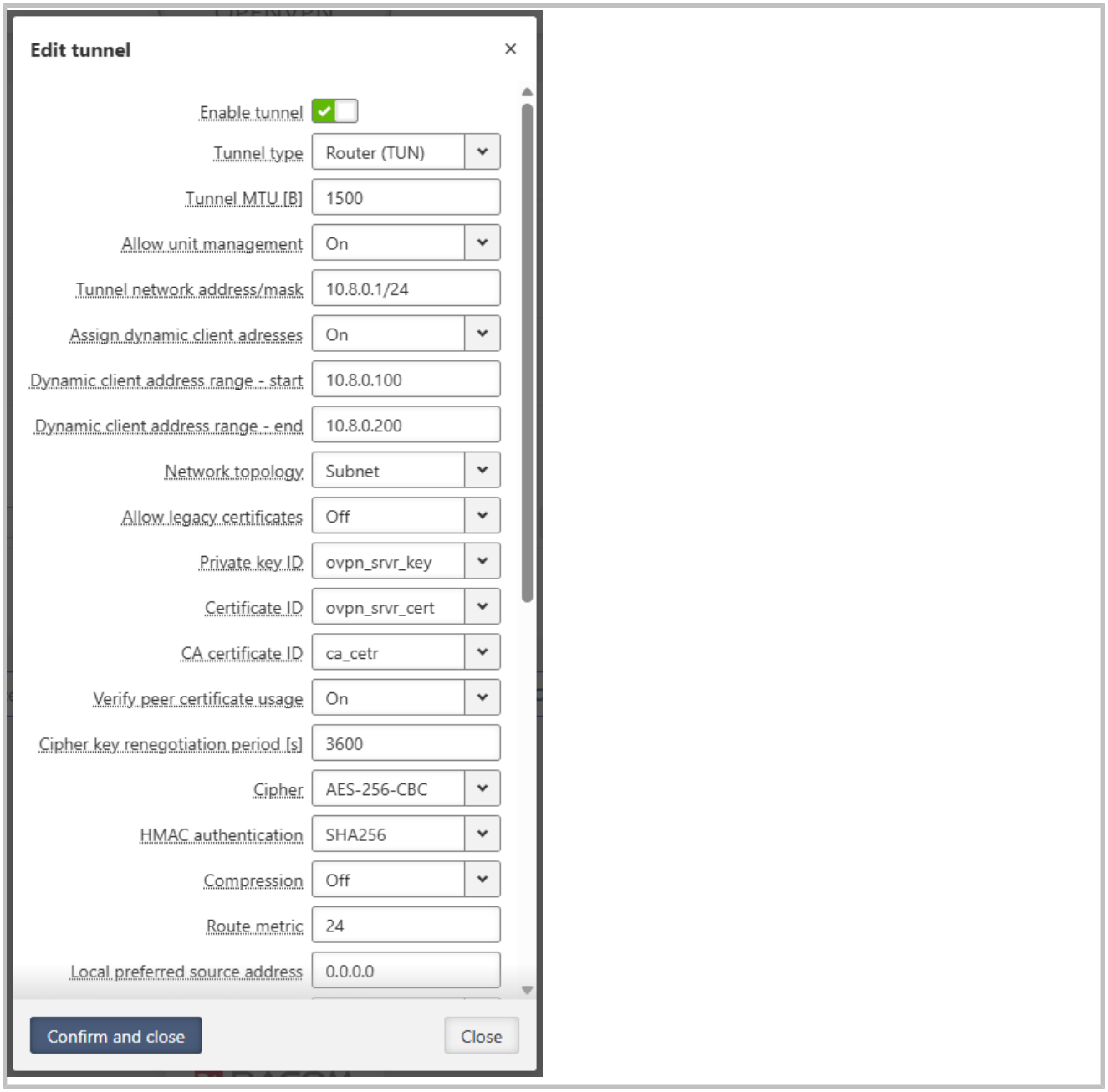


Fig. 7.27: OpenVPN Router tunnel settings

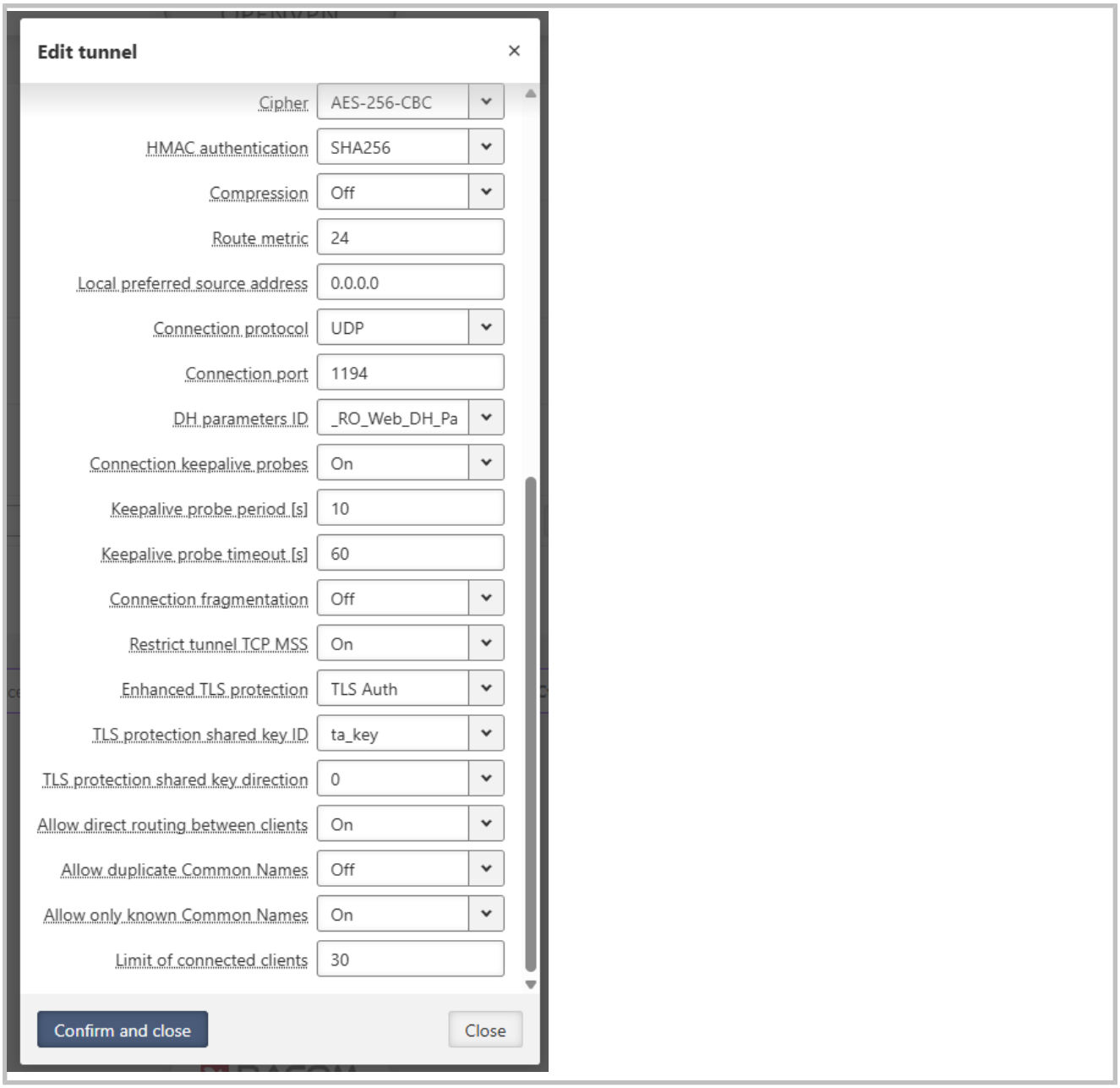


Fig. 7.28: OpenVPN Router tunnel settings

Enable tunnel

List box {Off; On}, default = "On"
Enables / disables OpenVPN tunnel.

Tunnel type

List box {Bridge, Router}, default = "Router"
Tunnel interface type selection.
Bridge: L2 interface (TAP) without its own address, connects as a port into a bridge (from Ethernet interfaces table).
Router: L3 interface (TUN) with its own IP address, routed using routing rules.

Tunnel MTU [B]

Number {100 – 1500}, default = "1500"
MTU size on the tunnel interface.

Must be consistent on all ends (server and all clients). The server can override client settings, but correct MTU setup on clients is important for consistency.

Network interface

List box {user defined bridge IDs}, default = "bridge"
Select your bridge interface. Your tunnel connects as a port into this bridge from your LAN interfaces table.
Only in Bridge (TAP)

Allow unit management

List box {On, Off}, default = "On"
Permit administration access to your station through your tunnel interface.
Only in Router (TUN)

Tunnel network address/mask

IP address and mask [16 - 29], default = "0.0.0.0/24"
Defines your address range on the tunnel interface. Your server receives the first unicast address in this range. The system assigns addresses from this range to your clients and sends the same mask for subnet topology.
Only in Router (TUN)

Assign dynamic client addresses

List box {On, Off}, default = "Off"
Turns on dynamic address allocation for your clients without a static address. Your server attempts to maintain persistent address allocation for your client via the Common Name on their certificate.
Only in Router (TUN)

Dynamic client address range - start

IP address, default = "0.0.0.100"
Defines your IP address range start for dynamic client allocation. This address must fall within your Tunnel network address/mask range. This start address must be less than or equal to your end address.
Only in Router (TUN)

Dynamic client address range - end

IP address, default = "0.0.0.200"
Defines your IP address range end for dynamic client allocation. This address must fall within your Tunnel network address/mask range. This end address must be greater than or equal to your start address.
Only in Router (TUN)

Network topology

List box {Subnet, Net30}, default = "Subnet"
Selects your network topology for address distribution.
Subnet: Assigns one address from the range to your clients and server.
Net30: Provides backward compatibility. Assigns a /30 subrange of 4 addresses to each participant. The two middle unicast addresses serve as the local and peer tunnel addresses.
Only in Router (TUN)

Allow legacy certificates

List box {On, Off}, default = "Off"
Allows certificates signed with weak algorithms like SHA1. OpenVPN rejects these certificates by default. Using weak signature certificates compromises your network security.

Private key ID
Keyring identifier
Choose your instance private key. The key must exist in your keyring with the Certificate key (PRI).

Certificate ID
Keyring identifier
Choose your instance certificate. The key must exist in your keyring with the Certificate (PUB). The fingerprint of the contained public key must match its private key.

CA certificate ID
Keyring identifier
Choose your Certificate Authority certificate. The key must exist in your keyring with the Certificate (PUB) or CA chain (PUB). This authority signs all participant certificates.

Verify peer certificate usage
List box {On, Off}, default = "On"
Strictly check the Extended Key Usage attribute on peer certificates. This prevents your clients from impersonating your server. Clients check server certificates for TLS Web Server Authentication. Servers check client certificates for TLS Web Client Authentication.

Cipher key renegotiation period [s]
Number [60, 86400], default = "3600"
Sets your data encryption key renegotiation period in seconds. The system uses the shorter period if your client and server settings differ. The system accepts the expired key for an equal duration from the start of renegotiation to maintain smooth traffic.

Cipher
List box {Default, AES-128-CBC, AES-128-CFB, AES-128-CFB1, AES-128-CFB8, AES-128-GCM, AES-128-OFB, AES-192-CBC, AES-192-CFB, AES-192-CFB1, AES-192-CFB8, AES-192-GCM, AES-192-OFB, AES-256-CBC, AES-256-CFB, AES-256-CFB1, AES-256-CFB8, AES-256-GCM, AES-256-OFB, ARIA-128-CBC, ARIA-128-CFB, ARIA-128-CFB1, ARIA-128-CFB8, ARIA-128-GCM, ARIA-128-OFB, ARIA-192-CBC, ARIA-192-CFB, ARIA-192-CFB1, ARIA-192-CFB8, ARIA-192-GCM, ARIA-192-OFB, ARIA-256-CBC, ARIA-256-CFB, ARIA-256-CFB1, ARIA-256-CFB8, ARIA-256-GCM, ARIA-256-OFB, CAMELLIA-128-CBC, CAMELLIA-128-CFB, CAMELLIA-128-CFB1, CAMELLIA-128-CFB8, CAMELLIA-128-OFB, CAMELLIA-192-CBC, CAMELLIA-192-CFB, CAMELLIA-192-CFB1, CAMELLIA-192-CFB8, CAMELLIA-192-OFB, CAMELLIA-256-CBC, CAMELLIA-256-CFB, CAMELLIA-256-CFB1, CAMELLIA-256-CFB8, CAMELLIA-256-OFB, CHACHA20-POLY1305, SM4-CBC, SM4-CFB, SM4-OFB, DES-EDE-CBC (legacy), DES-EDE-CFB (legacy), DES-EDE-OFB (legacy), DES-EDE3-CBC (legacy), DES-EDE3-CFB (legacy), DES-EDE3-CFB1 (legacy), DES-EDE3-CFB8 (legacy), DES-EDE3-OFB (legacy)}, default = "Default"
Selects your ciphers offered to the peer. Default uses the AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305 cipher list. The system uses the first cipher offered by both sides. Connections to older OpenVPN versions use a fallback setting of one algorithm matching the selected cipher. Default uses AES-256-GCM for fallback.

HMAC authentication
List box {MD5, MD5-SHA1, RIPEMD160, SM3, SHA1, SHA224, SHA256, SHA384, SHA512-224, SHA512-256, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, BLAKE2s256, BLAKE2b512}, default = "SHA1"
Selects your hash algorithm for HMAC authentication on data packets. This applies to the encrypt-then-mac method and TLS Auth. The system applies the internal MAC algorithm instead if you use a GCM cipher.

Compression
List box {Off, On, Asymmetric}, default = "Off"
Sets your data compression. Using compression compromises data security by allowing encryption breaking. Keep compression turned off. On enables two-way compression. Asymmetric accepts compressed packets but sends uncompressed packets. Set compression consistently across all participants. The migrate algorithm is an exception.

Compression algorithm
List box {LZO, LZ4, LZ4v2, Migrate}, default = "LZO"
Selects your compression algorithm. Your server overrides your client settings after login.
LZO: Use this older algorithm for backward compatibility.
LZ4: Use this newer, efficient algorithm.
LZ4v2: Use this LZ4 variant to send uncompressible data without compression.
Migrate: Use this option for your server during network migration from compression. Your server accepts client connections with or without compression. Your server forces an empty compression algorithm on clients connecting with compression. Your client treats this state as enabled compression with an empty algorithm.

Route metric
Number [0, 4294967294], default = "24"
Sets the metric for your routing rules added by OpenVPN.

Local preferred source address
IP address, default = "0.0.0.0"
Specifies your preferred source address for routing rules added by OpenVPN. Use one of the local addresses on your active device interfaces. The 0.0.0.0 option uses the address assigned to this OpenVPN tunnel.

Connection protocol
List box {UDP, TCP}, default = "UDP"
Selects your client and server communication protocol. TCP causes issues on lossy or congested links. TCP adds higher overhead. TCP over TCP causes inappropriate interactions.

Connection port
Number [1, 65535], default = "1194"
Sets the port where your server listens to clients.

DH parameters ID
Keyring identifier
Selects your Diffie-Hellman parameters for client and server key exchange. The key must exist in your keyring with the DH Parameters (PUB) type.

Connection keepalive probes
List box {On, Off}, default = "On"
Turns on connection maintenance. The server transfers this setting to the client after connection. Participants send packets to each other at the prescribed period. The system drops the connection if the timeout elapses without a received packet. The client attempts to reconnect.

Keepalive probe period [s]
Number [10, 3600], default = "10"
Sets your period in seconds for sending keepalive packets.

Keepalive probe timeout [s]
Number [30, 14400], default = "60"

Sets your timeout in seconds for waiting for a keepalive packet.

Connection fragmentation
List box {On, Off}, default = "Off"
Enables internal data fragmentation. This adds a small overhead but helps resolve MTU (Maximum Transmission Unit) issues on the network path.
Important: This setting must be enabled on all participants in the connection.

Fragment size [B]
Number [70, 1500], default = "1300"
Sets the maximum UDP packet size for internal fragmentation.
Guideline: Ensure the fragment size fits within your tunnel MTU. The internal limit is 32 fragments per packet. When calculating, account for approximately 58 bytes of OpenVPN overhead.

Restrict tunnel TCP MSS
List box {On, Off}, default = "On"
Enables TCP Maximum Segment Size (MSS) rewriting for packets carried inside the tunnel.
Benefit: This prevents TCP sessions from sending packets that would require IP fragmentation, improving performance and reliability.

Enhanced TLS protection
List box {Off, TLS Auth, TLS Crypt}, default = "Off"
Turns on additional protection for your OpenVPN control packets.
Off: Provides no additional protection.
TLS Auth: Adds authentication to control packets using a shared key. This prevents port scanning, UDP floods, and DoS attacks.
TLS Crypt: Adds authentication and encryption to control packets using a shared key. This provides TLS Auth protection and prevents control packet inspection, certificate attribute eavesdropping, and OpenVPN presence detection.

TLS protection shared key ID
Keyring identifier
Select your shared key for additional control packet protection. The key must exist in your keyring with the OpenVPN TLS protection key (PRI) type. Match this key across all participants.

TLS protection shared key direction
List box {0, 1}, default = "0"
Specifies your key direction component for TLS Auth authentication on the server. Set this to the opposite value on your client.

Allow direct routing between clients
List box {On, Off}, default = "On"
Turns on internal routing between your server clients. Your server forwards packets between clients internally without exiting the tunnel. Turning this off forces all client packets to exit the tunnel. Kernel routing rules take over and route packets back into the tunnel. This causes ICMP REDIRECT packets sent to your source client.

Allow duplicate Common Names
List box {On, Off}, default = "Off"
Permits simultaneous connections from multiple clients using the same Common Name attribute in their certificate.

Allow only known Common Names
List box {On, Off}, default = "On"

Rejects connections from clients without a Common Name listed in your OpenVPN client table for this server. Turn on dynamic address allocation if you allow unlisted clients and use Router mode. Otherwise, unlisted clients receive no address.

Limit of connected clients

Number [1, 30], default = "30"

Sets your maximum number of concurrent connected clients. Keep the sum of maximum connected clients across all your active servers under 30.

7.4.3.2. Clients

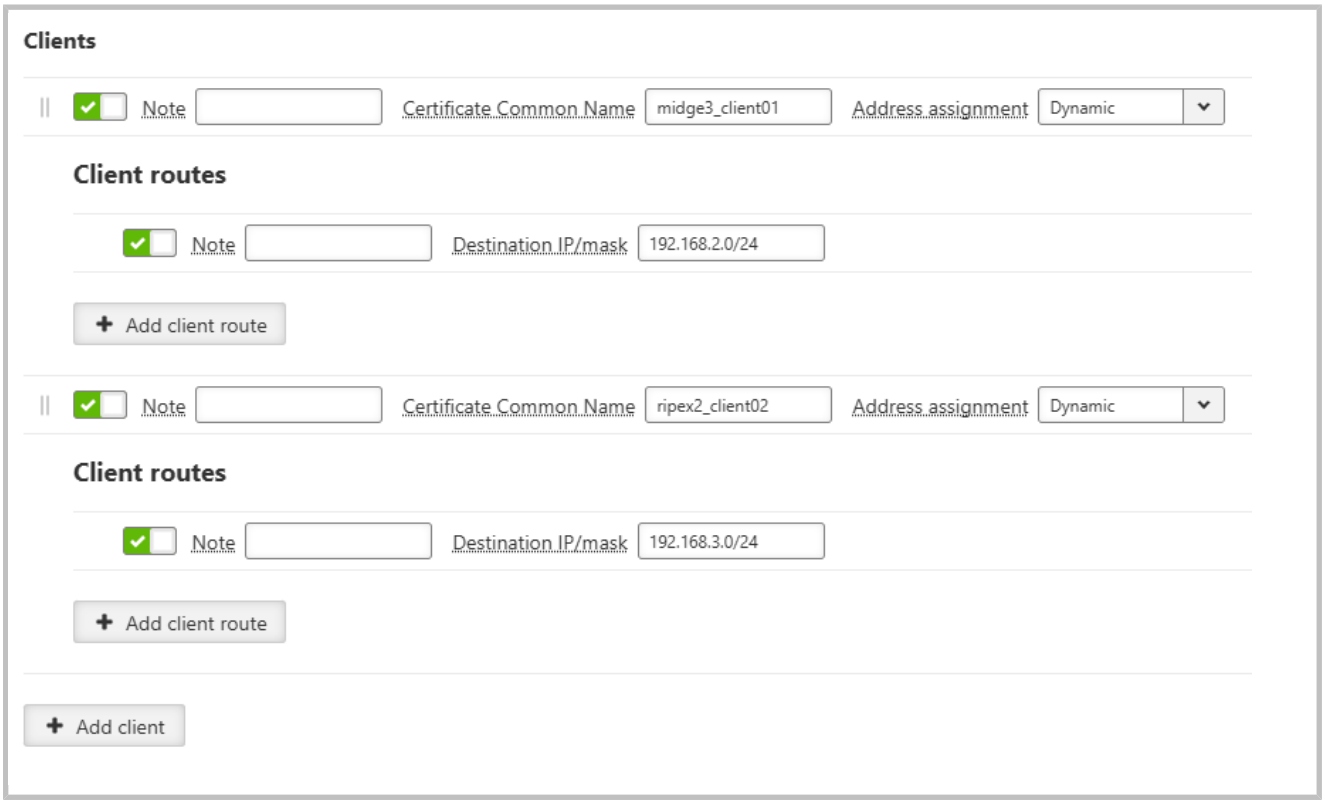


Fig. 7.29: OpenVPN Clients settings

Clients:

Enable client

Checkbox {On, Off}, default = "On"

Activate your client configuration. Deactivate the checkbox to turn off your client instance.

Note

Text input

Add a custom description for your client.

Certificate Common Name

Text input

Enter the Common Name attribute from your client certificate. The system uses this attribute to identify your client. OpenVPN replaces unsupported characters with an underscore.

Address assignment

List box {Dynamic, Static}, default = "Dynamic"

Select your tunnel address allocation method for your client. Dynamic assignment requires an active dynamic client address setting on your server.

Assigned address
IP address, default = "0.0.0.0"
Assign a specific IP address to your client. Apply this setting when your server operates in Router mode. Prevent IP address conflicts with other clients and your dynamic address pool.

Client routes:

Enable route
Checkbox {On, Off}, default = "On"
Activate your client routing rule. Deactivate the checkbox to turn off your route.

Note
Text input
Add a custom description for your client route.

Destination IP/mask
IP address and mask, default = "0.0.0.0/0"
Define the destination network range for your packets. Prevent address conflicts with other active client routes. Your server uses this rule to direct traffic to your client and its subnets. Your server exports this route to other connected clients to enable direct client-to-client communication.

7.4.3.3. Server routes



Fig. 7.30: OpenVPN Server routes settings

Enable route
Checkbox {On, Off}, default = "On"
Activate your server routing rule. Deactivate the checkbox to turn off your route.

Note
Text input
Add a custom description for your server route.

Destination IP/mask
IP address and mask, default = "0.0.0.0/0"
Define the destination network range for your packets. Your server exports this rule to connected clients. This rule directs traffic from your client to your server and its subnets. Prevent address conflicts with other active routes on the same server.

7.4.3.4. Servers

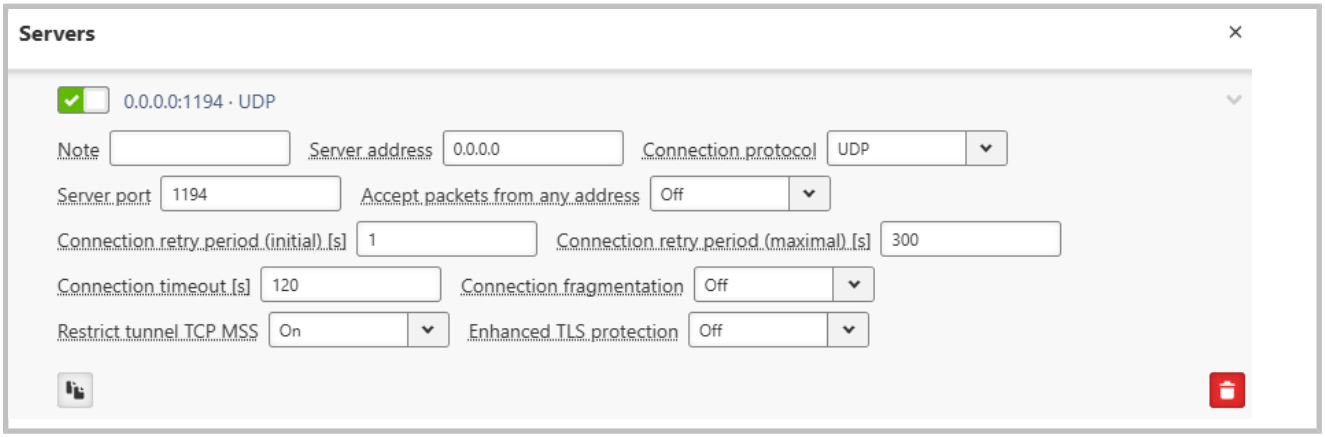


Fig. 7.31: OpenVPN Servers settings

Enable server
Checkbox {On, Off}, default = "On"
Activate your server connection profile. Deactivate the checkbox to turn off your profile.

Note
Text input
Add a custom description for your server profile.

Server address
IP address or hostname, default = "0.0.0.0"
Specify your OpenVPN server IP address or hostname. You must enable *DNS forwarding* on your device to use a hostname.

Connection protocol
List box {UDP, TCP}, default = "UDP"
Select your communication protocol with the server.

Server port
Number [1, 65535], default = "1194"
Specify the destination port where your server listens.

Accept packets from any address
List box {On, Off}, default = "Off"
Permit server packets arriving from varying source addresses. Use this setting when your server has a dynamic address or changes routing dynamically. Enable enhanced TLS protection alongside this setting.

Connection retry period (initial) [s]
Number [1, 60], default = "1"
Set your initial connection retry interval in seconds. The interval doubles every five failed attempts until it reaches the maximum retry period.

Connection retry period (maximal) [s]
Number [1, 600], default = "300"
Set your maximum connection retry interval in seconds.

Connection timeout [s]
Number [1, 3600], default = "120"
Set your connection timeout limit in seconds. The system measures this limit from the start of the connection attempt with this profile.

Connection fragmentation
List box {On, Off}, default = "Off"
Turn on internal data fragmentation between your participants.

Fragment size [B]
Number [70, 1500], default = "1300"
Set your maximum UDP packet size for internal fragmentation.

Restrict tunnel TCP MSS
List box {On, Off}, default = "On"
Turn on Maximum Segment Size rewriting in your TCP packets carried over the tunnel.

Enhanced TLS protection
List box {Off, TLS Auth, TLS Crypt}, default = "Off"
Turn on additional protection for your OpenVPN control packets.

TLS protection shared key ID
Keyring identifier
Select your shared key for additional control packet protection. The key must exist in your keyring with the OpenVPN TLS protection key (PRI) type. Match this key across all participants.

TLS protection shared key direction
List box {0, 1}, default = "1"
Specify your key direction component for TLS Auth authentication on the client. Set this to the opposite value on your server.

Note

OpenVPN has a very aggressive initialization process. It is not possible to operate OpenVPN within the Transparent protocol in Half duplex mode.

Dynamic routing protocols cannot be used over OpenVPN L3 due to static internal routing in the server. Additionally, for Babel, the server does not route IPv6 link addresses (dynamically assigned by the kernel) that it uses for its control packets. You need to use L2 variant, which is described in the *OpenVPN application note*[6].

Warning

Attention is required to prevent routing loops, where traffic from the link between OpenVPN endpoints is directed back into the OpenVPN tunnel. Unlike IPsec, there is no protective mechanism against packet wrapping.

7.5. Security

User authentication is required to access RipEX2 unit management. There are two types of user authentication which differ in the user account location:

[6] https://www.racom.eu/eng/products/m/ripex/app/openvpn/intr.html

Local authentication – user accounts are stored directly in the RipEX2 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, Radio, COM, Terminal servers, Cellular	Read-only	Write	Write	Write
		Radio - Encryption	Read-only	Read-only	Write	Write
	Routing	Static	Read-only	Write	Write	Write
		Babel, OSPF, BGP, Link management	Non-visible	Non-visible	Write	Write
	Firewall	L2, L3, NAT	Read-only	Write	Write	Write
	VPN	IPsec	Non-visible	Non-visible	Write	Write
		OpenVPN	Non-visible	Non-visible	Write	Write
		GRE	Read-only	Write	Write	Write
	Quality of service		Read-only	Write	Write	Write
	Security	Policy	Non-visible	Non-visible	Non-visible	Write
		Local authentication	Non-visible	Non-visible	Non-visible	Write
		Credentials	Non-visible	Non-visible	Non-visible	Write
		Management access	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. Policy

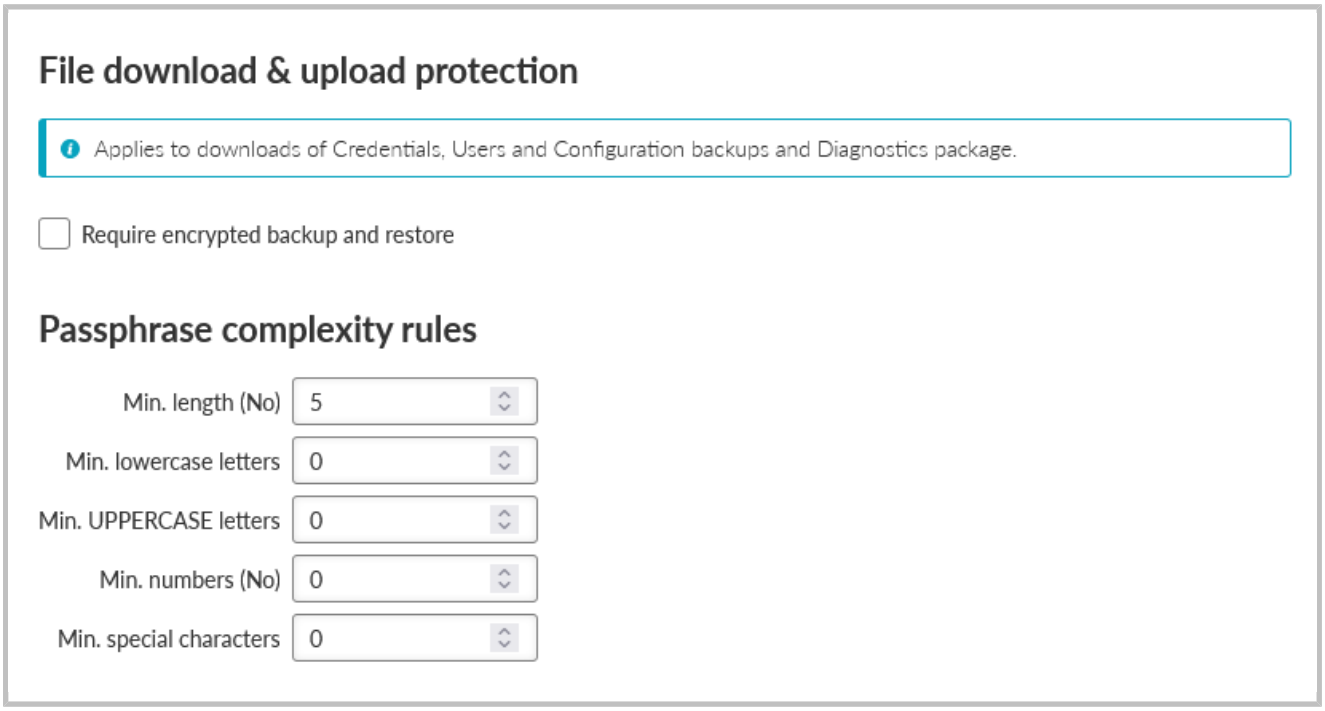


Fig. 7.32: SETTINGS > Security > Policy

Passphrase - Minimal length
Number {5 – 64}, default = 5
The minimum length of the passphrase.

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 passphrase.

Passphrase - Minimal number of uppercase characters
Number {0 – 5}, default = 0
The minimum number of uppercase letters (English letters) which are required in the passphrase.

Passphrase - Minimal number of digits
Number {0 – 5}, default = 0
The minimum number of number characters (0 to 9) which are required in the passphrase.

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 passphrase. Non-English letters (like Greek, Russian, Arabic) are counted as special characters.

This setting applies to the download of Credentials, Users, Configuration backups, and Diagnostics packages. The **Require encrypted backup and restore** parameter enforces the use of encrypted files for all users. The following parameters allow you to define passphrase complexity rules for encryption.

7.5.2. Local authentication

7.5.2.1. User Accounts

The following settings are available only for user with the Administrator role.

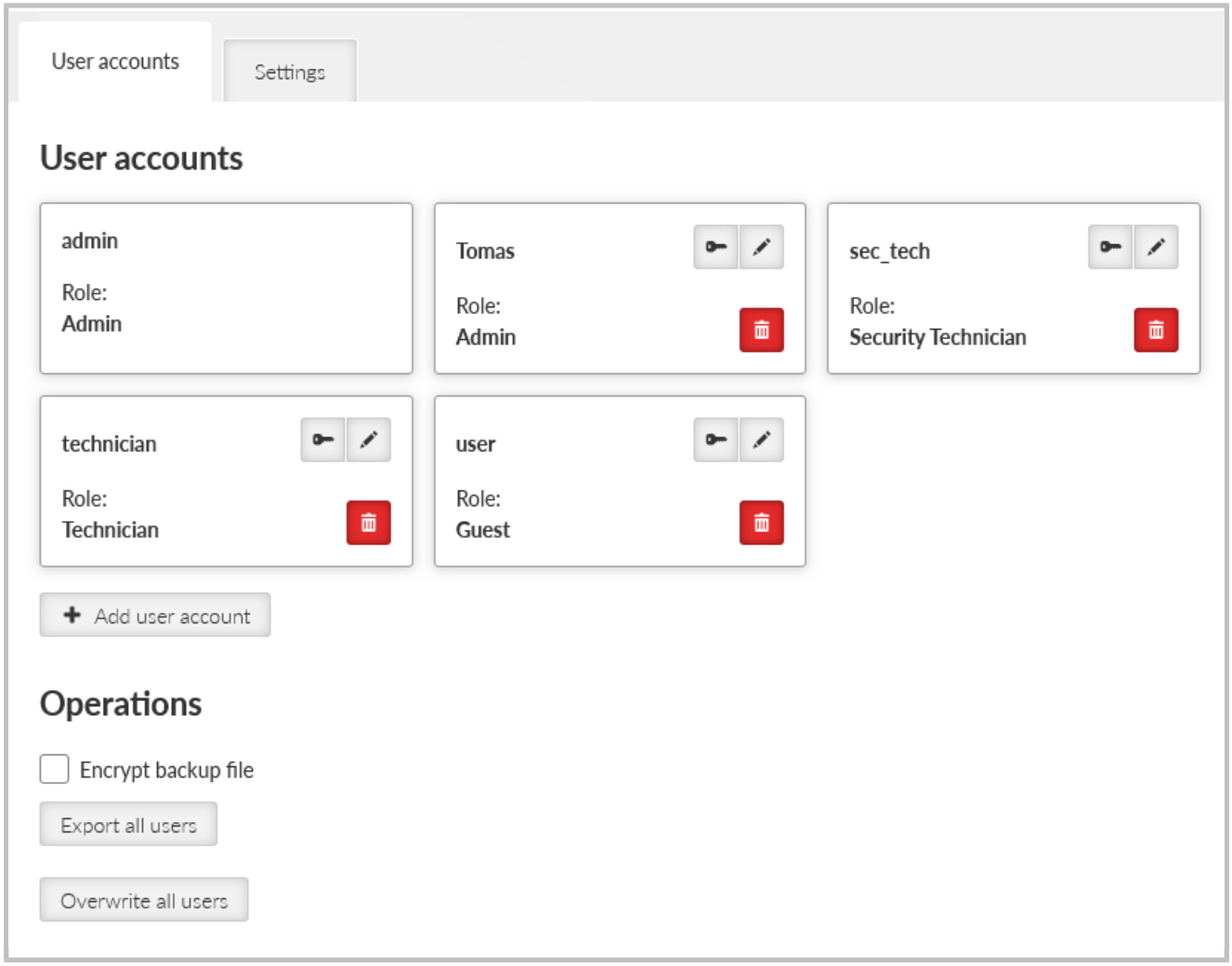


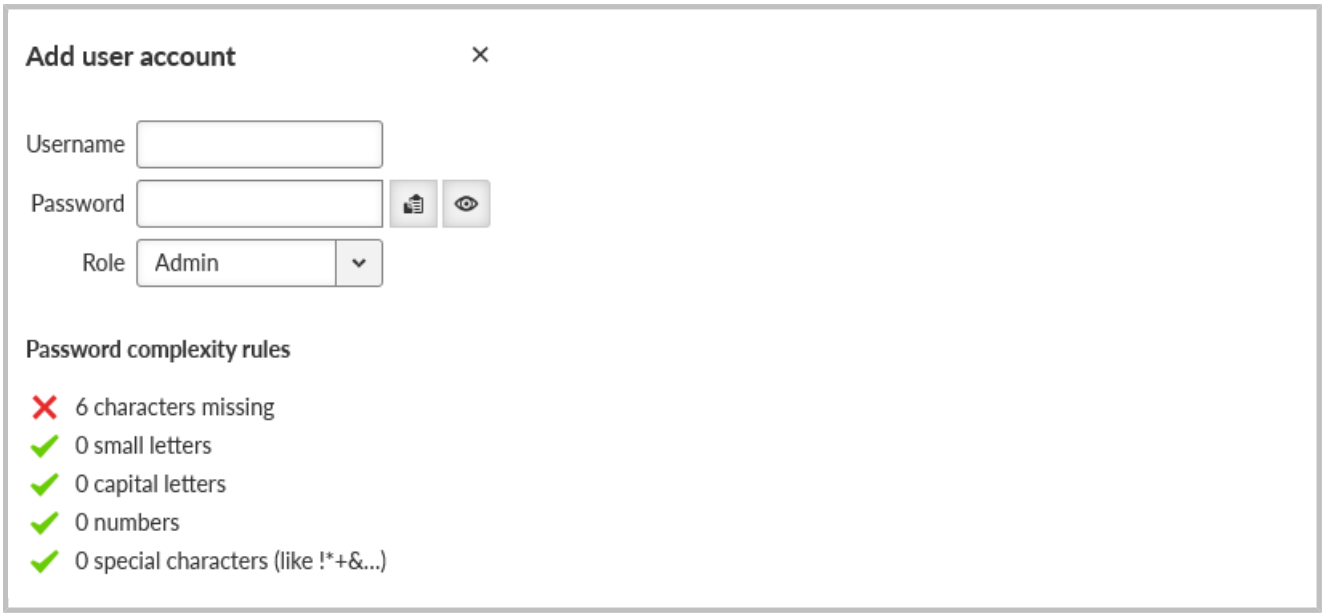
Fig. 7.33: SETTINGS > Security > Local authentication

Following user account parameters can be changed: password, user role. Any account (expect 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:



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.

Export all users

The exported user accounts are stored in a text file (.json file type) or in an encrypted .zip file. The rules for encryption (forced requirement and password complexity) shall be set in SETTINGS > Security > Policy see section 7.5.1 Policy.

Overwrite all users

All existing current users will be deleted and replaced by users stored in imported file. You will be logged off after the import and you have to log in using the imported user 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**).

Note

It is necessary to install firmware version 1.4.5.0 or higher to assure proper functionality of Local and Remote authentication.

7.5.2.2. Settings

Allows to set password complexity rules.

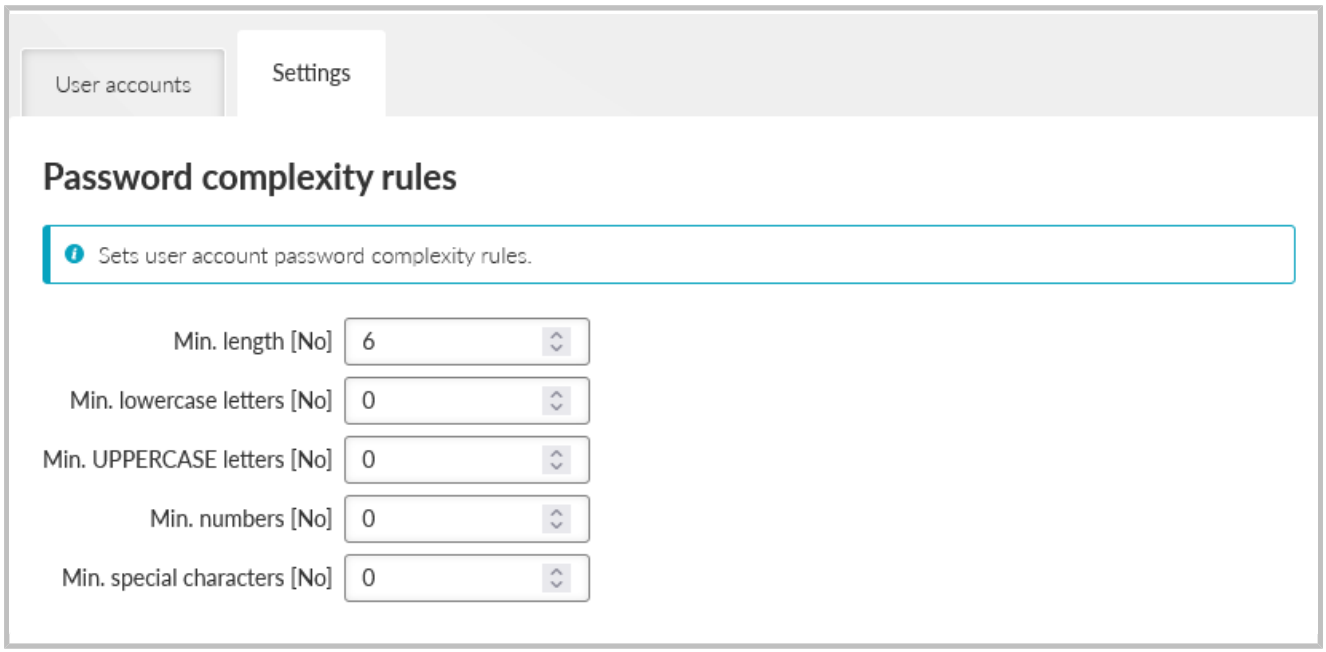


Fig. 7.34: SETTINGS > Security > Local authentication > Settings

Min. length [No]
Number {8 – 64}, default = 8
The minimum length of the password for all users.

Min. lowercase letters [No]
Number {0 – 5}, default = 1
The minimum number of lowercase letters (English letters) which are required in the user password.

Min. UPPERCASE letters [No]
Number {0 – 5}, default = 1
The minimum number of uppercase letters (English letters) which are required in the user password.

Min. numbers [No]
Number {0 – 5}, default = 1
The minimum number of number characters (0 to 9) which are required in the user password.

Min. special characters [No]
Number {0 – 5}, default = 1
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

RipEX2 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. The rules for encryption (forced requirement and password complexity) shall be set in SETTINGS > Security > Policy see section *7.5.1 Policy*.

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 credential” and “Add credential” 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. 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. Management access

7.5.4.1. Administration website

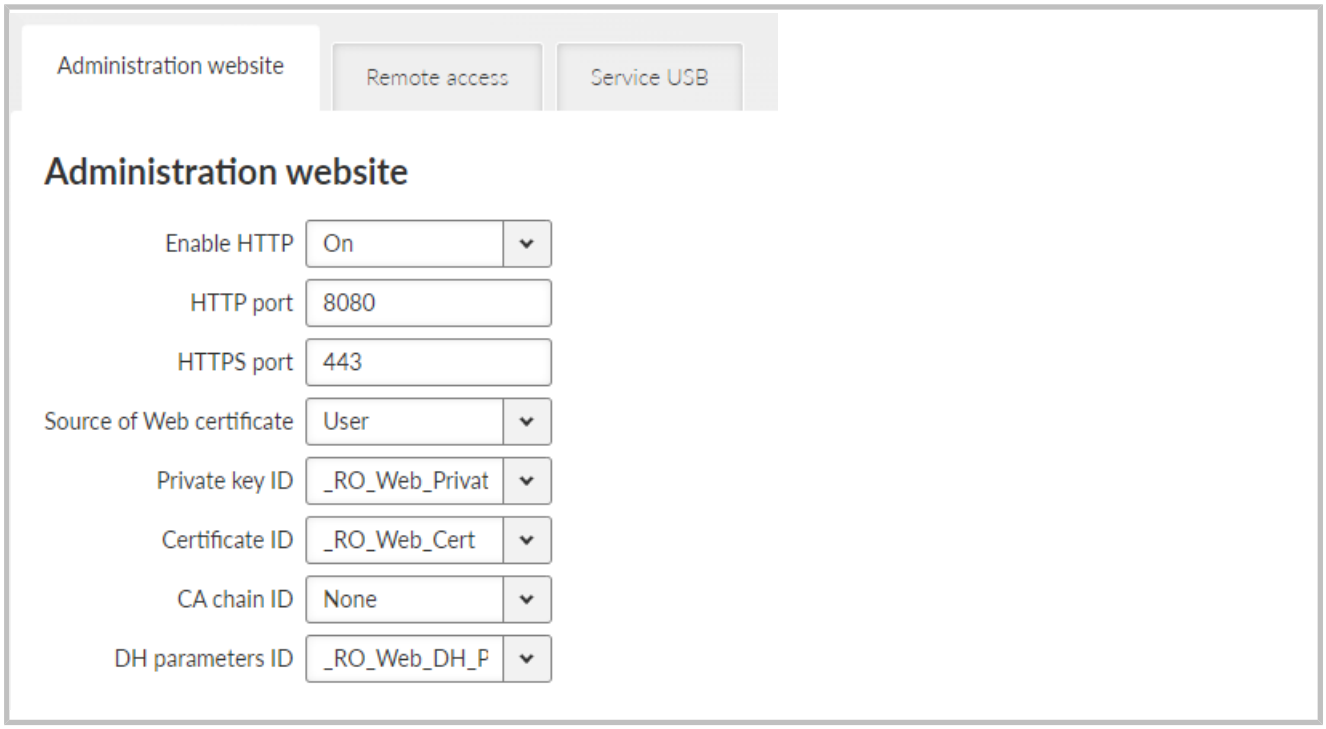


Fig. 7.35: SETTINGS > Security > Management access > Administration website

Enable HTTP — List box {On; Off}, default = "On"

Enables HTTP access to the station. When enabled, HTTP immediately redirects to HTTPS.

HTTP port — Number {1 – 65535}, default = 80

The TCP port number on which HTTP access is available.

HTTPS port Number {1 – 65535}, default = 443

The TCP port number on which HTTPS access is available.

Source of Web certificate

List box {Default; User}, default = "Default"

Choses source of Web server certificate. "Default" uses key, certificate and DH parameter distributed in FW (see SETTINGS > Security > Credentials), default values are as follows:

- Private key: _RO_Web_Private_Key
- Certificate : _RO_Web_Cert
- CA chain: _RO_Web_CA_Chain": CA chain, of the CA which signed the certificate. For self-signed certificate shall remain empty - None).
- DH parameters: _RO_Web_DH_Param

Web inactivity timeout [min] Number {5 – 2880}, default = 1440

When the inactivity timeout is reached, the HTTPS session terminates.

Available in ADVANCED > Security > Management access menu.

“User” allows to use user key and certificate included in the Credentials storage. Add your certificate and other files using menu SETTINGS > Security > Credentials. In the individual list boxes will be shown available certificate of keys for each category and you can choose those previously added.

7.5.4.2. Remote access

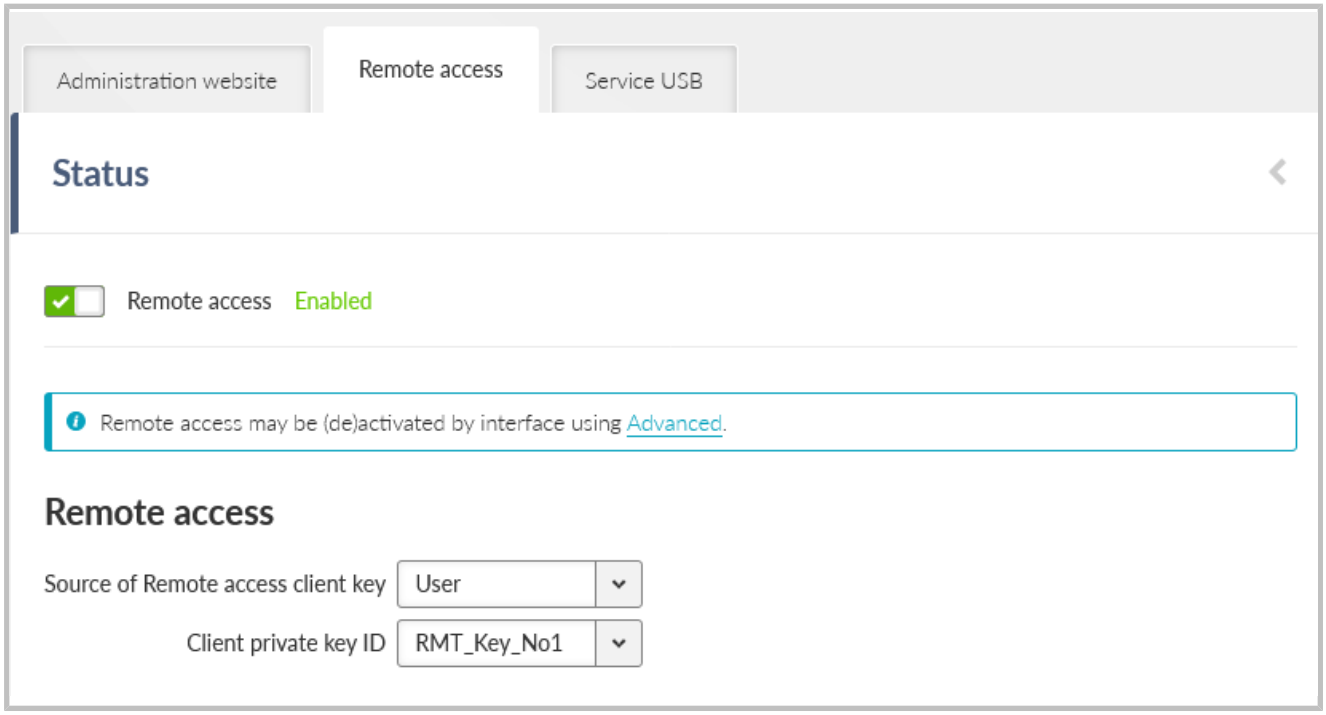


Fig. 7.36: SETTINGS > Security > Management access > Remote access

Enable/Disable
If enabled, allows the unit to be accessed via the Remote access feature.

Note
Remote access is enabled or disabled globally in this menu. Individual settings for each interface are available in the ADVANCED menu. By default, Radio and Ethernet interfaces are enabled, while all other interfaces are disabled. The current settings are displayed in the Status area.

Source of Remote access client key
List box {Default; User}, default = "Default"

Client private key ID
When the User in list box above is chosen, then you cab select a key previously downloaded to the Credentials storage (SETTINGS > Security > Credentials) or or generated in the same menu. The Remote access key has to be the same for the whole network (or the part of it for which you will use the Remote access). The remote access to the unit with different Remote access key is not possible.

Note

The use of a dedicated **Client private key** is highly recommended.

7.5.4.3. Service USB

The USB service interface primary purpose is to provide unit service and management access. Ethernet or Wi-Fi connection can be established using an external ETH/USB or Wi-Fi adapter.

Only adapters supplied with the product can be used for this purpose.

See *list of available adapters*[7].

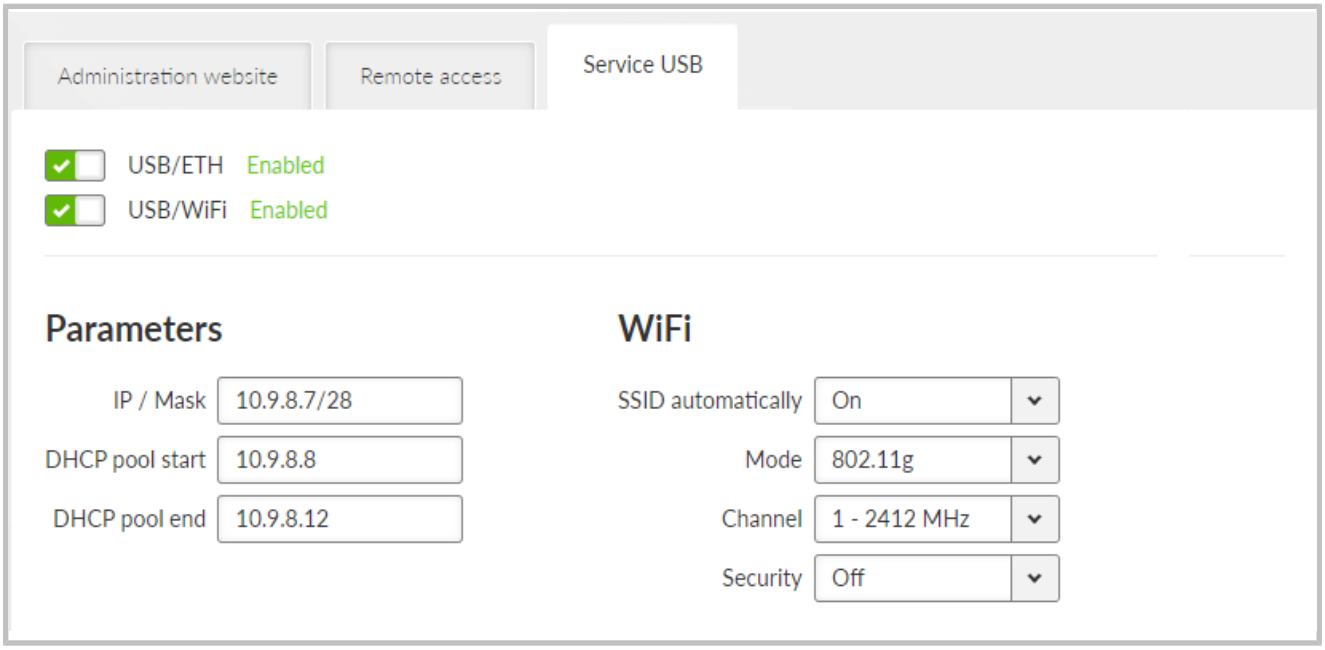


Fig. 7.37: SETTINGS > Security > Management access > Service USB

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 Wi-Fi service can be enabled or disabled separately. When the Wi-Fi is enabled, the unit acts as a Wi-Fi 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).

Wi-Fi
Wi-Fi 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
Wi-Fi AP SSID. When entered manually, it must follow SSID naming conventions.

[7] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb

Mode
List box {802.11g; 802.11g }, default = "802.11g "
Wi-Fi AP mode.

Channel
Selected Wi-Fi 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 Wi-Fi adapter installation.

7.5.5. RADIUS

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 RipEX2 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.



Fig. 7.38: SETTINGS > Security > 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 RipEX2 did not receive a valid reply.

Additional expert parameters shall be set in the ADVANCED menu.

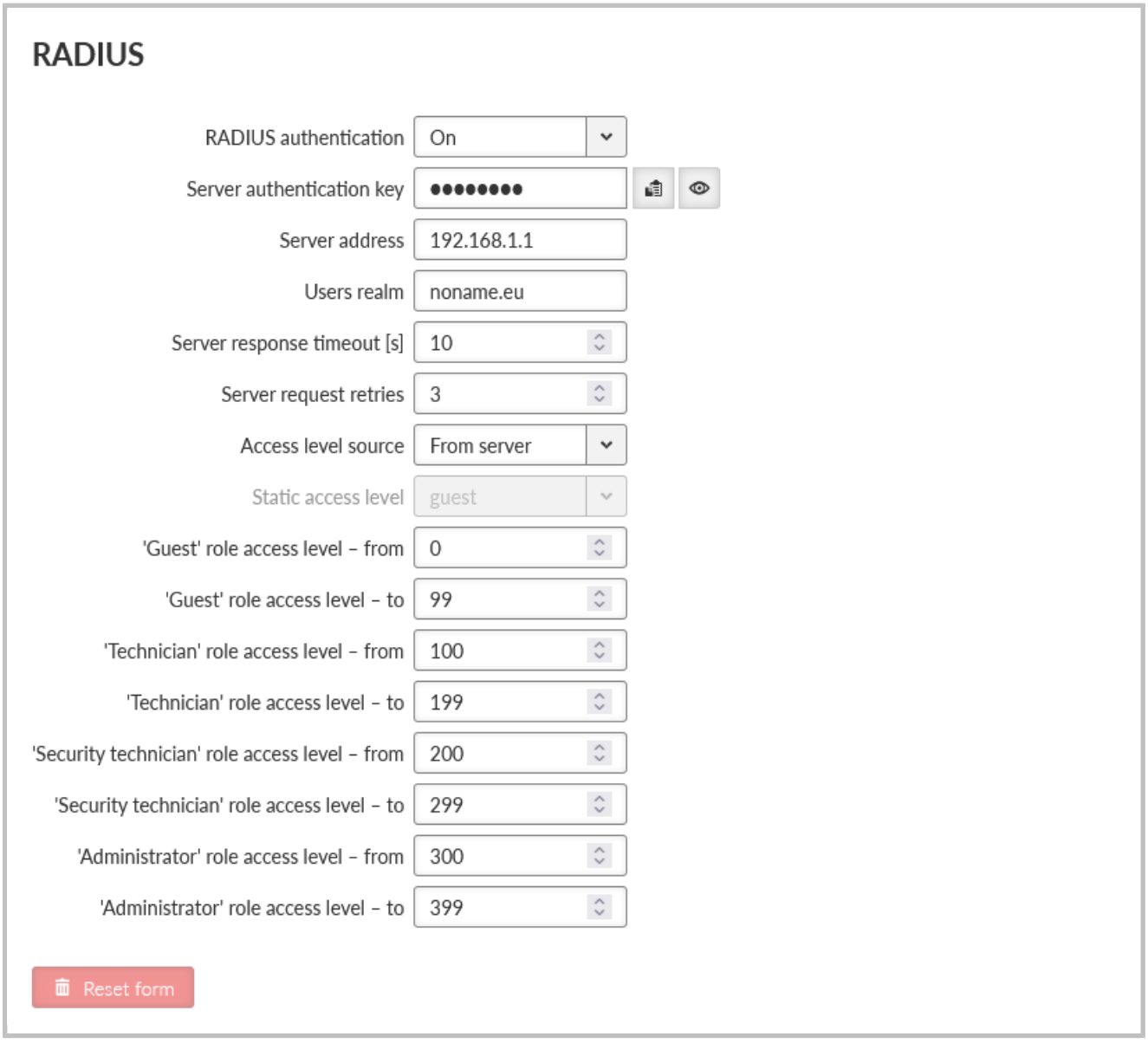


Fig. 7.39: ADVANCED > Security > RADIUS

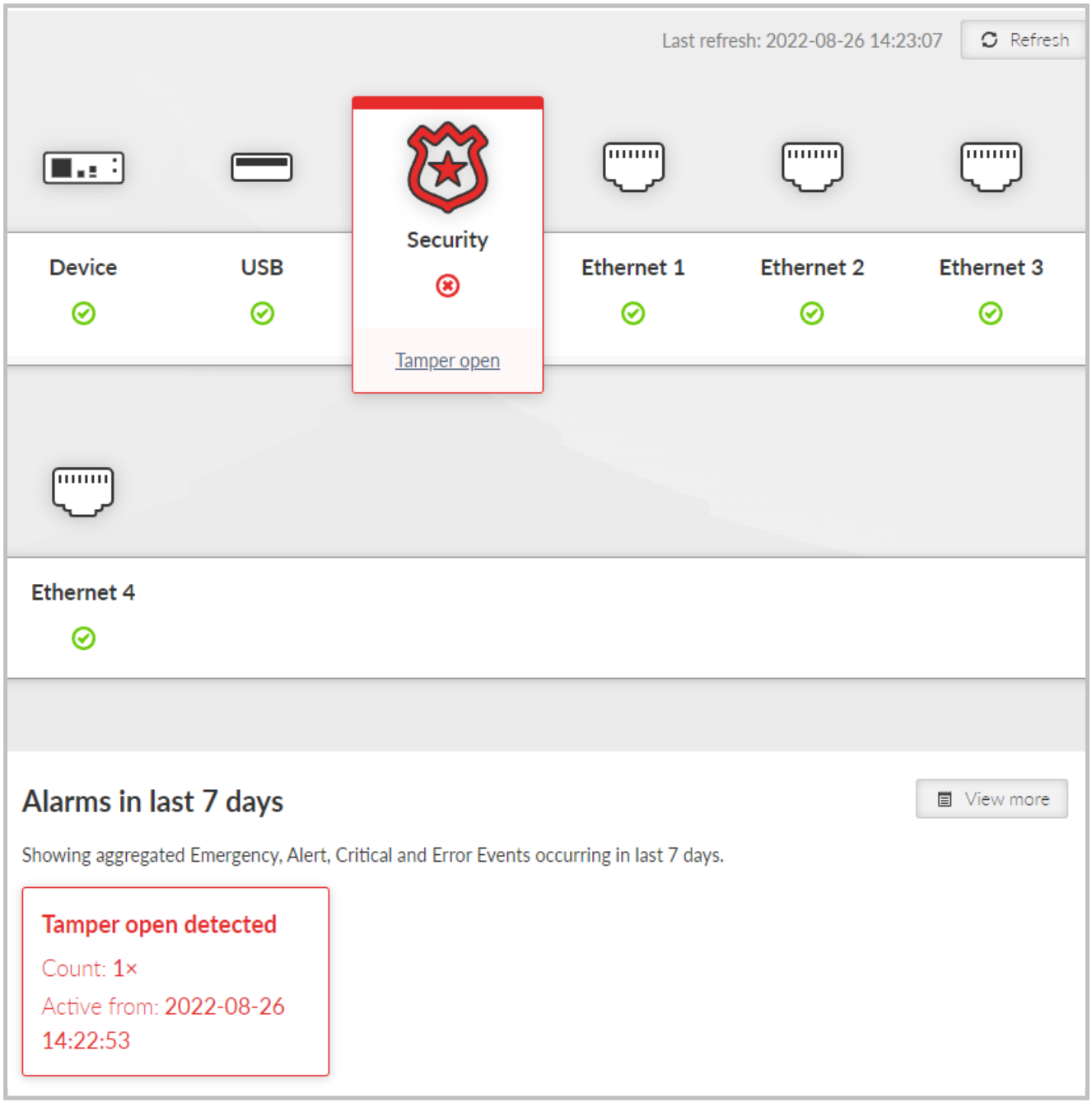
The level of access is realised by Management-Privilege-Level (RFC 5607, index 136, type integer). The level for each account shall be set during the server configuration. The user access level will be granted according to the integer ranges for individual role levels. When the server does not allow setting of Management-Privilege-Level the static account level option (for all users) has to be used.

7.5.6. Tamper reset

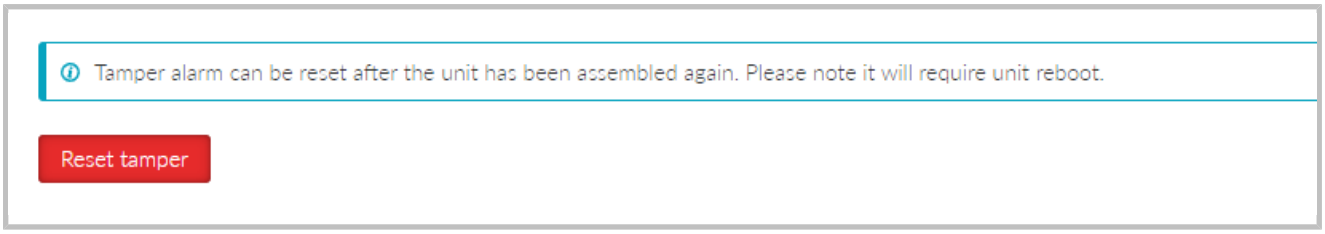
Tamper is a detection service, which is triggered, when the RipEX2 chassis is physically opened. There are 2 contacts (securing top and bottom casing) and the event is triggered even if the unit is without power. When the chassis is opened an alarm is triggered and shown in Status report. Triggered Tamper 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. See the STATUS menu:

Note

M!DGE3e has not the Tamper detection functionality.



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.



Note

The unit must be re-assembled before clicking the "Reset tamper" button, otherwise it returns an error.



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.

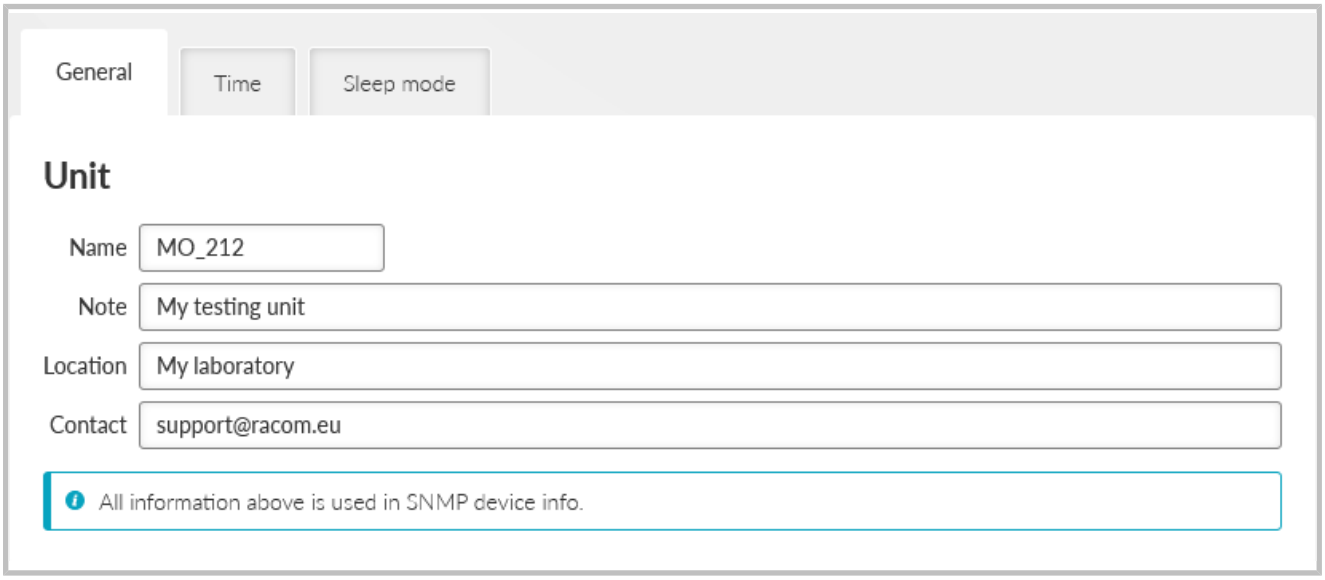


Fig. 7.40: SETTINGS > Device > Unit

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. 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.

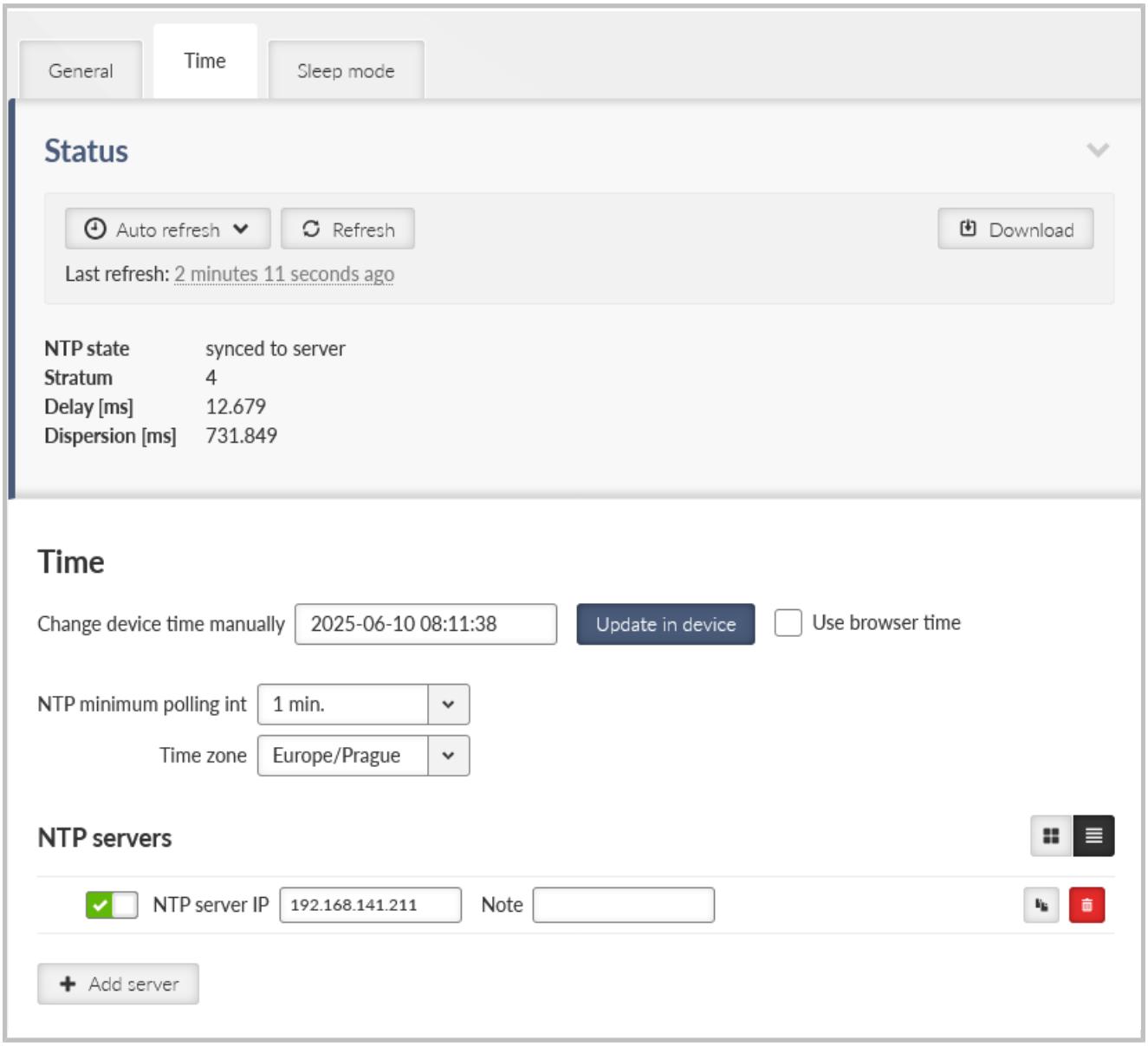


Fig. 7.41: SETTINGS > Device > Unit > Time

Status

The Status field provides information about NTP synchronization status.
Refresh button is used to update the Status information.

7.6.1.2.1. 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). Not only GNSS data, but also precise time pulses generated by the GNSS module are used for time synchronization. GNSS (GPS) synchronisation has priority over other NTP sources. This parameter occurs only if GNSS (GPS) is enabled in *Section 7.6.1.4, “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.

7.6.1.2.2. 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.

7.6.1.3. Sleep mode

RipEX2 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, RipEX2 has extremely low power consumption (10 mW). The time needed for a complete wake-up from the Sleep mode (booting time) is approx. 45 seconds or more - depending on the configuration. Sleeping unit indicates its state by green flashing SYS LED.

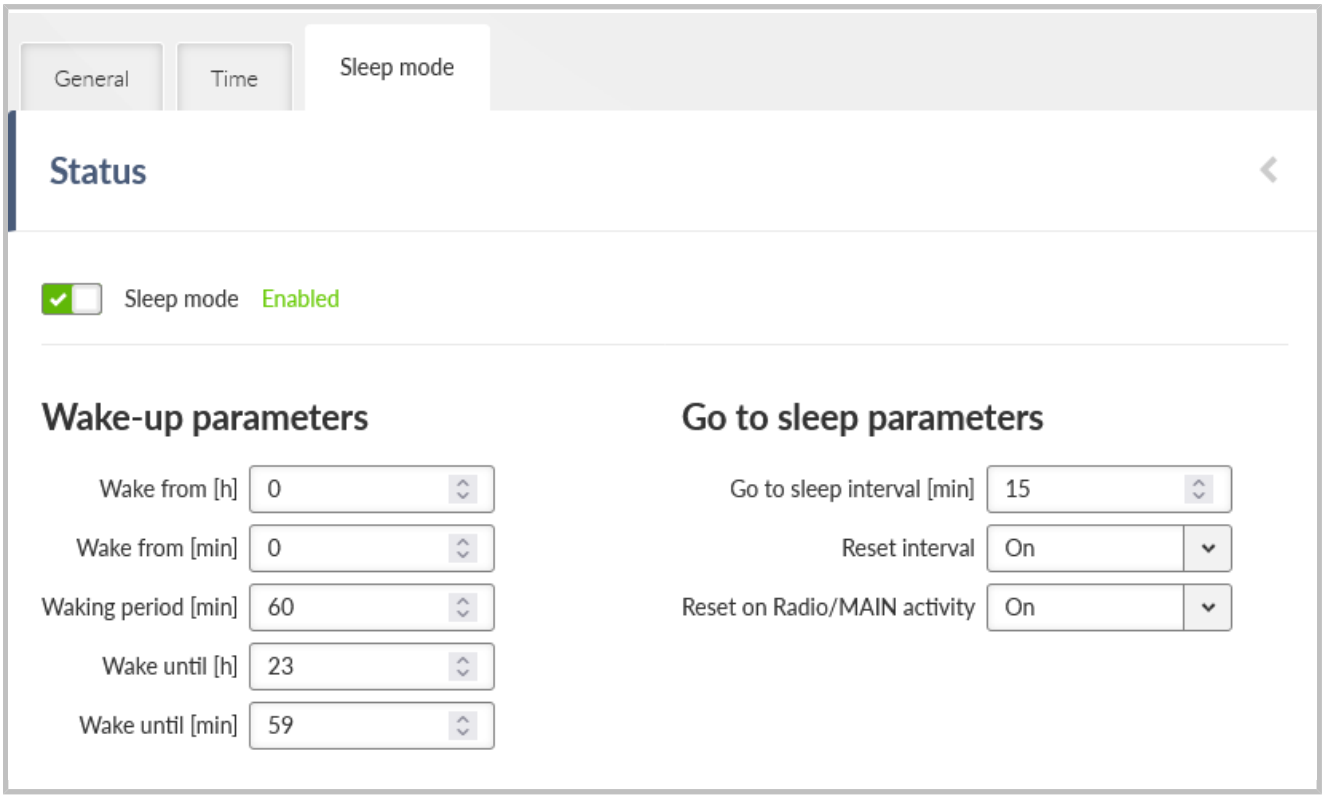


Fig. 7.42: SETTINGS > Device > Unit > Sleep mode

Sleep mode

Enable / disable, default = disable

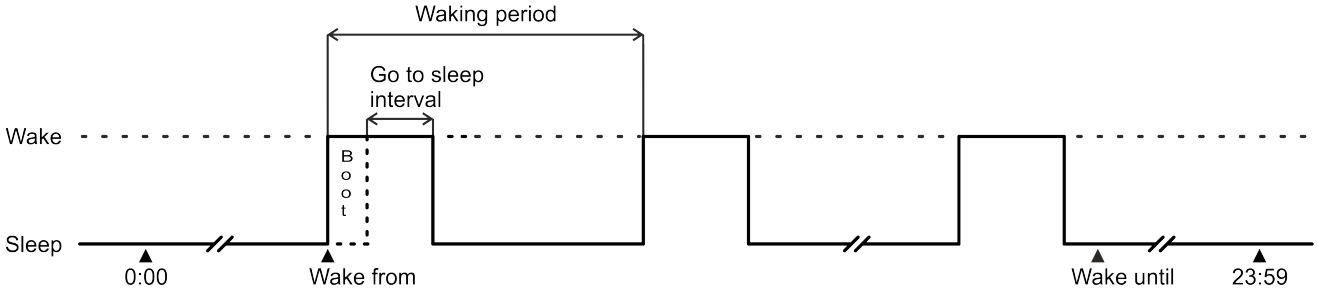
Enables / disables Sleep mode. When enabled, the unit will periodically go into Sleep mode depending on conditions defined by the following configuration.

Sleep mode cannot be used if:

- The unit is in Hot standby mode
- The unit's Radio protocol is set to Base driven (BDP) and the Station type is set to Base.

7.6.1.3.1. Wake-up parameters

Waking up the RipEX2 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).



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 awaken - hour.

Wake until [min]
Number {0 – 59}, default = 59
Defines the time in a day after which the unit will not be awaken - 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]**.

7.6.1.3.2. Go to sleep parameters

RipEX2 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-Wi-Fi 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 RipEX2 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 Radio or Cellular-MAIN interface, the count down timer is reset back to the initial value **Go to sleep interval [min]**.

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 RipEX2 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 RipEX2 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 RipEX2 stays awake in case of any radio or Cellular activity at the scheduled sleep time.

7.6.1.3.3. Wake up on Sleep Input (SI)

Sleep Input (SI) is a trigger signal that can be used to wake up a station from sleep.

SI is trigged/activated if it is pulled below 1.1 VDC. See more details in *Pin assignment*

If the RipEX2 is in the Sleep mode and SI is triggered, the unit will wake up for the set awake period and go back to sleep. The Sleep Input signal is not monitored while RipEX2 is awake so any additional SI trigger does not increase the awake period.

Example:

The unit is set to be waking up every hour for 10 minutes.
If a unit were to receive a SI command at 10:15 it will wake up and be awake until 10:25.
Unless another SI command is received after 10:25 the unit will stay asleep until 11:00

7.6.1.4. 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.

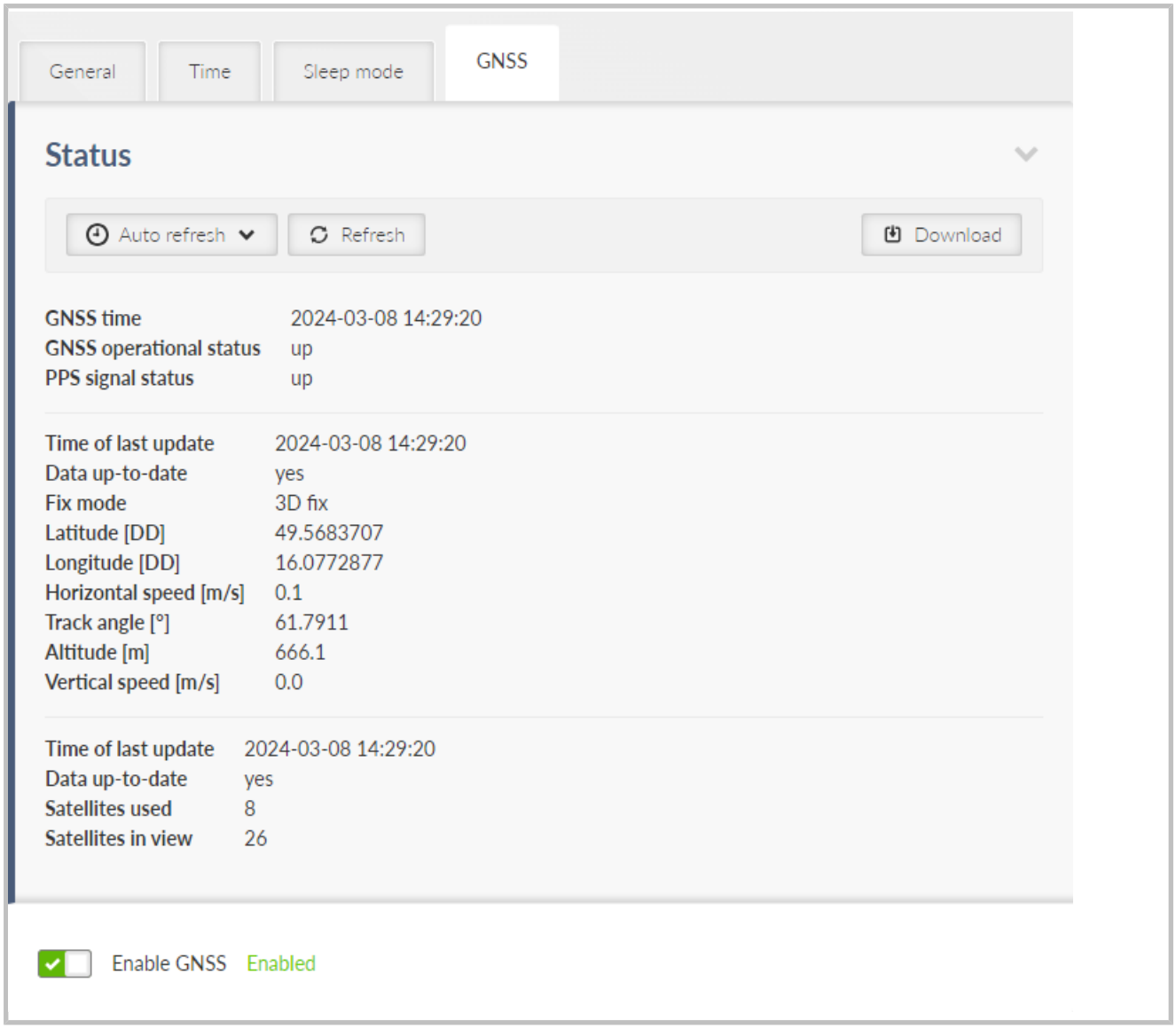


Fig. 7.43: SETTINGS > Device > Unit

Enable; Disable, default = "Disable"
Enables / Disables the GNSS (GPS).

To set up GNSS (GPS) see *Section 7.7.8, "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.

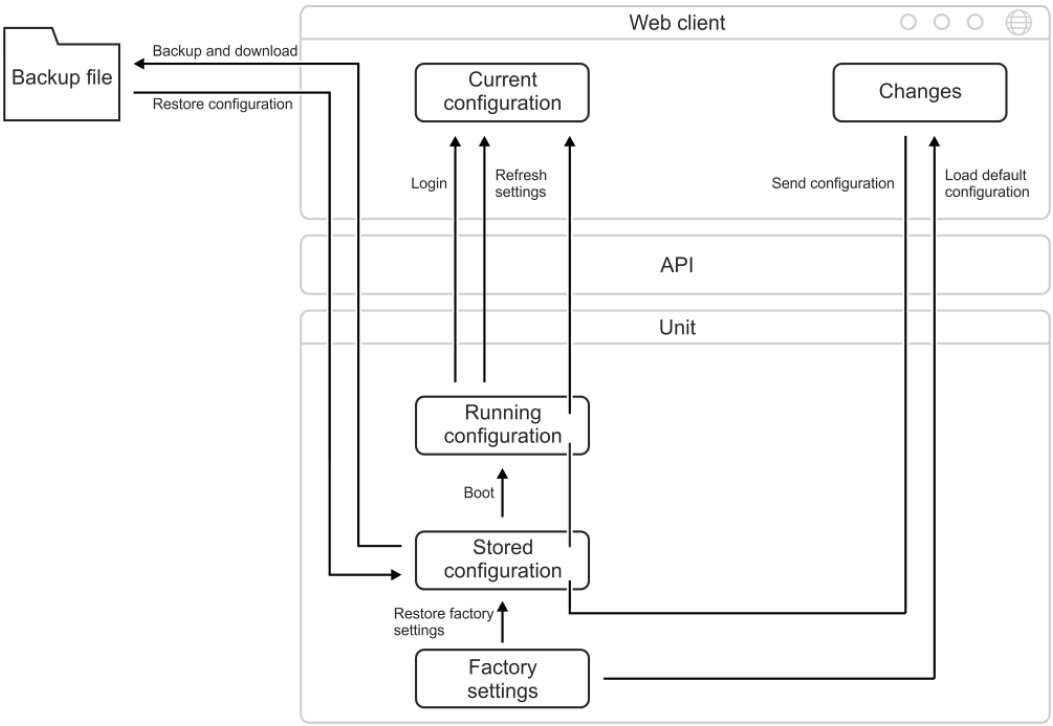
7.6.1.4.1. Cooperation with other services

- Hot standby - GNNS (GPS) is disconnected in passive mode and activated in active.

7.6.2. Configuration

Configuration in RipEX2 operates on following system:

- Current configuration - displayed configuration, which is seen in the web client.
- Running configuration - actual configuration, running in the RipEX2 unit.
- Stored configuration - configuration stored in the RipEX2 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"*.



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) or in an encrypted .zip file. The rules for encryption (forced requirement and password complexity) shall be set in SETTINGS > Security > Policy see section *7.5.1 Policy*.
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).

- The configuration data are valid only for the given configuration version (CNF version - see below). If the new firmware version brings the new configuration version, **the new configuration backup file needs to be downloaded after the firmware upgrade.**

Note
The current unit configuration (inside the running unit) is converted to a new version automatically during the firmware upgrade. No need to take care about that process.

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.

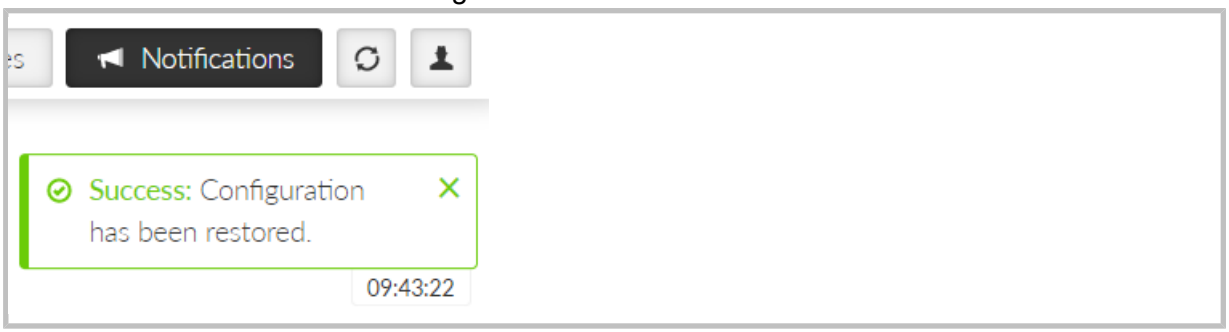
Factory settings

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.

Total purge

Restores all configuration parameters to default setup (including monitoring settings). Logout from station will apply.
Deletes user database.
Deletes all diagnostic logs and statistics.
Clears Radio Tx and antenna degradation detector calibration.

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.

Configuration validation

FW from version 2.2.0.0 introduces an improved configuration validation process. In older FW versions, some configuration item validations (e.g., allowed value range, string length) were validated only in the web application (front-end). When modifying the configuration in other ways (API calls, direct editing of the backup configuration file), it was possible to enter a value into a configuration item that caused the resulting unit configuration to be invalid. Recently, full configuration validation is performed directly in the unit (back-end). No method of configuration change (web interface, API, text backup modifications) can cause the unit to use an invalid configuration.

Notice for upgrading FW from older versions to version 2.2.0.0 and higher:
Units with FW older than 2.2.0.0 may have worked with a configuration that is not fully valid. Upon upgrading the unit to FW 2.2.0.0, or higher, a configuration validity check will be performed during startup the unit. If the configuration fails this check, the user will be informed by the generation of the system event "EVENT_CNF_BOOT_ERROR". The notification center will provide detailed alarm messages referencing individual invalid configuration items. However, the unit will continue to operate with this configuration as it did before the FW upgrade. The functions of the unit are not affected by this situation.

Consequences of running the unit with an invalid configuration:
The system event "EVENT_CNF_BOOT_ERROR" is active. The event has a default severity of Alarm, which causes the SYS status LED to light up red.

Until all items that failed the validation process are corrected, no configuration changes can be saved. The updated configuration can only be activated once the entire configuration successfully passes validation.

Tab. 7.4: Configuration versions

CNF version	FW version
31	2.3.6.0
30	2.3.4.0
29	2.2.9.0
28	2.2.6.0
27	2.2.4.0
26	2.2.2.0
25	2.2.1.0
24	2.2.0.0
23	2.1.7.0
22	2.1.6.0
21	2.1.2.0
20	2.1.1.0
19	2.1.0.0
18	2.0.18.0
17	2.0.16.0
16	2.0.14.0
15	2.0.13.0
14	2.0.10.0

CNF version	FW version
13	2.0.8.0
12	2.0.7.0
11	2.0.5.0
10	2.0.3.0
9	2.0.1.0
8	1.4.8.0
7	1.4.6.0
6	1.4.5.0
5	1.4.3.0
4	1.4.1.0
3	1.3.6.0
2	1.3.4.0
1	1.3.2.0
0	1.3.1.0

The Status section displays the **Configuration checksum**. This checksum is unique to each unit and its current settings. Any modification to the configuration will result in a different checksum value. The checksum can also be retrieved via an API call.

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 7.7.6, "SMS"*).

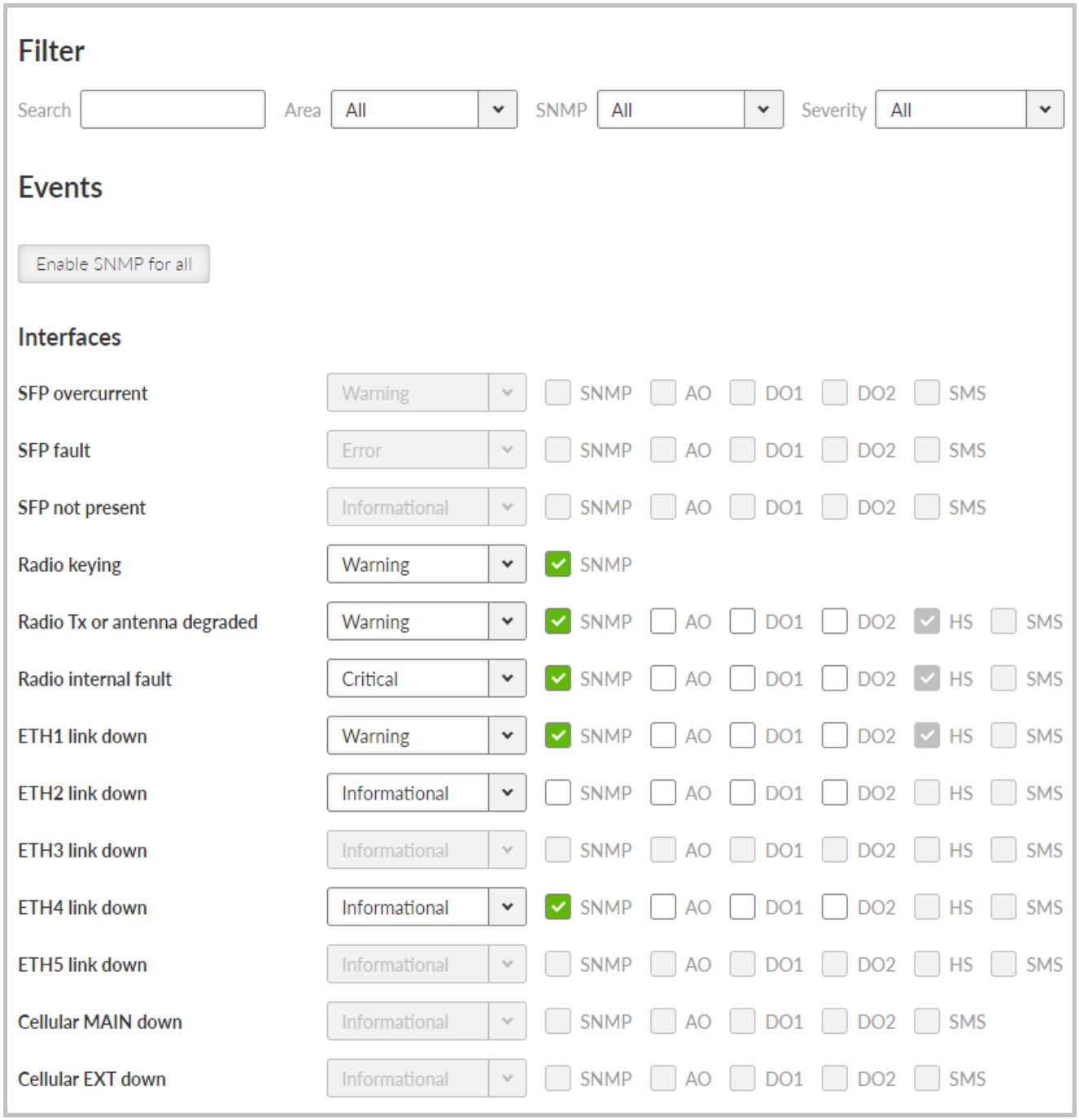


Fig. 7.44: SETTINGS > Device > Events

7.6.3.1. Test event

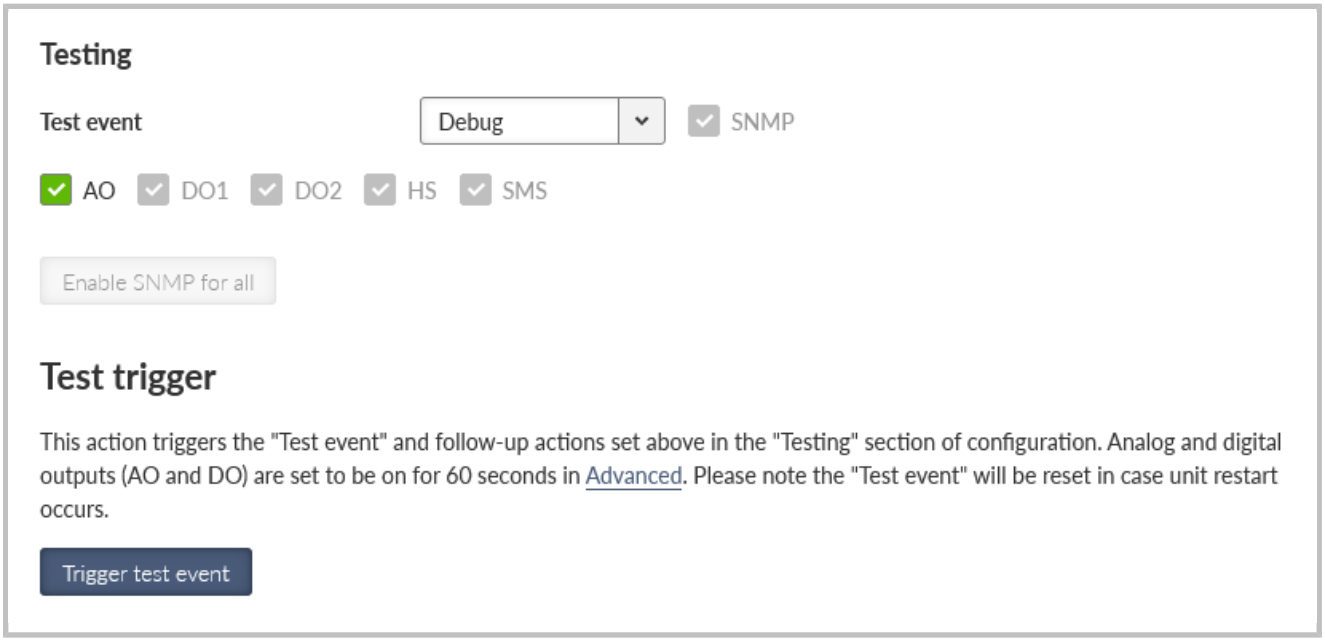


Fig. 7.45: SETTINGS > Device > Events

Pressing the "Trigger test event" button will activate the 'Test event' along with any subsequent actions defined in the 'Testing' configuration section . Specifically, the analog and digital outputs (AO and DO) will be active for 60 seconds (can be changed in Advanced menu).

Note

Unit restart will reset the Test event.

7.6.4. SW keys

Certain RipEX2 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.

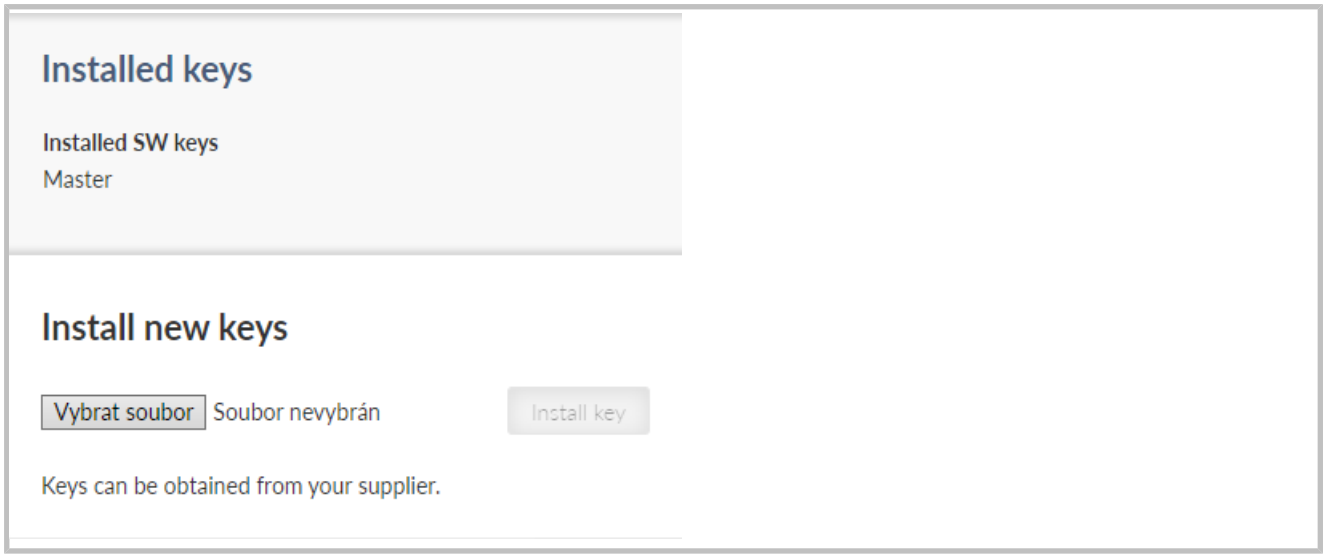


Fig. 7.46: SETTINGS > Device > Software keys

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	Without Key
Radio protocols	RProt	Protocols	Transparent and None
BGP	BGP	Dynamic routing	NA
OSPF	OSPF		NA
Babel	Babel		NA
Link management	LMgmt		NA
PPPoE*	PPPoE		NA
256 QAM	256Q	Speed	up to 64 QAM
Channels > 50 kHz	50kHz		up to 50kHz
Full duplex	FD		NA
RF power 40 dBm PEP	40dBm	Power	up to 37 dBm
IPsec	IPsec	Security	NA
OpenVPN	OpenVPN		NA
Multiple users	Users		Only one user
RADIUS	Radius		NA
Tamper detection	Tamp		NA
SFP	SFP	SFP	NA
DB9 COM2	COM2	COM2	NA

*By defaults from 03/2024, if you've purchased RipEX2 before this date and want to use this functionality, you will need to request the atomic key from the supplier.

Note

The newly added atomic keys are not included in the delivery of the previously ordered SW key (Link management for units dispatched before 07/2023, OpenVPN for units dispatched before 10/2023). Dispatch date is a part of Quality Inspection Report, which is available for each individual S/N via RACOM's WebService.

Installed atomic keys you can check using menu SETTINGS > Device > SW keys.

Master key substitutes all atomic keys (even these newly and in future added)

7.6.5. Firmware

7.6.5.1. Firmware versions

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). RipEX2 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.

Follow this recommended sequence to update your device from legacy versions:

Step 1:
Update from 1.X.X.X to 2.0.10.0.

Step 2:
Proceed to 2.1.0.0.

Step 3:
Move to 2.2.4.0.

Step 4:
Advance to 2.2.6.0 or 2.2.9.0.

Step 5:
Install the latest version (2.3.4.0 or higher).

This multi-step process ensures stability when you transition from older firmware versions.

7.6.5.2. Local

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.

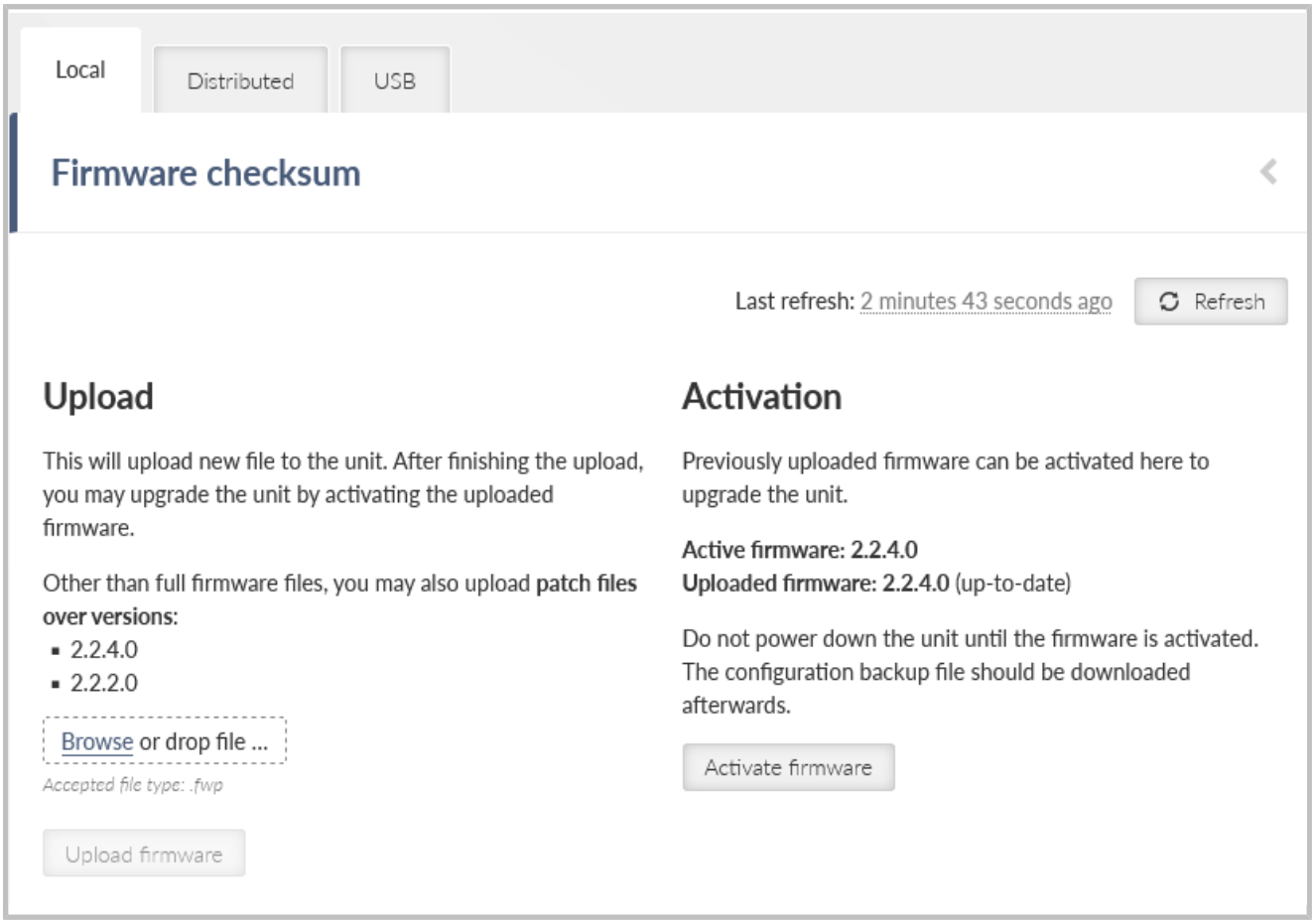


Fig. 7.47: SETTINGS > Device > Firmware

The Status section displays the Firmware checksum. This checksum is unique to each individual unit, differing even between units with the same firmware version. The checksum can also be retrieved via an API call.

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*[8]: Products – RipEX – Download – Firmware RipEX2 – ripex2-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 RipEX2 unit. In case of slow connection and file transfer longer than 120 s, the web browser will shut down the

[8] https://www.racom.eu/eng/products/radio-modem-ripex.html#download

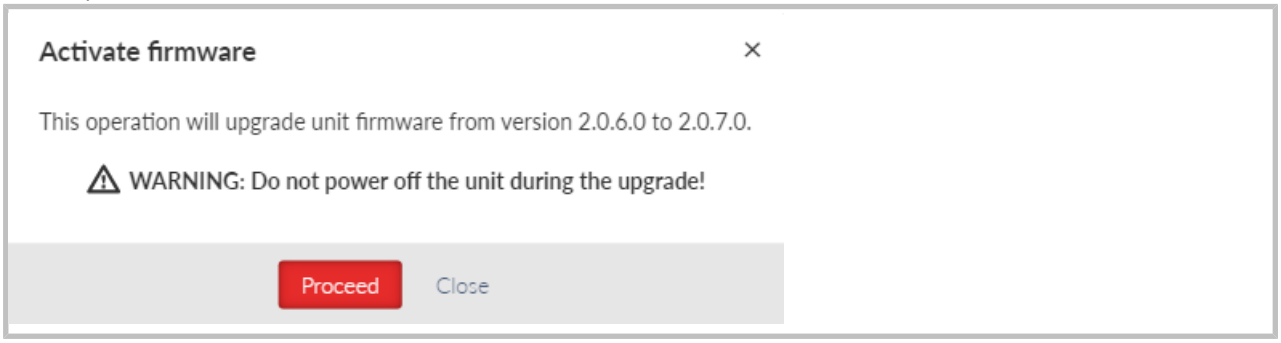
connection and the action will not finish successfully. This action does not update the running unit firmware yet. There is no affection on the other communication running through this unit. Successful uploading of the new firmware into the archive is announced in the Notifications and the available firmware version is highlighted under the "Activation" heading as "**Uploaded firmware:**".



Note

Admin level account has a possibility to dissable FW downgrade (menu ADVANCED > Firmware > Firmware - local by seting of the **Enable firmware downgrade** to Off), by default is this functionality allowed.

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.

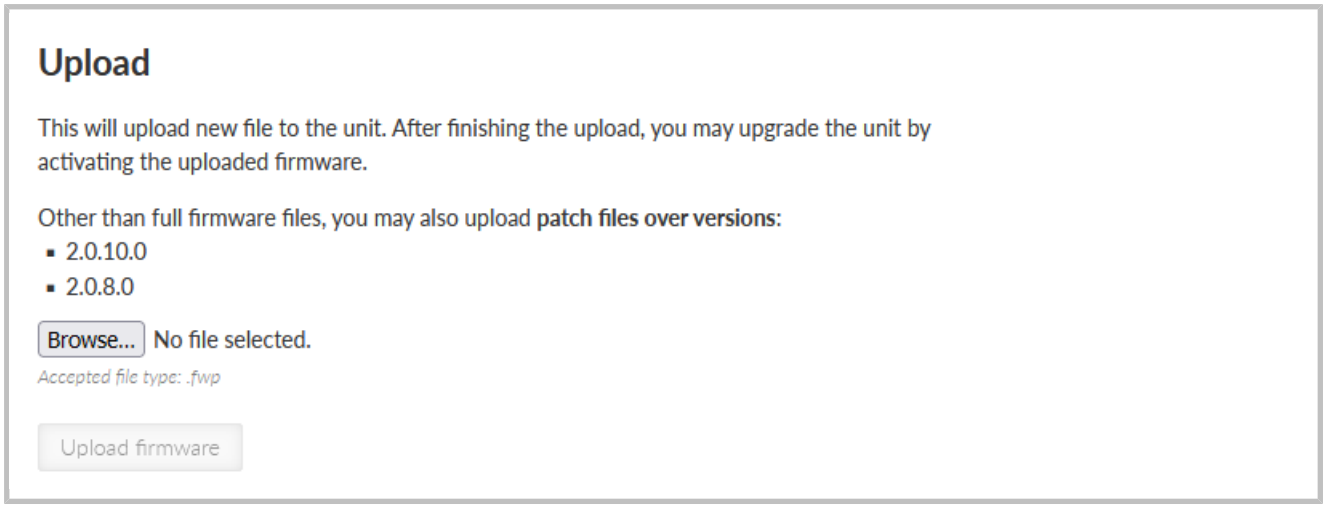
6. It is possible not only to upgrade the firmware version, but to even downgrade it, although this operation is not recommended. Be aware of eventual security issues of firmware downgrade as eventually outdated security code can be part of an old firmware. After FW downgrade, all unit parameters will be set to factory defaults.

7.6.5.3. 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 RipEX2 can be downloaded from *RACOM's web site*[9]. FW versions stored in RipEX2 are displayed in SETTINGS > Device > Firmware.

[9] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr2



Example: There are 2 older FW versions (2.0.8.0 and 2.0.10.0) stored in RipEX2 (picture above).

For successful activation of newer FW version (e.g. 2.0.13.0) using patch file either:

- Download patch files version upgrading from 2.0.8.0 to 2.0.13.0 or
- Download patch files version upgrading from 2.0.10.0 to 2.0.13.0 (recommended, because this patch file will be smaller).

The result will be the very same in both cases.

Note

FW versions (both patch files and full versions) are stored in *RipEX2 archive*[10] .

7.6.5.4. Distributed

When enabled, firmware file (or patch file) can be delivered to this unit using Firmware distribution service. This section configures the receiver part of the service. Receiver units accept distributed firmware files only from authorized senders. When the whole firmware file is accepted, it is saved into units firmware archive. Received firmware must be manually activated (SETTINGS > Device > Firmware > Local > Activate firmware button). Receiver unit will delete all transfers which are older than 14 days.

For more information, see *Section 7.7.1, "Firmware distribution"*.

[10] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_archive

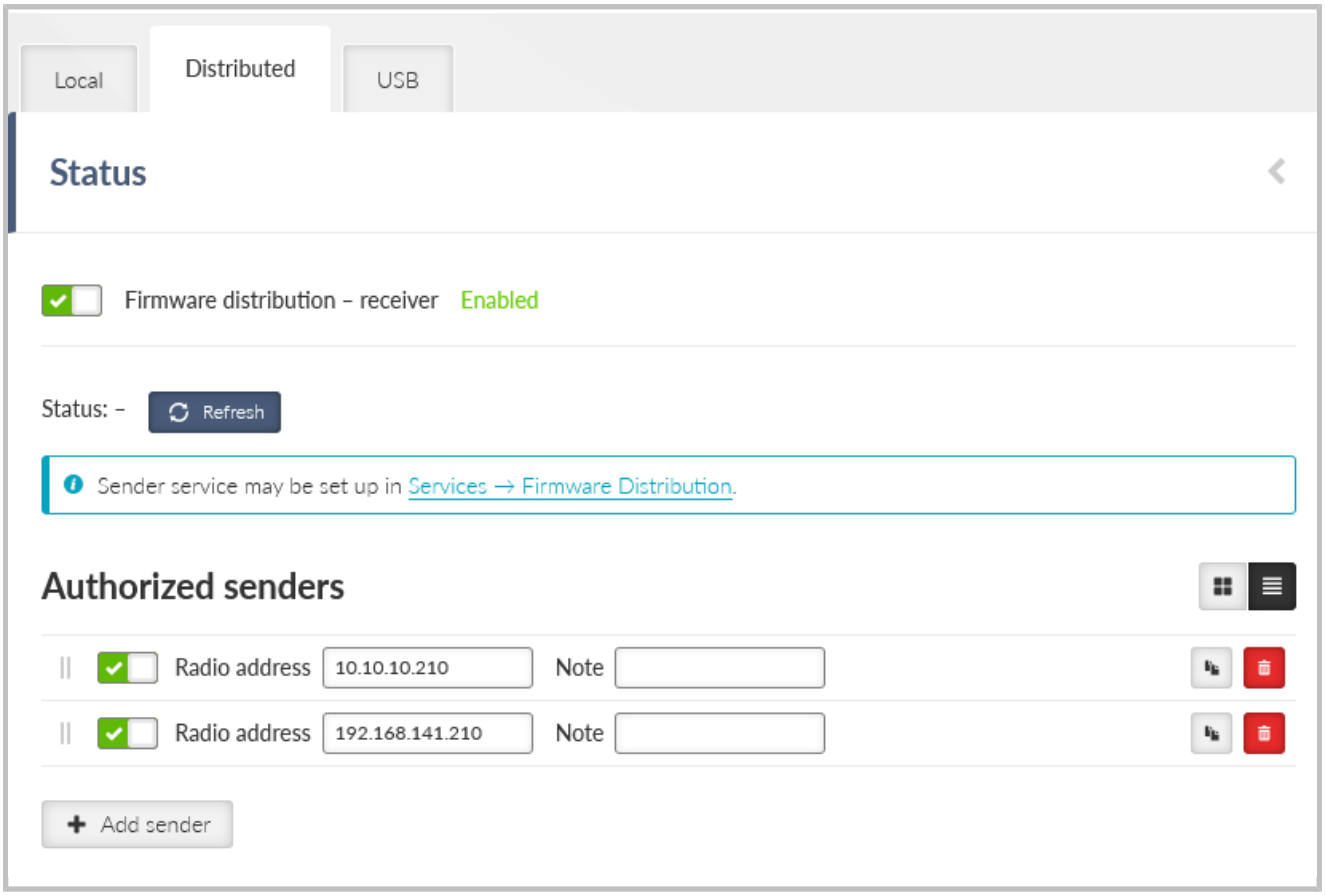


Fig. 7.48: SETTINGS > Device > Firmware > Distributed

Firmware distribution - receiver
Enable; Disable, default = "Disable"
Enables / disables the unit as a receiver.

7.6.5.4.1. Status

Information about running firmware distribution process (status, firmware file name, file size, progress) is described in this section.

7.6.5.4.2. Authorized senders

Defines the sender, from which the receiver unit accepts the distributed FW file.

Enable / Disable
Enables / disables the specific remote radio - sender.

Radio address
Defines the IP address of the radio interface.

Note
Informational note.

7.6.5.5. USB

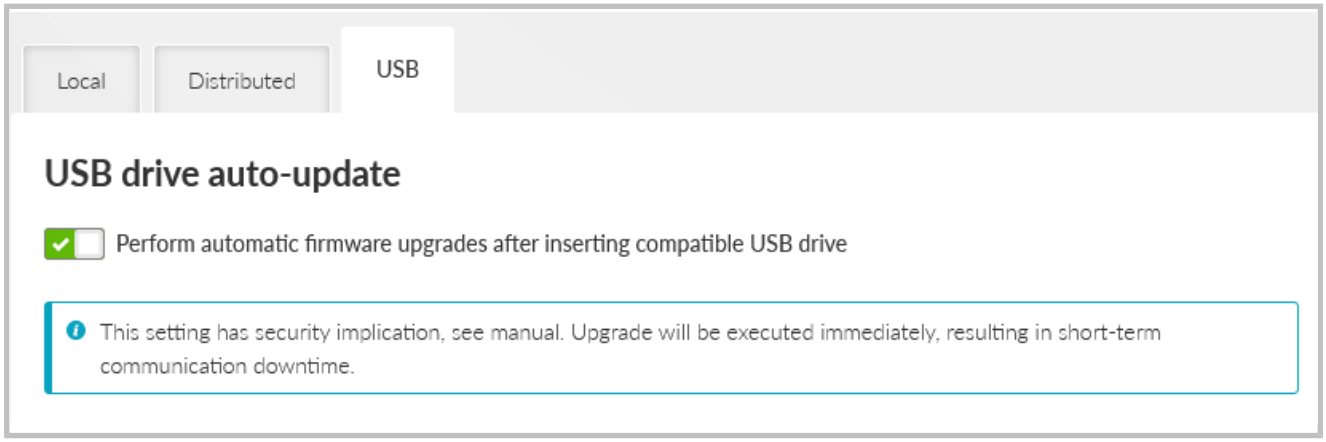


Fig. 7.49: SETTINGS > Device > Firmware > USB

Switch **Perform automatic firmware upgrades after inserting compatible USB drive** allowing FW upgrade from a USB flash disk. Downgrading using a USB disk is not possible. The change of this setting is activated after a new boot process.

The FW of the unit itself will be upgraded (not the FW of an eventual embedded module).

When allowed, the FW upgrade (from the USB flash disk) starts automatically after inserting the USB flash disk into the USB connector. The user is informed about the process via the SYS LED signalization (see Chapter 2.4. *Indication LEDs*).

The following conditions apply to processing:

- The USB drive must contain at least one partition. If there are more partitions, only the first one will be connected to the device.
- The first partition must be primary (physical) and must be formatted with the FAT12, FAT16, or FAT32 file system.
- The FW files must be located in the root directory. Subdirectories are not searched. FW files can be either standard files or soft links.
- The FW file name must have a .fwp or .cpio.enc extension. It does not matter whether the characters are lowercase or uppercase (case insensitive).
- There are no restrictions on the name of the FW file, only the extension rules must be followed. The character set allowed by the file system of the given USB drive (but we still recommend using the standard ASCII set).
- Any number of FW files (FW packages) can be stored on the USB drive (not all of them even have to be for a given device). From these, the device then "chooses" the FW that suits the given HW and has the highest version.
- If two or more suitable FWs are found on the disk, which have the same version, the first one is selected in order according to the lexicographic arrangement (this can happen, for example, if one file is full FW, while the other is FW-patch).

7.7. Services

7.7.1. Firmware distribution

RipEX2 can distribute its uploaded firmware to other RipEX2 units. This feature can be used during unit's regular traffic and offers to distribute firmware from one unit (sender) to another unit(s) (receiver) within one network. Firmware distribution is suitable especially in potentially problematic cases, e.g. for units with low signal quality, busy traffic or placed in a hard-accessible environment.

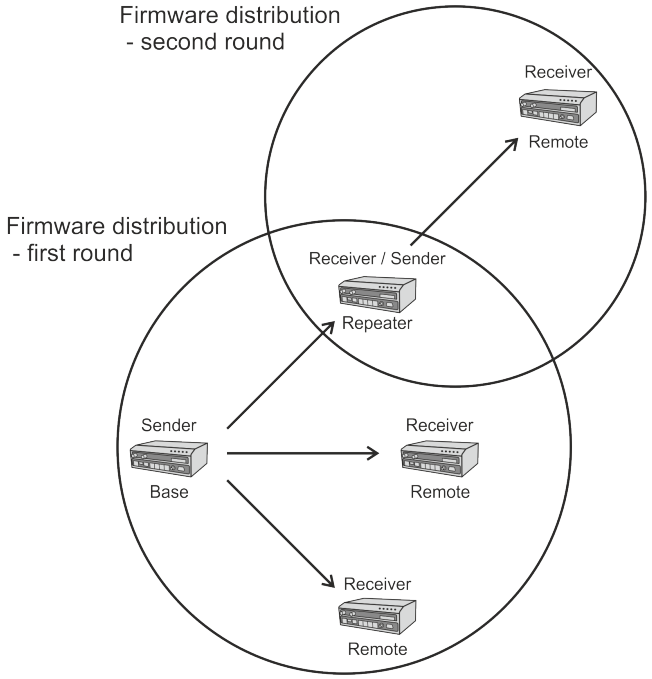
Distribution works over the radio network (FOTA - Firmware over the air) in form of multicast. Units must be available to each other within one IP hop. To set up FW distribution, RipEX2 unit must be set either as a sender or a receiver.

The process of Firmware distribution is composed of individual attempts of delivering the firmware file. The firmware file is uploaded into RipEX2's firmware archive. During distribution, the file is divided into multiple pieces (data blocks) which are gradually transferred to defined receiver units (the size of a data block is set to 512 B). If a data block is not transferred successfully (it gets lost), the receiver unit will again request the sender for it, until the data block is received (more information in ***Loss limit*** parameter). Only one file at a time can be distributed.

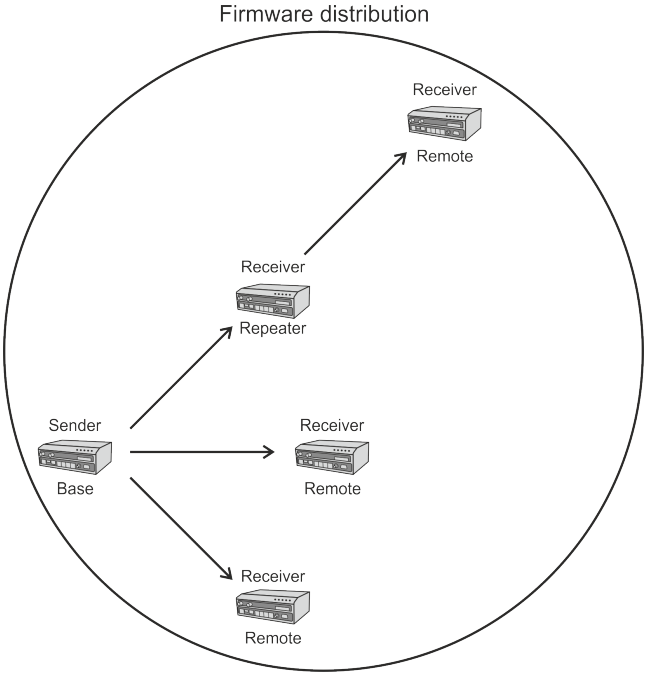
The transfer can be interrupted by events such as changing the configuration, unit reboot, Hot standby unit switch, etc. When the transfer is interrupted, its status is saved into unit's FLASH memory. The transfer will continue once the unit returns to its normal state. Interruptions which do not save the status (e.g. power outage) can lead into the loss of the distribution progress. If such a case occurs, the transfer will start from the beginning.

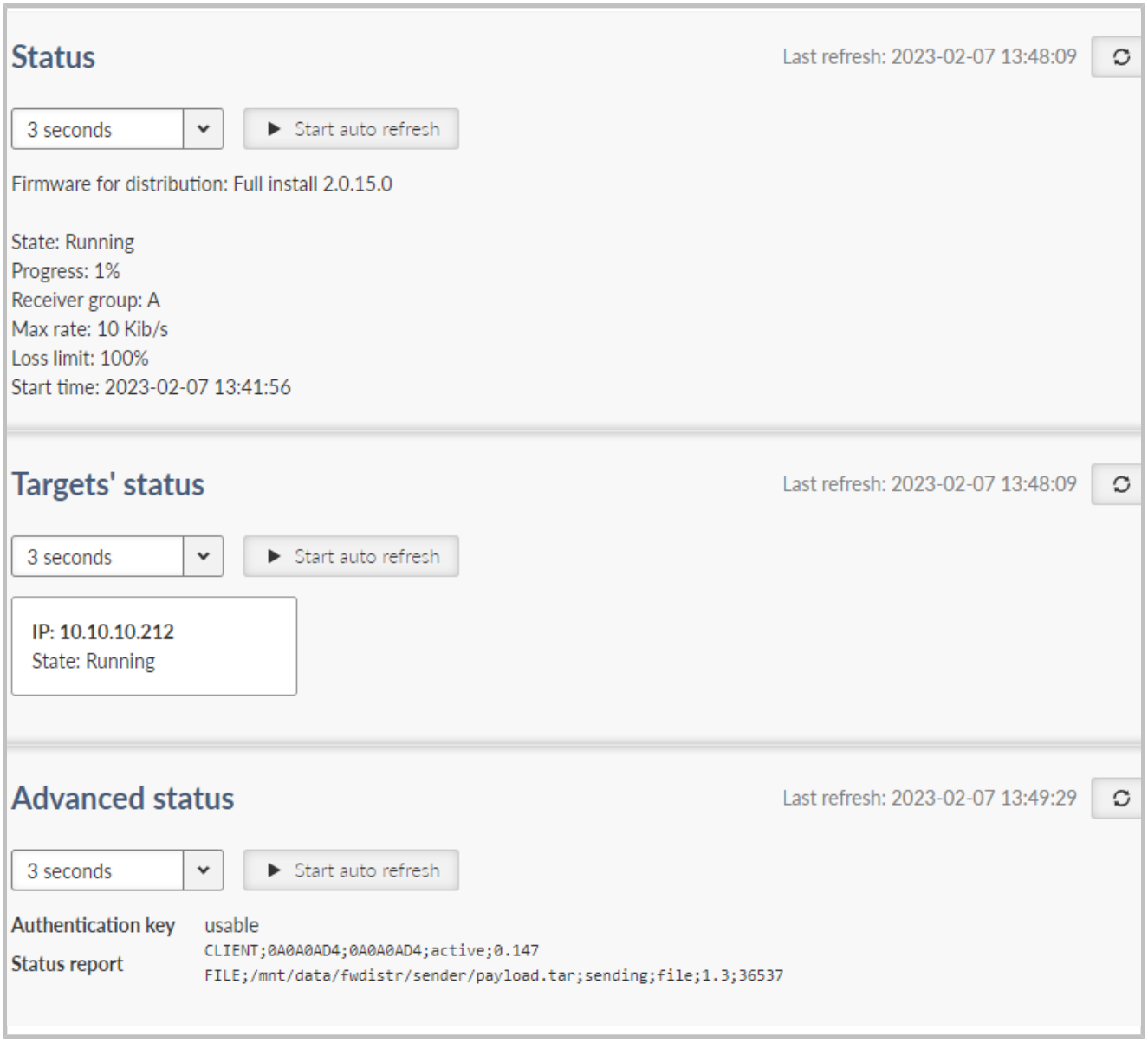
Patch files can be also distributed via Firmware distribution. A compatibility between the patch file and firmware of the receiver unit must be ensured (for more information, see *Section 7.6.5.3, "Patch files"*.

- When in Flexible protocol, the Firmware distribution works only in a star topology. In case of more complex topology, the firmware distribution must be launched gradually (from star to star). After the first round of firmware distribution finishes, another one can be launched from the repeater. The repeater will be re-configured to a sender and will distribute its uploaded firmware to receiver units within its star topology.



- When in Base driven protocol, the firmware is distributed from base unit to all units within the network which are defined as a receiver.




Status
Last refresh: 2023-02-07 13:48:09
3 seconds
Start auto refresh
Firmware for distribution: Full install 2.0.15.0
State: Running
Progress: 1%
Receiver group: A
Max rate: 10 Kib/s
Loss limit: 100%
Start time: 2023-02-07 13:41:56
Targets' status
Last refresh: 2023-02-07 13:48:09
3 seconds
Start auto refresh
IP: 10.10.10.212
State: Running
Advanced status
Last refresh: 2023-02-07 13:49:29
3 seconds
Start auto refresh
Authentication key
usable
Status report
CLIENT;0A0A0AD4;0A0A0AD4;active;0.147
FILE;/mnt/data/fwdistr/sender/payload.tar;sending;file;1.3;36537

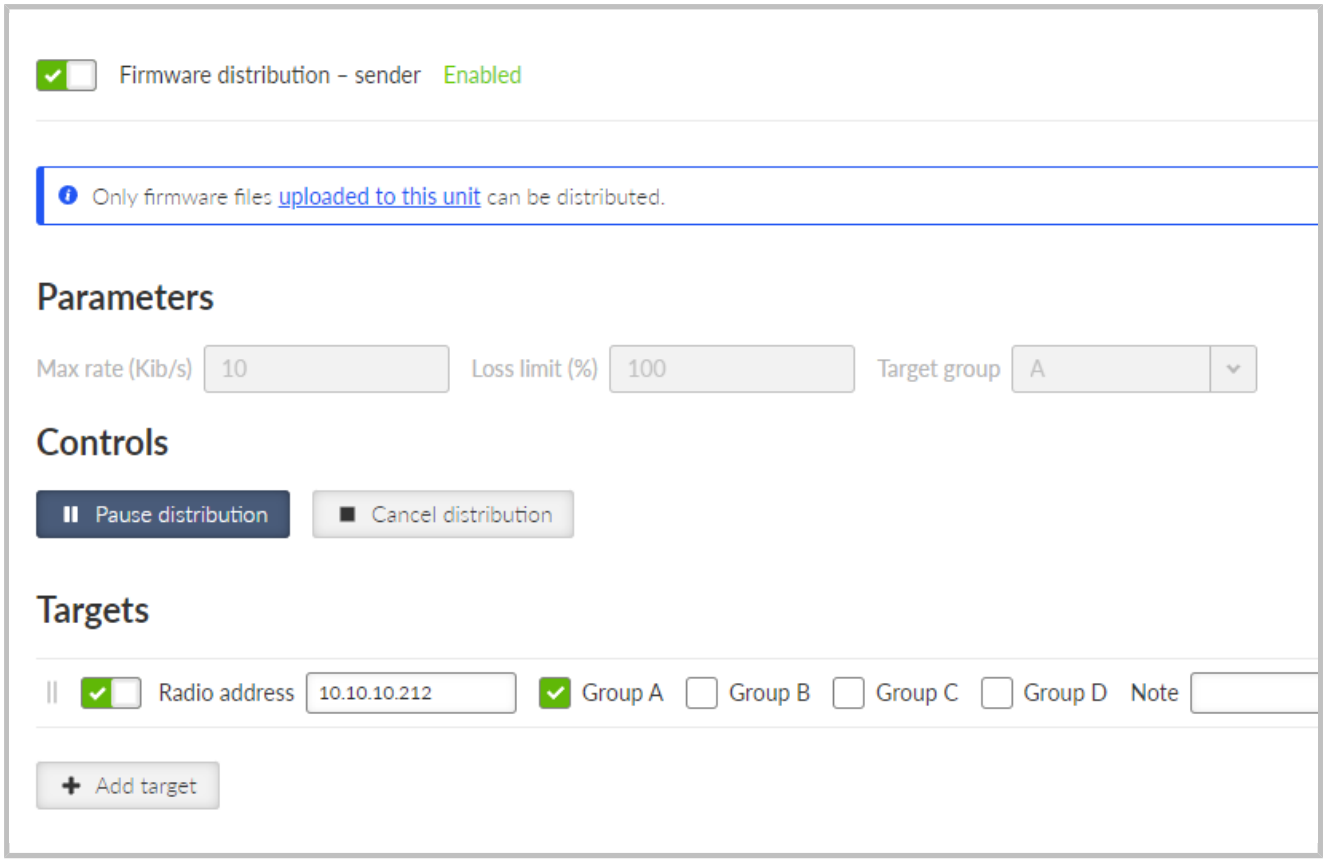


Fig. 7.50: SETTINGS > Services > Firmware distribution

Firmware distribution - sender

Enable; Disable, default = "Disable"

Enables / disables the unit as a sender. When enabled, the unit can transfer its uploaded firmware to defined receiver units.

To set the unit as a receiver, see *Section 7.6.5.4, "Distributed"*.

7.7.1.1. Status

Information about running firmware distribution process (status, progress, receiver group, max. rate, loss limit, start time) is described in this section.

7.7.1.2. Parameters

Max. rate (Kib/s)

Number {1 – 1000}, default = 10

Defines the maximum broadcast speed. The broadcast starts at a lowest speed and accelerates until it reaches the defined limit.

Loss limit [%]

Number {0 – 100}, default = 100

Defines the acceptable % of data loss (lost data blocks) for the first attempt to deliver the file. During the first attempt, receivers which exceeds the set Loss limit can be temporarily disabled from the transfer, so they would not restrain other receivers. After delivering the firmware file to receivers which were not disabled by the Lost limit, the transfer is restarted and attempts to deliver lost data

blocks to remaining units without Loss limit control. The number of attempts is limited to 256. If the data block is not successfully transferred after the last attempt, the transfer is declared to be invalid.

Target group (A, B, C, D)
List box {Group A; Group B; Group C; Group D}, default = "Group A"
Selects the group of receivers to which the firmware will be distributed.

7.7.1.3. Controls

Start / Pause distribution
Starts / Pauses the Firmware distribution. Once the firmware distribution is launched, **Loss limit** and **Target group** cannot be changed.

Cancel distribution
Cancels the Firmware distribution. If the firmware distribution is cancelled, the transfer progress will be lost.

7.7.1.4. Targets

Enable / Disable
Enables / disables the specific remote radio - receiver.

Radio address
IP address, default = 0.0.0.0
Defines the IP address of the radio interface.

Target Group
Click box {Group A; Group B; Group C; Group D}, default = "Group A"
Selects the receiver unit into a individual group to which the firmware will be distributed. One unit can be in multiple groups.

Note
Informational note.

7.7.2. DHCP servers

The DHCP server listens on selected interfaces. When a client from another station requests it, it assigns an IP address (DHCP lease) from the specified range.

Corresponding network interface must have a defined network range that includes the allocated range.

The DHCP server is then used specifically for this interface (ETH1 - ETH5, Wi-Fi).



Fig. 7.51: SETTINGS > Services > DHCP servers

7.7.2.1. DHCP servers configuration

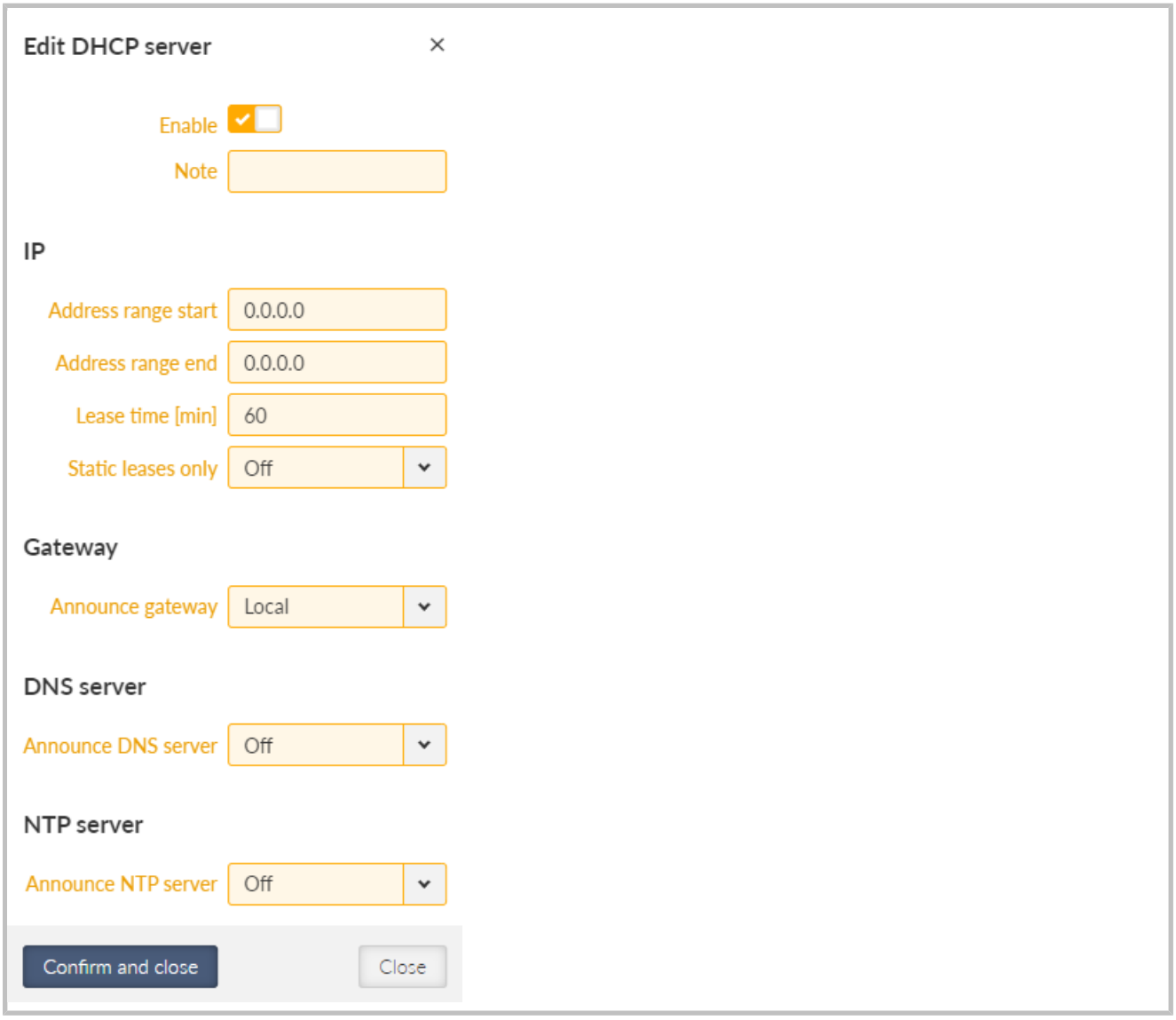


Fig. 7.52: SETTINGS > Services > DHCP servers > Configure

Enable
{Enable; Disable}, default = "Enable"
Enables the currently selected DHCP server.

Note
Informational note.

Address range start
IP address, default = 0.0.0.0
The start of the range of IP addresses allocated. It must be the case that **Address range start** <= **Address range end**.
Address must be in the address range of the ETH, LAN, VLAN, or Wi-Fi interface.

Address range end
IP address, default = 0.0.0.0

The end of the range of IP addresses allocated. It must be the case that **Address range start** <= **Address range end**.
Address must be in the address range of the ETH, LAN, VLAN, or Wi-Fi interface.

Note
The ranges of active DHCP servers must not overlap.

Lease time [min]
Number {2 – 10080}, default = 60
Address lease period. It is applied to both dynamic and static addresses.

Static leases only
List box {Off; On}, default = "Off"
Specifies whether the range is used only for allocating fixed (static) addresses. If enabled, it must be in the Static Leases table.

Announce gateway
List box {Off; Local; Manual}, default = "Local"
Configures the announcing of the router to clients.
Off: Gateway is not announced.
Local: The router's IP is announced as a gateway.
Manual: Manually set IP address is announced as a gateway.

Gateway address
IP address, default = 0.0.0.0
The IP address of the gateway being announced.

Announce DNS
List box {Off; Local; Manual}, default = "Local"
Configures the announcing of the DNS server to clients.
Off: DNS server is not announced.
Local: The router's IP is announced as a DNS server. Only if **DNS forwarding** is enabled.
Manual: Manually set IP address is announced as a DNS server.

Primary DNS server
IP address, default = 0.0.0.0
The IP address of the primary DNS server being announced.

Set secondary DNS server
List box {Off; On}, default = "Off"
Determines if the secondary DNS server is announced.

Secondary DNS server
IP address, default = 0.0.0.0
The IP address of the secondary DNS server being announced.

Announce NTP server
List box {Off; Local; Manual}, default = "Off"
Configures the announcing of the NTP server to clients.
Off: NTP server is not announced.
Local: The router's IP is announced as an NTP server. In RipEX2, the NTP daemon is always active, even if it only uses local time.
Manual: Manually set IP address is announced as an NTP server.

NTP server
IP address, default = 0.0.0.0
The IP address of the NTP server being announced.

7.7.2.2. Static leases



Fig. 7.53: SETTINGS > Services > DHCP servers > Static leases

Each line defines a static assignment of a fixed IP address to the client based on the MAC address.

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

IP address
IP address, default = 0.0.0.0
The fixed IP address assigned to the client.
Must be unique in the Static Leases table.
Must belong to the parent range in the DHCP Servers table.
It must not conflict with the local station address.

MAC address
MAC address, default = 00:00:00:00:00:00
The MAC address of the client for which the fixed IP address is assigned.
Must be unique in the Static Leases table.

Note
Informational note.

7.7.3. DNS

DNS forwarding functions as a DNS proxy server. Receives DNS queries from clients on selected interfaces. Filters queries. Translation of selected names can be blocked. Sends custom queries to a specified list of servers. Maintains a cache from which the client can respond immediately without querying parent servers.

7.7.3.1. Configuration

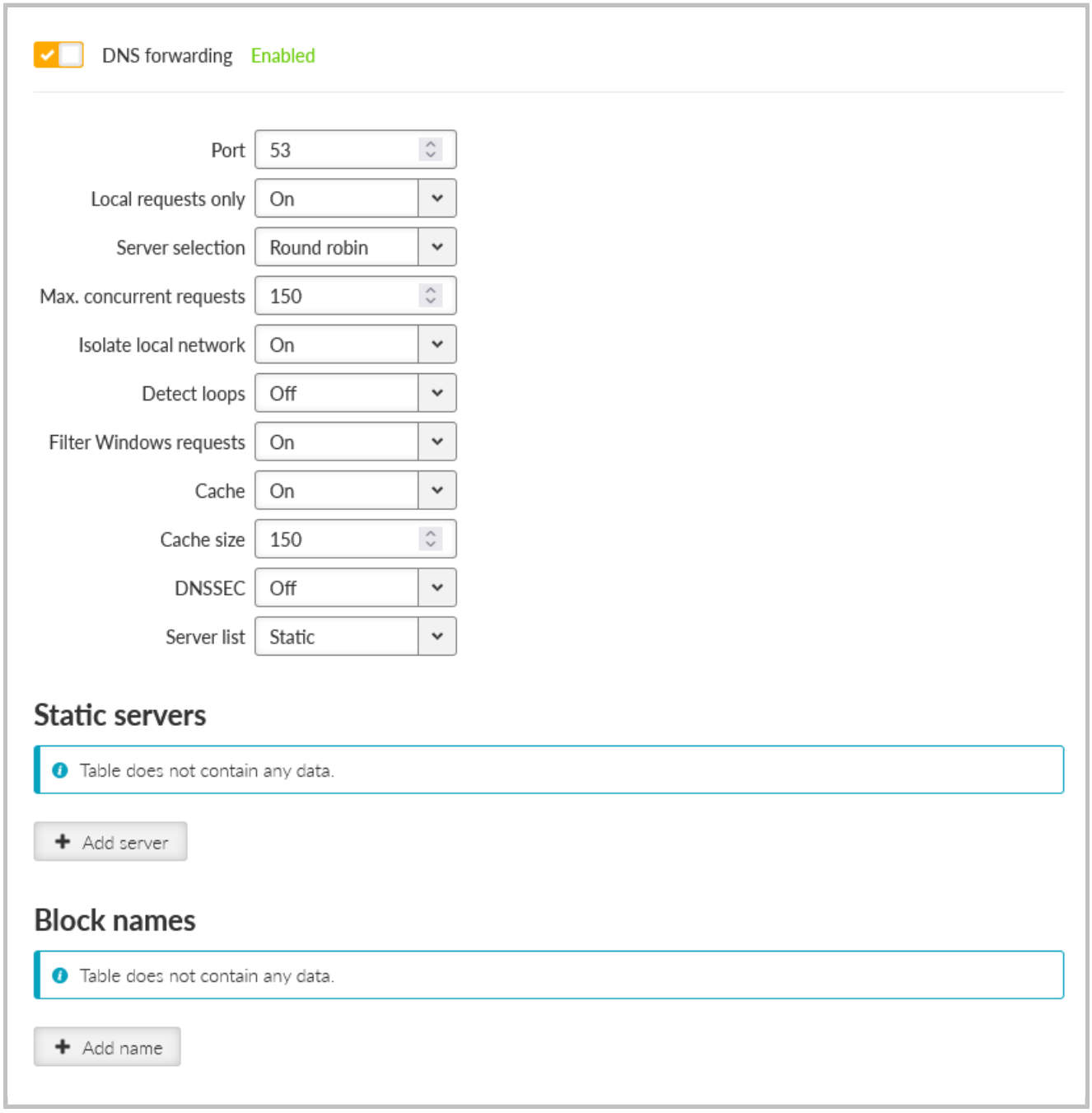


Fig. 7.54: SETTINGS > Services > DNS

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables DNS forwarding.

Port
Number {1 – 65535}, default = 53
The port number (both UDP and TCP) on which the server listens for client requests.

Local requests only
Listbox {Off; On}, default = "On"

Determines if the server only serves requests from addresses on the local network (from addresses in ranges set on the interfaces). Requests from other addresses will be rejected.

Server selection
List box {Round robin; Strict order; All simultaneously}, default = "Round robin"
Sets how servers are selected for the query.

Round robin
Selects servers one by one, preferring those that answered.

Strict order
Always starts with the first server in the list, and tries the next in the sequence if it fails.

All simultaneously
The request is sent to all servers at the same time and the first response is awaited.

Max. concurrent requests
Number {5 – 250}, default = 150
The maximum number of DNS requests running simultaneously.

Isolate local network
Listbox {Off; On}, default = "On"
Determines whether the server isolates the local network. If enabled, it blocks forcing translation of local addresses from parent servers, it does not send reverse queries to private addresses to parent servers.

Detect loops
Listbox {Off; On}, default = "Off"
Enables loop detection between DNS servers.

Filter Windows requests
Listbox {Off; On}, default = "On"
Filters periodic DNS requests generated by Windows.

Cache
Listbox {Off; On}, default = "On"
Enables cache responses to DNS requests. If the response to the client request is cached, it is returned immediately and there is no need to make further requests to the parent servers.

Cache size
Number {50 – 10000}, default = 150
Maximum number of entries in the cache.

DNSSEC
Listbox {Off; On}, default = "Off"
Enables authentication of responses from parent servers using DNSSEC and chain of trust (**DNS trust anchors** table).

Server list
Listbox {Static; Dynamic}, default = "Static"

Static
Static list of servers in the **Static servers** table.

Dynamic
Listbox {WWAN (MAIN); WWAN (EXT); PPP 1; PPP 2; PPP 3; PPPoE client}, default = "PPPoE client"
The list of servers is obtained from the dynamic WAN interface parameters. The corresponding interface must be active.

7.7.3.1.1. Static servers

The rows define the addresses of the parent DNS servers in the static list.

The maximum number of DNS servers is 32.

Active only if Server list is set to Static.



Fig. 7.55: SETTINGS > Services > DNS > Static servers

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

Domain
String {0–128 char}, default = <empty>
Domain name.

IP address
IP address, default = 0.0.0.0
IP address of the static server.

Port
Number {1 – 65535}, default = 53
The destination port on which the server listens for DNS requests.

Note
Informational note.

7.7.3.1.2. Block names

Each line defines DNS names whose translation is blocked.

The maximum number of blocked names is 128. The order does not matter.

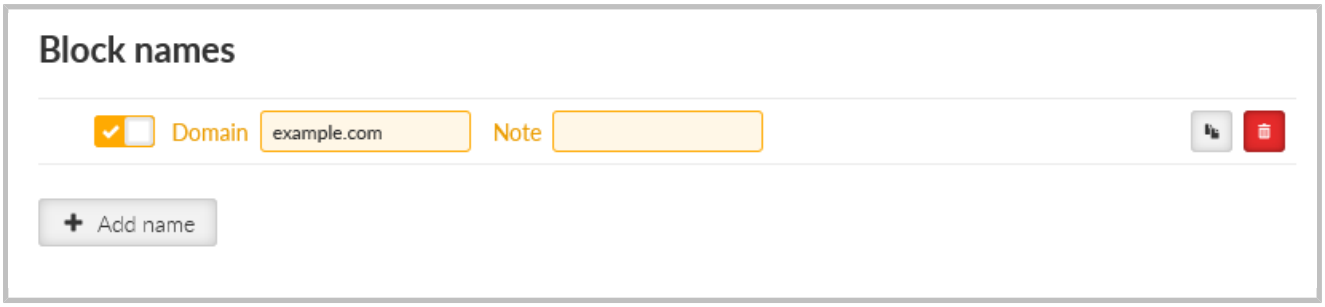


Fig. 7.56: SETTINGS > Services > DNS > Block names

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

Domain
String {0–128 char}, default = "example.com"
Domain name, which translation to the address will be blocked.

Note
Informational note.

7.7.3.1.3. DNS trust anchors

Each line defines a DNSSEC Trust Anchor.

The maximum number of DNSSEC Trust Anchors is 8. The order does not matter.

Active only if Cache and DNSSEC are turned On.

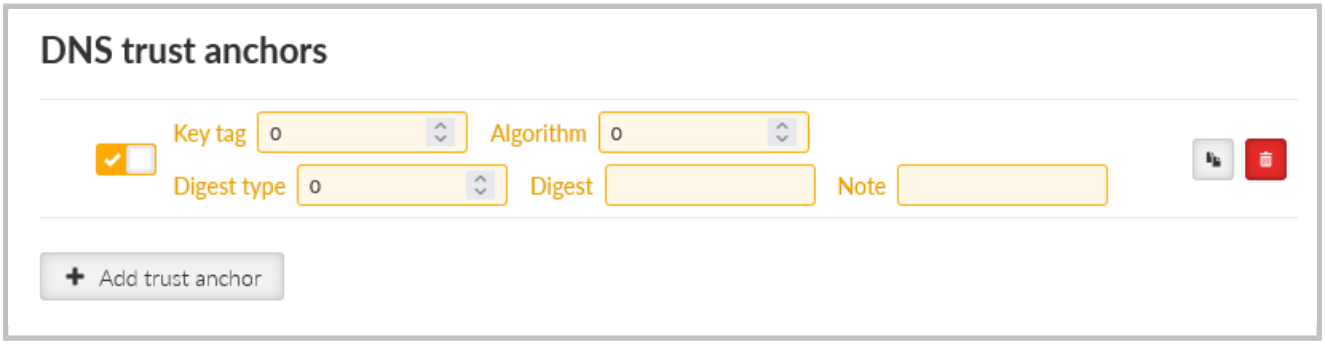


Fig. 7.57: SETTINGS > Services > DNS > DNS trust anchors

Enable
Listbox {Enable; Disable}, default = "Enable"
Enables/Disables selected line.

Key tag
Number {0 – 65535}, default = 0
Key identifier. Must be unique among the active lines in the table.

Algorithm
Number {0 – 255}, default = 0
Key algorithm identifier.

Digest type
Number {0 – 255}, default = 0
Key digest algorithm identifier.

Digest
Hexadecimal string, default = <empty>
Digest (hash) key.

Note
Informational note.

7.7.4. SNMP

SNMP (Simple Network Management Protocol) implementation in RipEX2 provides three SNMP versions: v1, v2c and v3.

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 RipEX2 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 RipEX2 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*[11].

[11] https://www.racom.eu/eng/products/m/ripex/app/snmp-ripex2/index.html

7.7.5. Syslog

Syslog enables logging of events on a remote server. Syslog messages are created in the unit in accordance with RFC5424 and sent to a remote server. Messages can be sent using UDP or TCP.

New system logs and events start to be sent to the remote server after the station boots. Incase of unavailability of the remote server, the logs are stored in the disk buffer and sent to the remote server after re-establishing a connection with it.

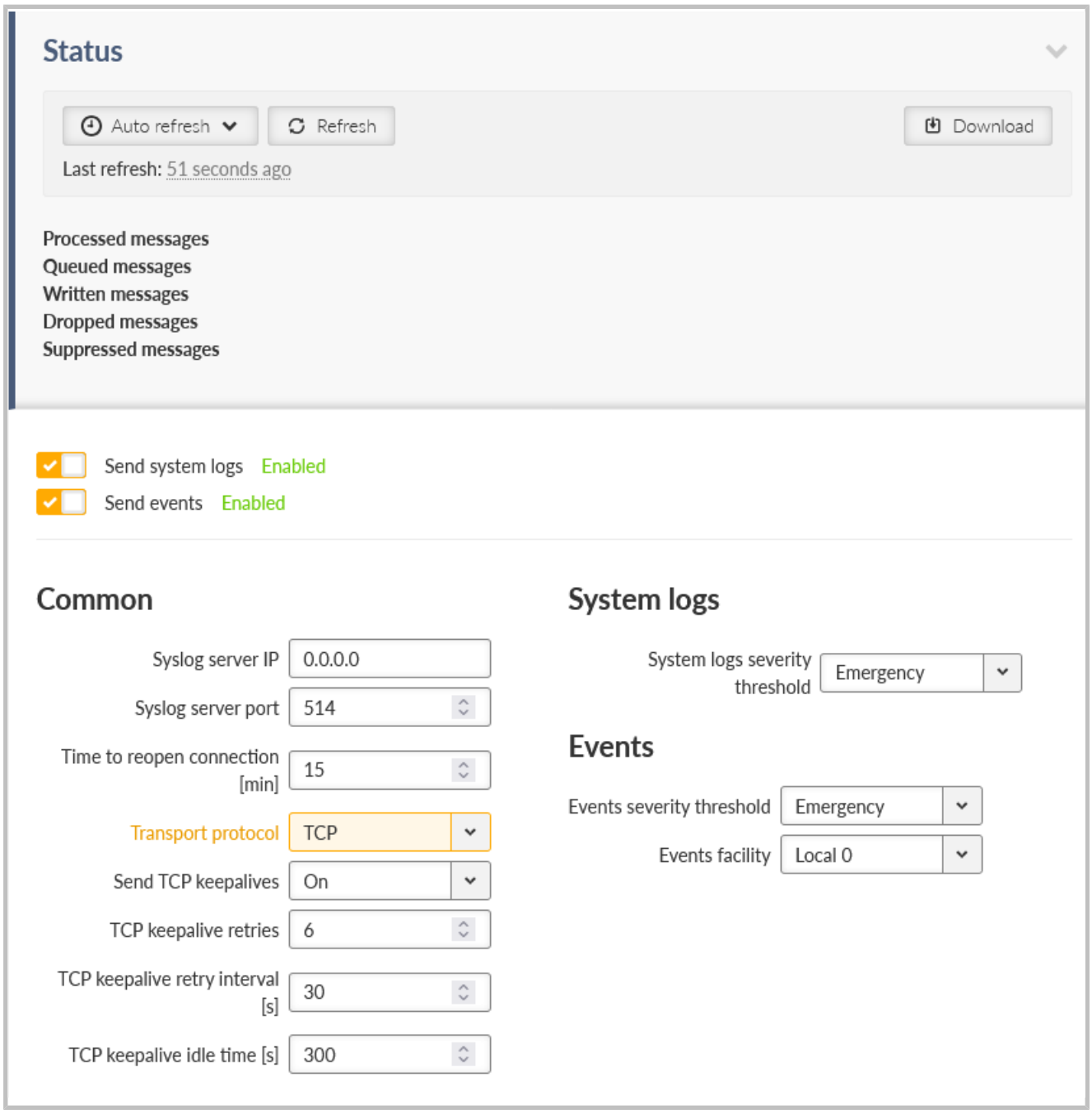


Fig. 7.58: SETTINGS > Services > Syslog

Send system logs
{Enable; Disable}, default = "Disable"
Activates/Deactivates sending of system logs to the remote server

Send events
{Enable; Disable}, default = "Disable"
Activates/Deactivates sending of system events to the remote server

Common

Syslog server IP
IP address, default = 0.0.0.0
IP address of the remote syslog server

Syslog server port
Number {1 – 65535}, default = 514
Syslog remote server port number

Time to reopen connection [min]
Number {1 – 240}, default = 15
Time (in minutes) to wait to retry of the connection to the remote server when the connection was closed

Transport protocol
List box {UDP; TCP}, default = "UDP"
Type of the protocol for the data transport

When TCP:

Send TCP keepalives
List box {Off; On}, default = "On"
Switches On/Off sending of the TCP keepalives messages

TCP keepalive retries
Number {1 – 15}, default = 6
Number of keepalive retries when the reply was not received.

TCP keepalive retry interval [s]
Number {10 – 240}, default = 30
The interval (in seconds) at which a TCP keepalive message is re-sent if no response is received.

TCP keepalive idle time [s]
Number {60 – 64800}, default = 300
Connection inactivity time (in seconds) waiting for the TCP keepalive message to be sent.

System logs

System logs severity threshold
List box {Emergency; Alert; Critical; Error}, default = "Emergency"
System messages with this and higher severities will be sent to the remote server. Messages with lower severities will not be sent.

Events

Events severity threshold
List box {Emergency; Alert; Critical; Error; Warning; Notice; Informational}, default = "Emergency"
System events with this and higher severities will be sent to the remote server. Events with lower severities will not be sent.

Events facility
List box {Local 0; Local 1; Local 2; Local 3; Local 4; Local 5; Local 6; Local 7}, default = "Local 7"
Classification of system events into facilities as per RFC 5424 for local use: Local 0 to Local 7 (numerical codes 16 to 23) can be set. Consult with your Syslog server administrator about which facility will be used for individual groups of units.

7.7.6. SMS

RipEX2, 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.

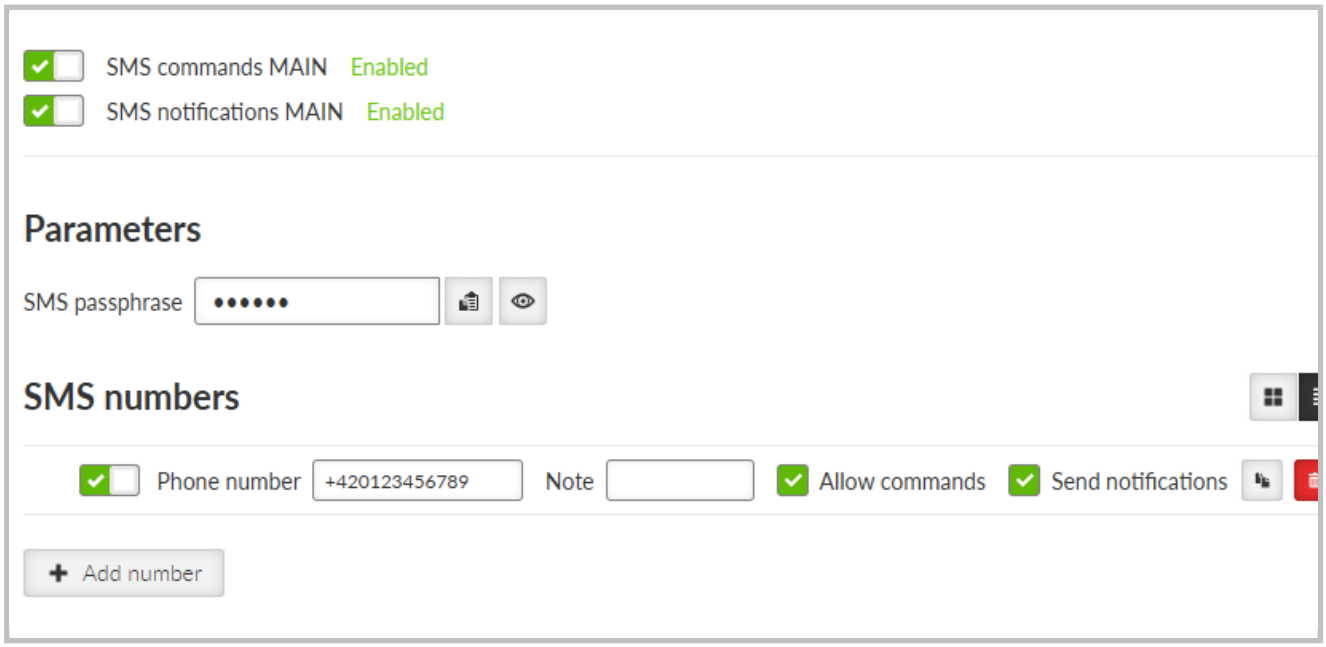


Fig. 7.59: SETTINGS > Services > SMS

Note

This section closely cooperates with *Section 7.1.5, "Cellular"*.

SMS commands EXT
{Enable; Disable}, default = "Disable"
Enables / Disables SMS commands for Cellular EXT. When enabled, the software module allows all incoming SMS and proceeds to initiate commands.

- 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 passphrase to pass the authentication (parameter **SMS passphrase)**.

- 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 EXT
{Enable; Disable}, default = "Disable"
Enables / Disables SMS commands for Cellular 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"*.

7.7.6.1. Parameters

SMS passphrase
String {2–16 ASCII char}, default = "public"
Sets an SMS passphrase, which serves as an authentication to send SMS from defined phone number(s). The range of length of the passphrase is between 2–16 characters. SMS passphrase must not contain any unsupported characters. Unsupported characters are: ", `, \, $, ;.

7.7.6.2. 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 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 EXT is enabled.

7.7.6.3. SMS commands

All commands must match following format:

<passphrase>"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.

7.7.7. Hot standby

7.7.7.1. Hot standby settings

Following settings is supported by the controller version of the RipEX2-HS, where the controller manages the active and passive/standby RipEX2 units and their accessing to the shared channels (e.g. radio).

The HW switch (mode selector) has to be set to AUTO position for switching between units, otherwise the selected unit remains active even if an error occurs on the selected one.

AUTO regime allows switching to the standby unit when an error status occur in active unit – if both units are without alarms, the A unit will be active.

For detailed settings of unit switching (and its conditions of switching) see sections *Events*[12] and *Antenna detection*[13] in RipEX2 User manual and section *"Switching over" Ripex2-HS*[14].x

Important

The communication between individual RipEX2 units and HS controller use DI/DO interfaces, so other use of these interfaces is not possible.

Note

HW option RipEX2e (product variant ‘H' and 'J’) cannot be used in Hot standby configuration.

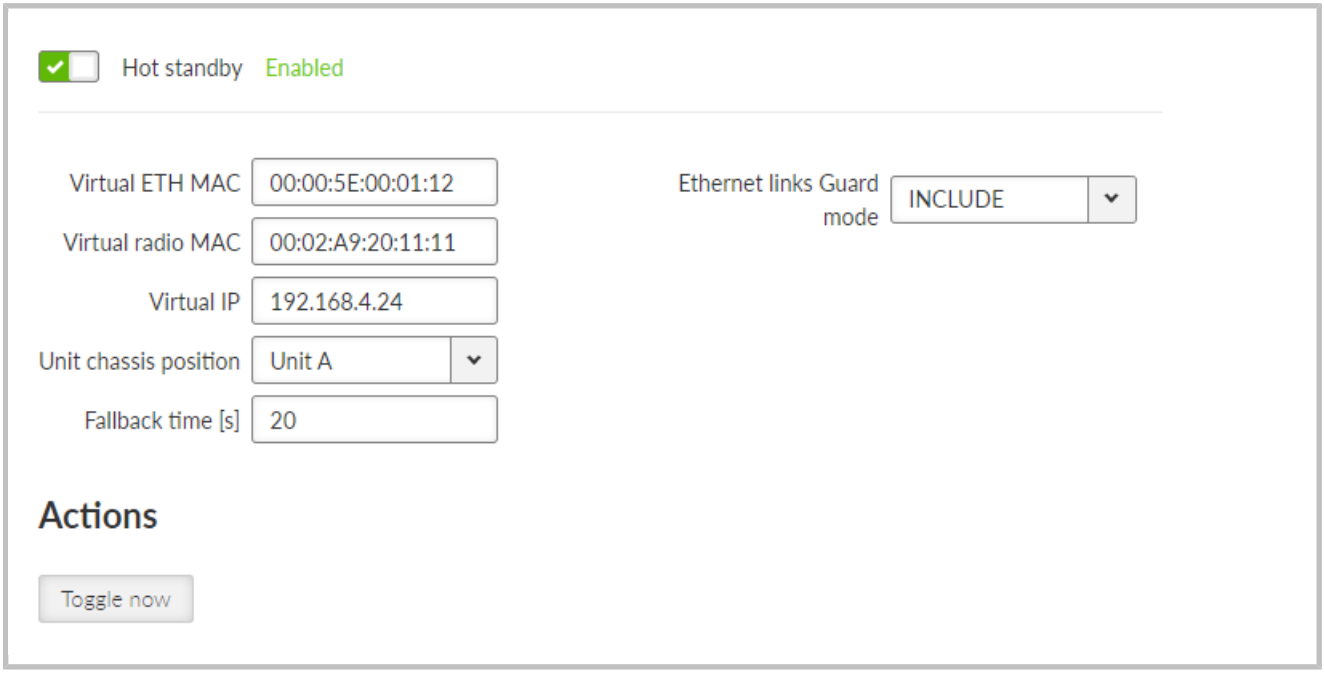


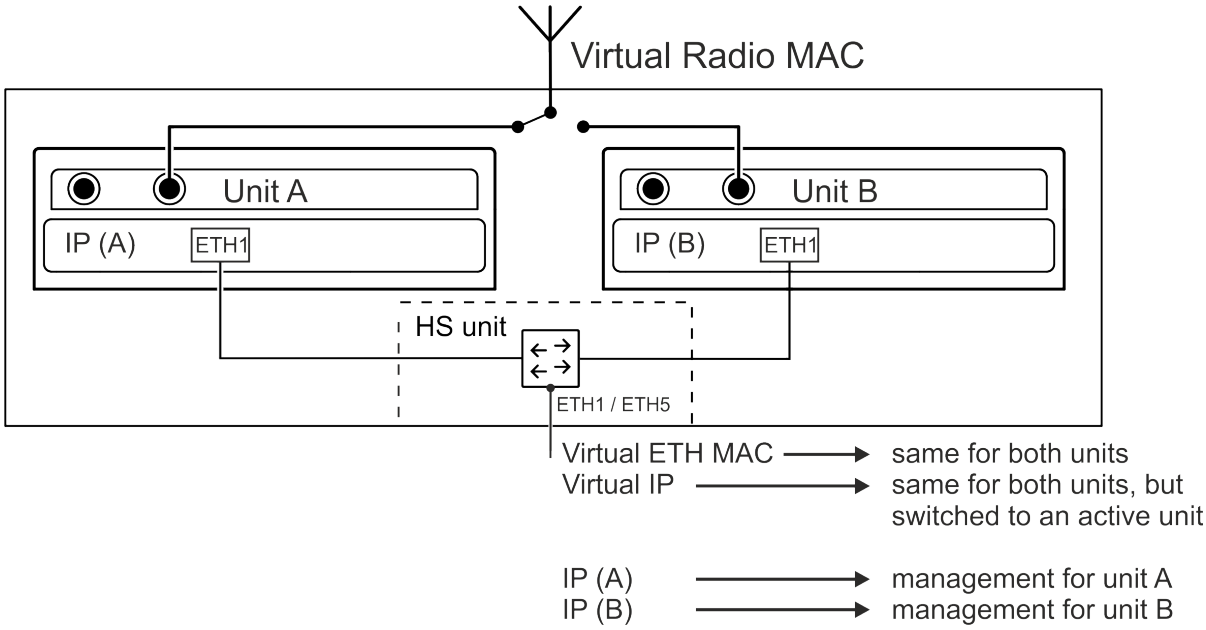
Fig. 7.60: SETTINGS > Services > Hot standby

Hot standby mode enabled
List box {On; Off }, default = "Off"
Switches Hot standby functionality.

Virtual ETH MAC
MAC address of shared LAN interface. It should be same for both individual RipEX2 units. This MAC address has to differ from other MAC addresses used in unit. It is possible to use e.g. VRRP type of addresses: 00:00:5E:00:01:XX.

Virtual Radio MAC
While in Hot standby mode, it is necessary to set identical radio MAC address (HotStdby_RadioMac) in both stations, because protocol link address is derived from the address.

[12] https://www.racom.eu/eng/products/m/ripex2/set.html#set-device-events
[13] https://www.racom.eu/eng/products/m/ripex2/diagnostic.html#diag-tools-antenna
[14] https://www.racom.eu/eng/products/m/ripex2-hs/ripex_detail.html#d6e553



Virtual Radio MAC address has to differ from Virtual MAC address and all other addresses in the unit.
This parameter is used only, if the unit is running on Flexible protocol.
To prevent a collision with broadcast addresses (in case of Flexible protocol usage), the address must not be ended with :FF:FF:FF.

Virtual IP

This address has to fit into range of addresses used for the relevant network interface (e.g. ETH 1) and will be used as shared IP address for LAN interface. Typically used for connection of attached technology.

Note
The radio address used according to setting in SETTINGS > Interfaces > Radio > IP - the same address has to be set in both radio modems.

Unit chassis position

List box {Unit A; Unit B}, default = "Unit B"Position of the unit in HS chassis, set Unit A for unit in A position and vice versa.

Fallback time

Time in seconds. The time delay to stay on the standby unit, after all alarms are solved.

Ethernet links Guard mode

List box {INCLUDE; EXCLUDE}, default = "INCLUDE"Defines the behavior of guarding of ETH interfaces. "INCLUDE" requires all guarded lines in UP status – if one of these guarded lines is not in UP state, alarm occurs and the switching to the standby unit is executed. "EXCLUDE" requires at least one guarded line in UP status.

Toggle now

This button allows to switch from unit Active status to the non-active.
It will not be possible if:

- The second unit is in alarm status.
- The HW MODE selector is not set to AUTO.
- The unit is in not-active status.

7.7.7.2. Hot standby LAN interface settings

It is necessary to set LAN interface used for HS functionality.

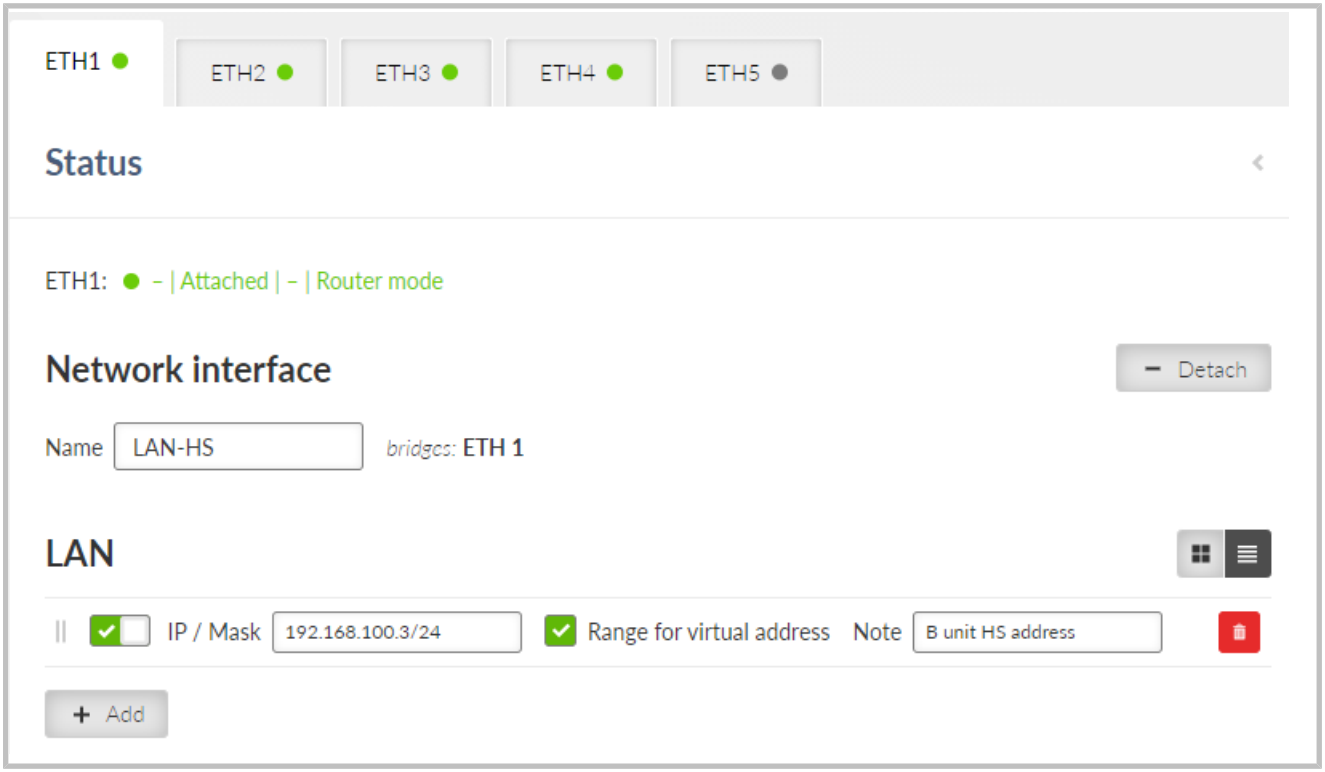


Fig. 7.61: SETTINGS > Interfaces > Ethernet

The Range for virtual address parameter is in this menu available only when HS functionality in the menu SETTINGS > Device > Unit > Hot standby is enabled (see above).

The parameter Range for virtual address has to be set to On for the LAN address interconnected with shared ETH interface (Range for virtual address set to On).

Note

Interconnected ETH interface IP addresses of both ETH addresses must be different as well as addresses of A and B units, yet in the same range as the virtual shared address (= together three different addresses in the same range).

7.7.7.2.1. Hot standby switching settings

The events which switch HS shall be set in menu SETTINGS > Device > Events, check the HS box for events required for switching from the active unit to the backup one. Settings in both units has to be the same.

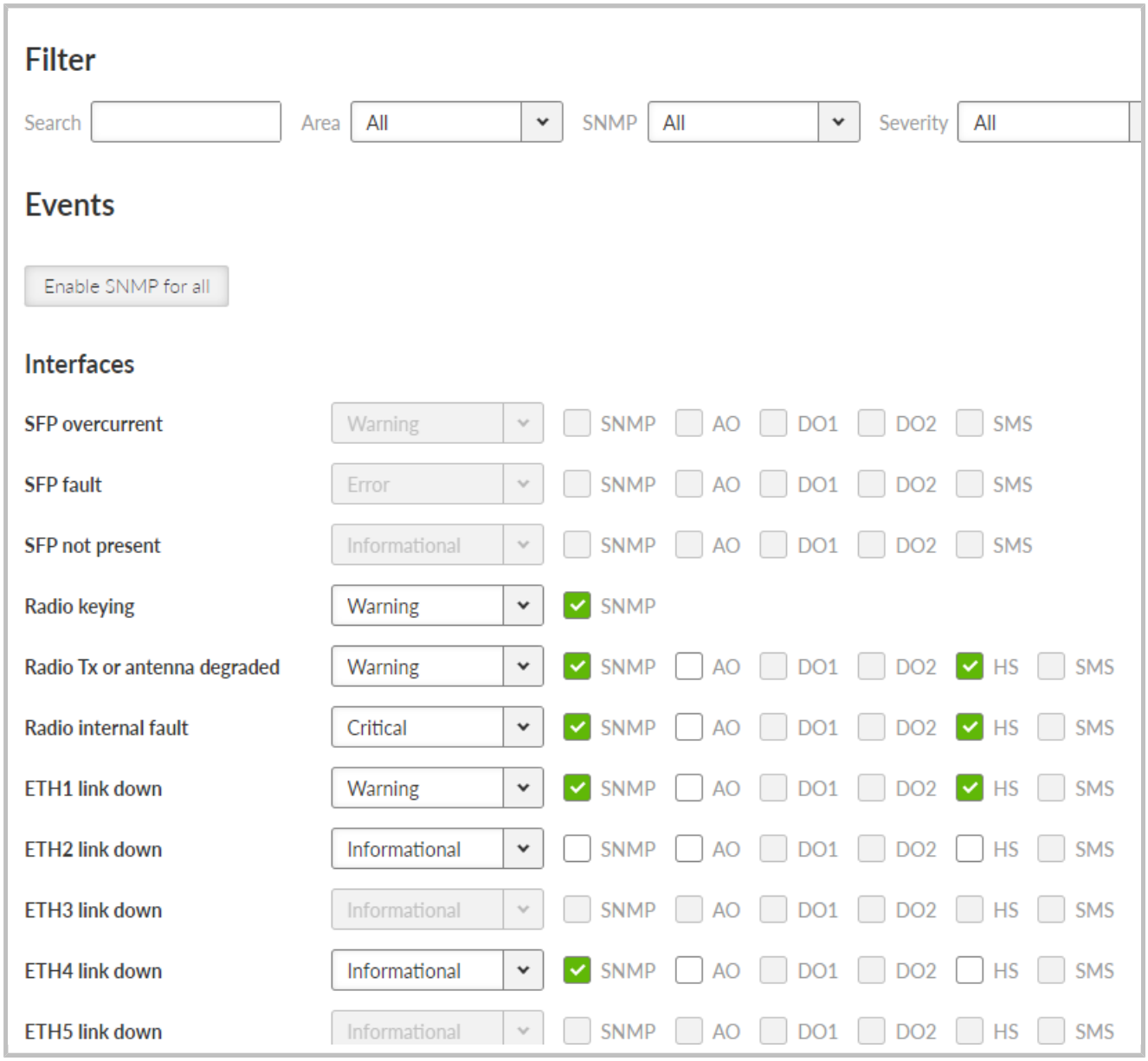


Fig. 7.62: SETTINGS > Device > Events

7.7.8. 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.

Data retrieval is possible using a gpsd client application (such as cgps or gpspipe). JSON data format is supported, and TPV, SKY, and PPS data frames are available.

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 GNNS 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

RipEX2 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 RipEX2.

Please note, that RipEX2 is a very powerful device and it really shows all parameters in the Advanced section.

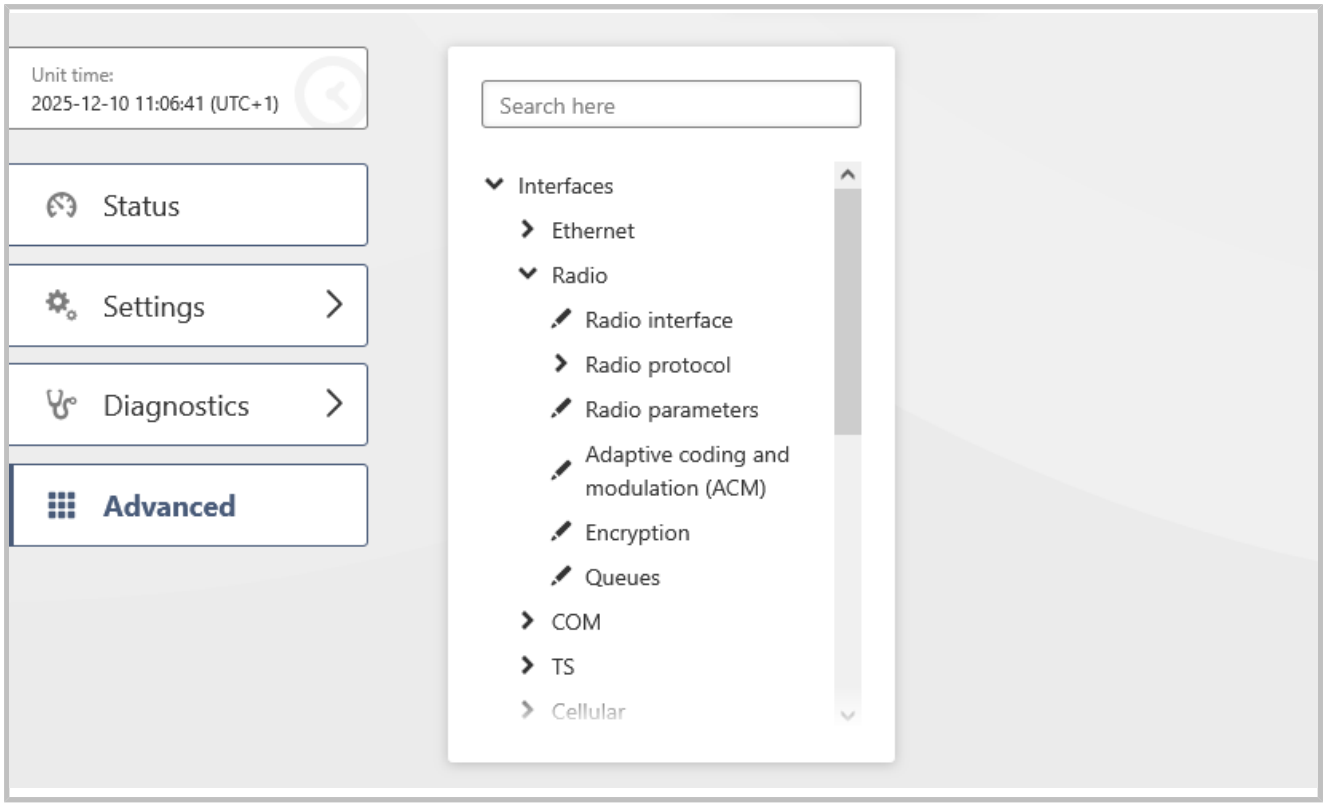


Fig. 7.63: ADVANCED

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 “Generic”, 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”.

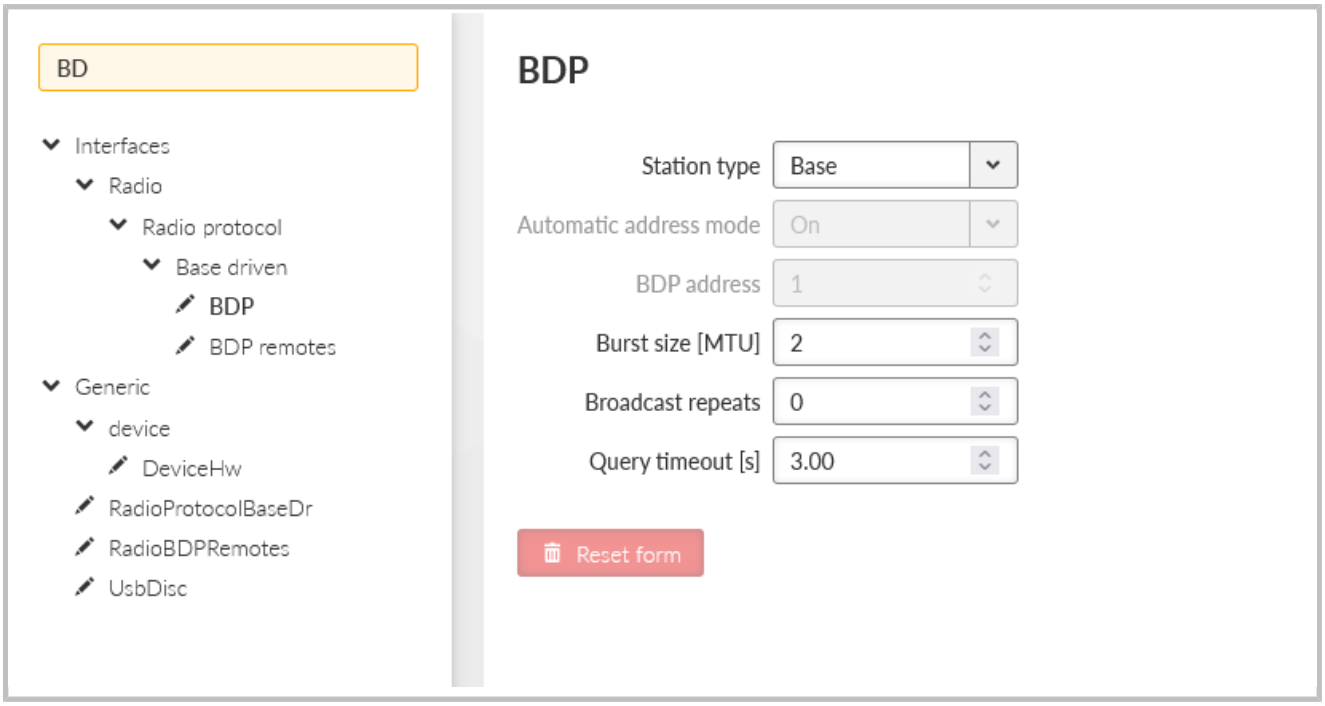


Fig. 7.64: ADVANCED > Search

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 overview information about individual sections of the unit. Each section is linked with an area of Events (see Section 8.4, *"Events"*).

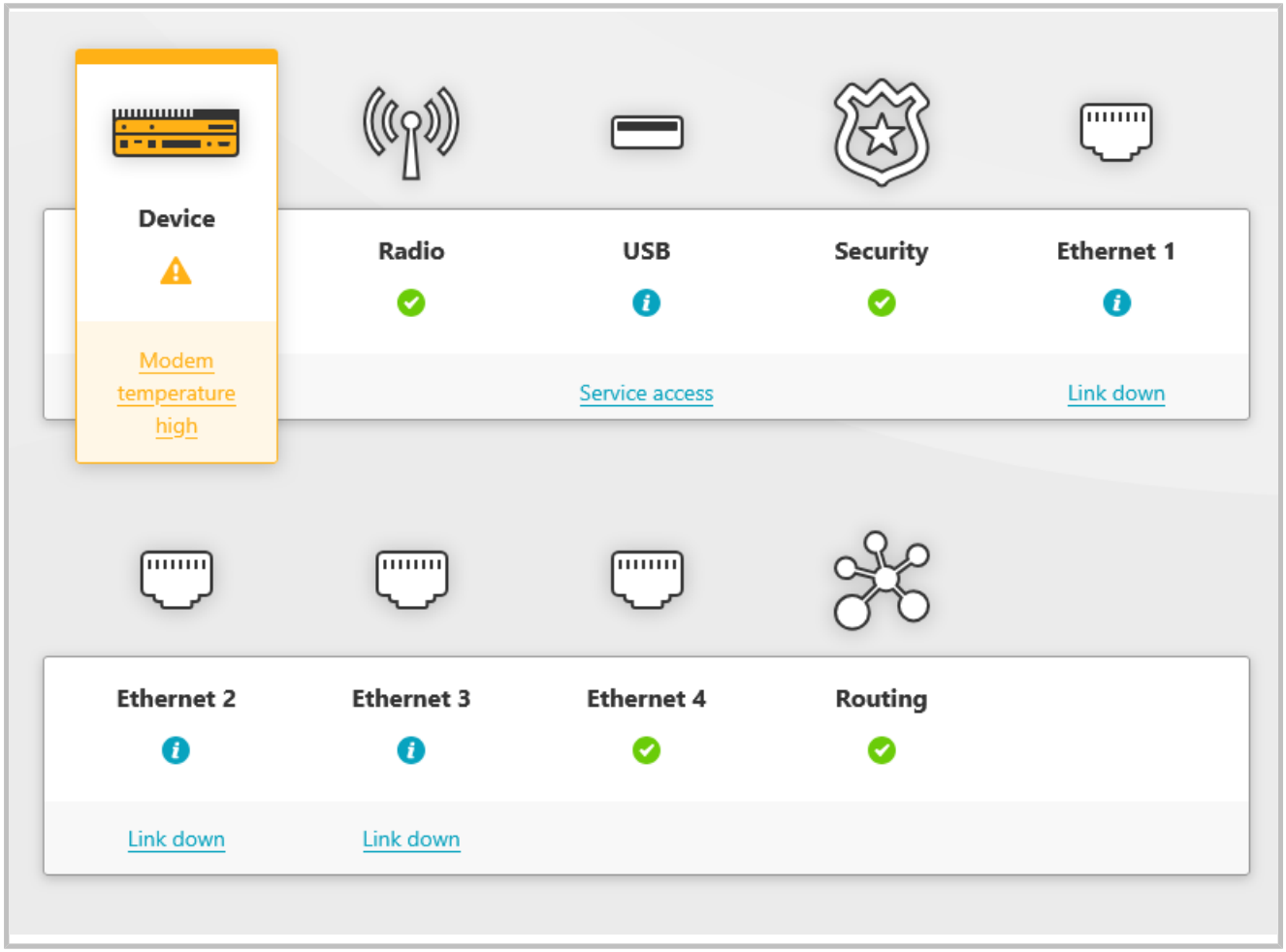


Fig. 8.1: STATUS

When any event with severity higher than Notice occurs in the unit, corresponding icon will change the color according to the severity of the event, the link leads to further information about the event in the DIAGNOSTICS menu. 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 page.

Tab. 8.1: Unit section icons

	Device
	Radio

	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

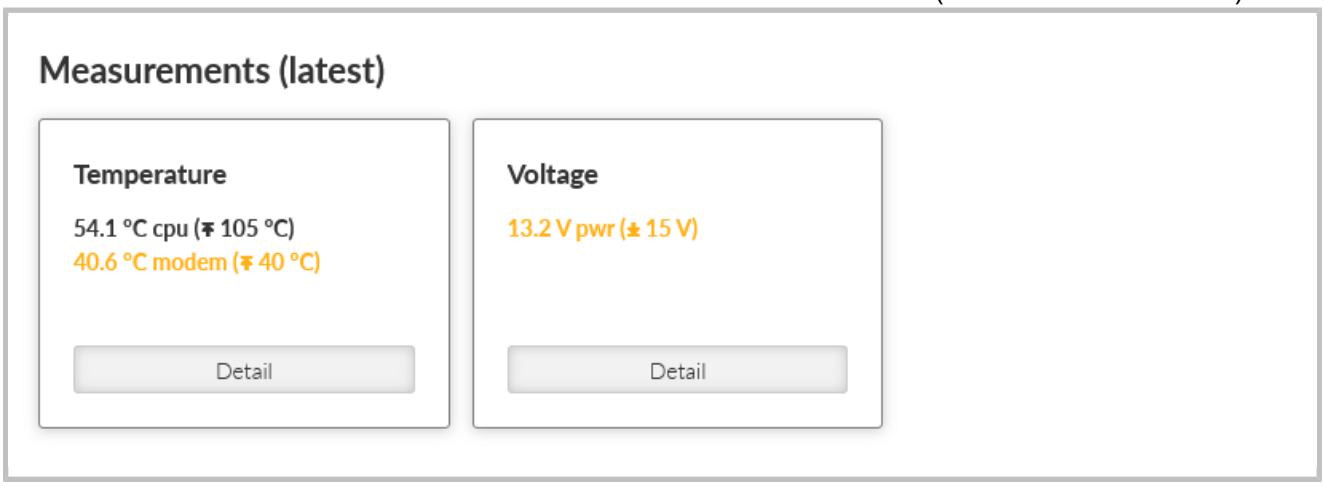
	Unit works flawlessly
	Informational, Notice
	Warning
	Error, Critical, Alert, Emergency

8.2. Overview

The Overview section serves to give general information about the RipEX2.

8.2.1. Measurements

Section Overview - Measurements contains current data measurement (obtained from sensors).



- Card Temperature - provides data about temperature (on CPU, modem and radio).

Note

If the temperature exceeds its specified range (-45 – +95 °C), the radio receiving/transmitting will be blocked. If the temperature will return to a specified range (-40 – +85 °C), the radio starts receiving/transmitting again.

This feature can be disabled in parameters ADVANCED > Interfaces > Radio > Radio parameters > Block radio in extreme temperatures.

- Card Voltage - provides data about voltage measured on input connector.

Arrow-headed symbols (↑, ↓, →) have following meaning:

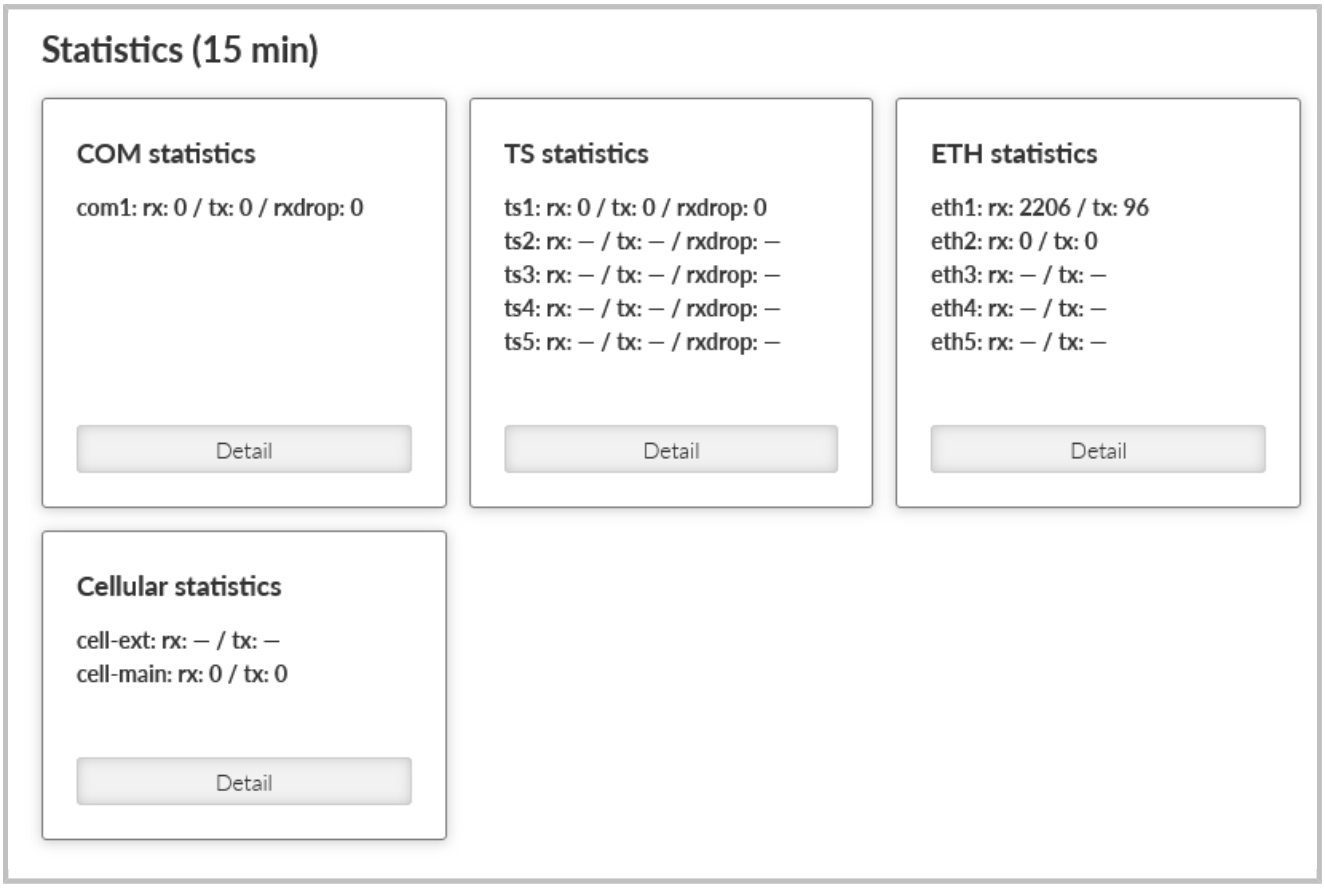
- ↑ - Maximum-limit value. An alarm is triggered, when the value (displayed in brackets) is exceeded.
- ↓ - Minimum-limit value. An alarm is triggered, when the value falls under the value, which is displayed in the brackets.
- →- Value is supposed to head to another one.

Note

Value measurements are collected once per 10 s (excluding radio interface, where values can be collected once per 10 s or more often – depends on the radio communication character).

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).



- 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. 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 npi, loop, ag, ip6tnl, etc.) are displayed in this section.

8.3.1.1. Ethernet Interfaces

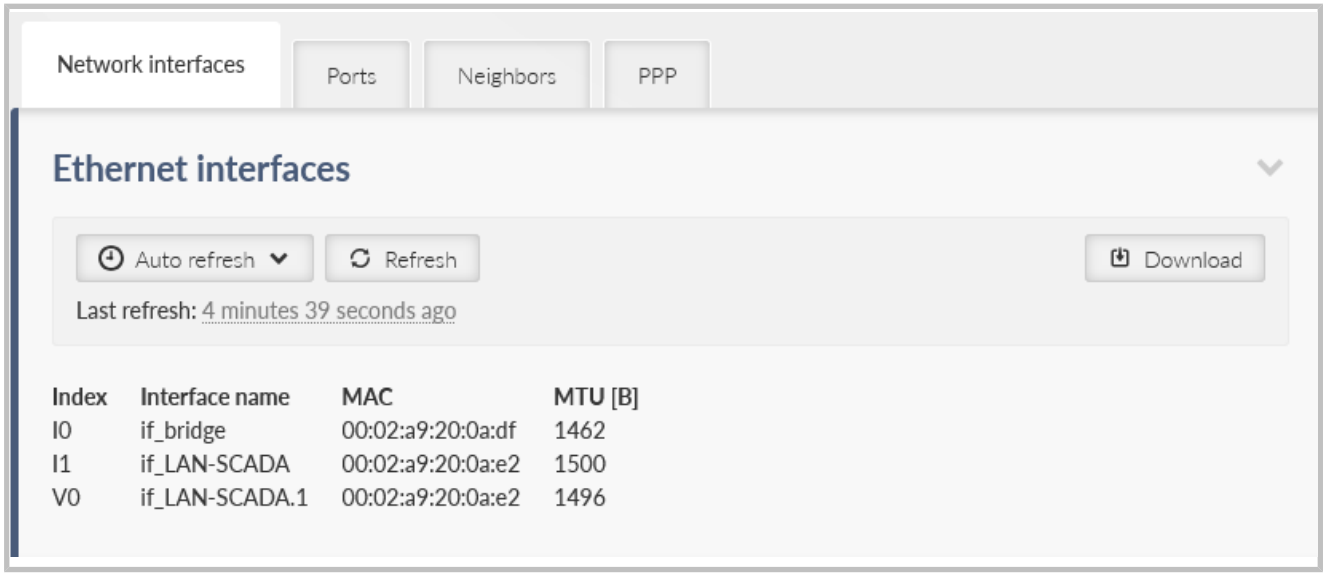


Fig. 8.2: DIAGNOSTICS > Information > Interfaces > Ethernet

Interfaces used in RipEX2 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)

8.3.1.2. Network Interfaces

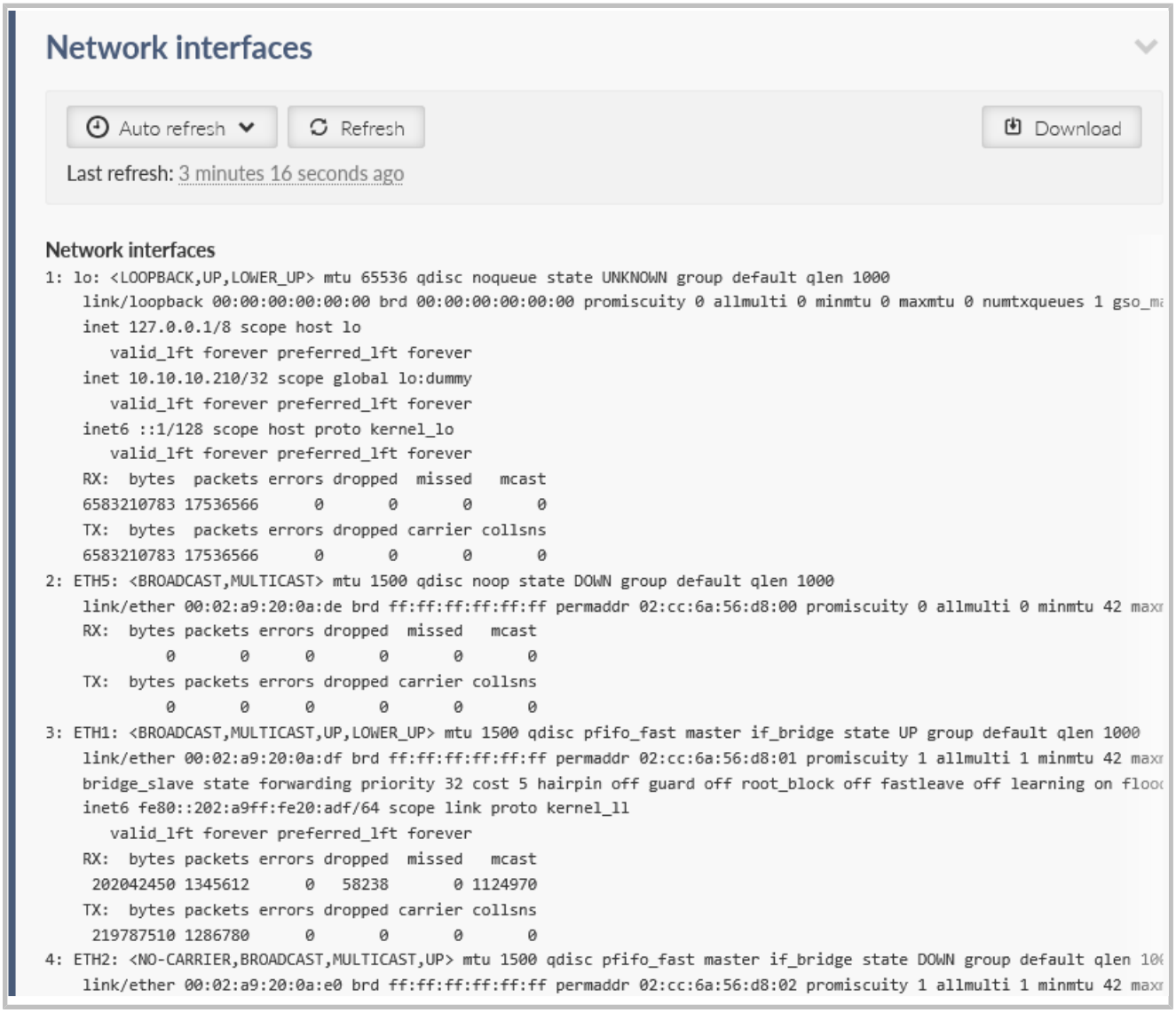


Fig. 8.3: DIAGNOSTICS > Information > Interfaces > Ethernet

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

hstdby
Switched Hot standby LAN interface – only in the active HS unit – used for traffic switched by HS unit, RI-L3 type of interface (SETTINGS > Interface > Radio)

radio
RF radio interface

- BP-L2 interface type when Bridge mode of Radio interface is used (SETTINGS > Interface > Radio)

- BP-L2 interface type when Bridge mode of Radio interface is used (SETTINGS > Interface > Radio)

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).

8.3.1.3. Neighbors

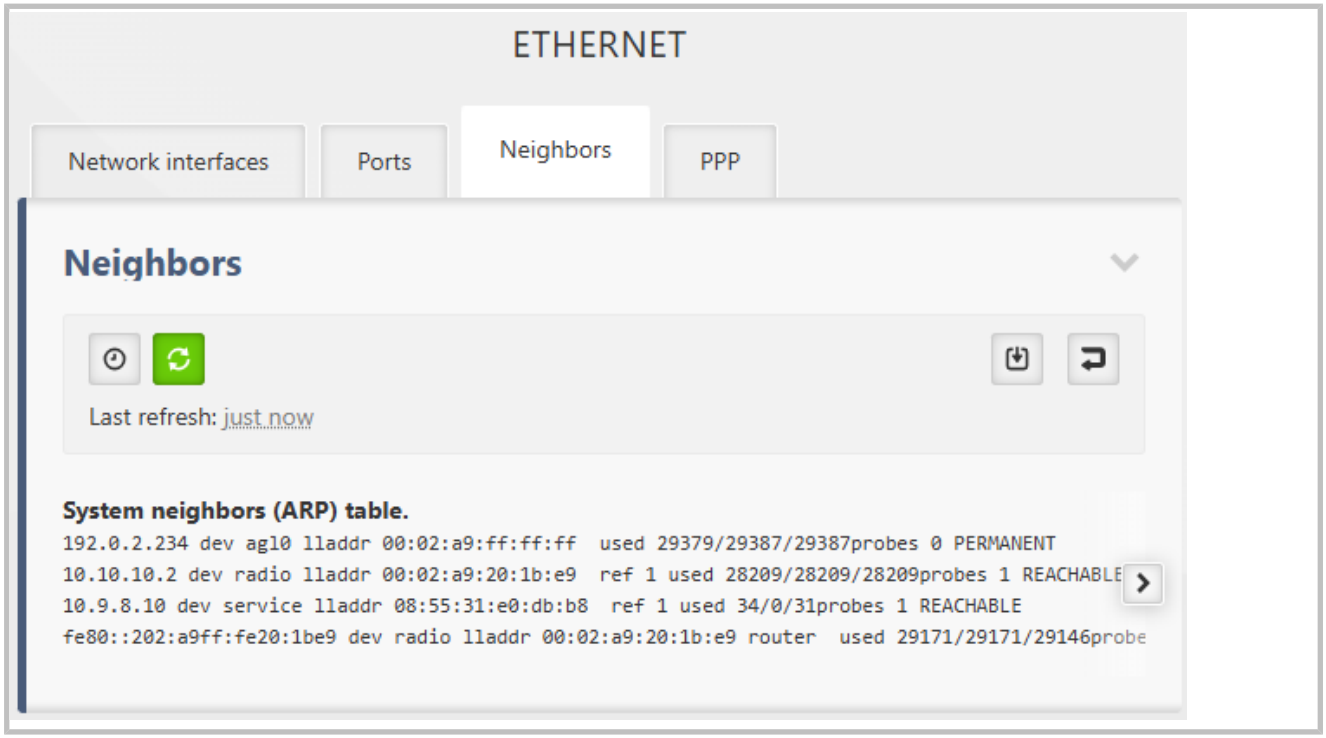


Fig. 8.4: DIAGNOSTICS > Information > Interfaces > Ethernet > Neighbors

The Neighbors tab displays the current System neighbors (ARP) table on the IP layer. The data presented here is the direct output of the internal Linux command "ip -s neigh show".

The ARP cache table provides a mapping between the Network Layer (IP addresses) and the Link Layer (MAC addresses).

8.3.1.4. Radio interface



Fig. 8.5: DIAGNOSTICS > Information > Interfaces > Radio

8.3.1.5. Cellular interfaces

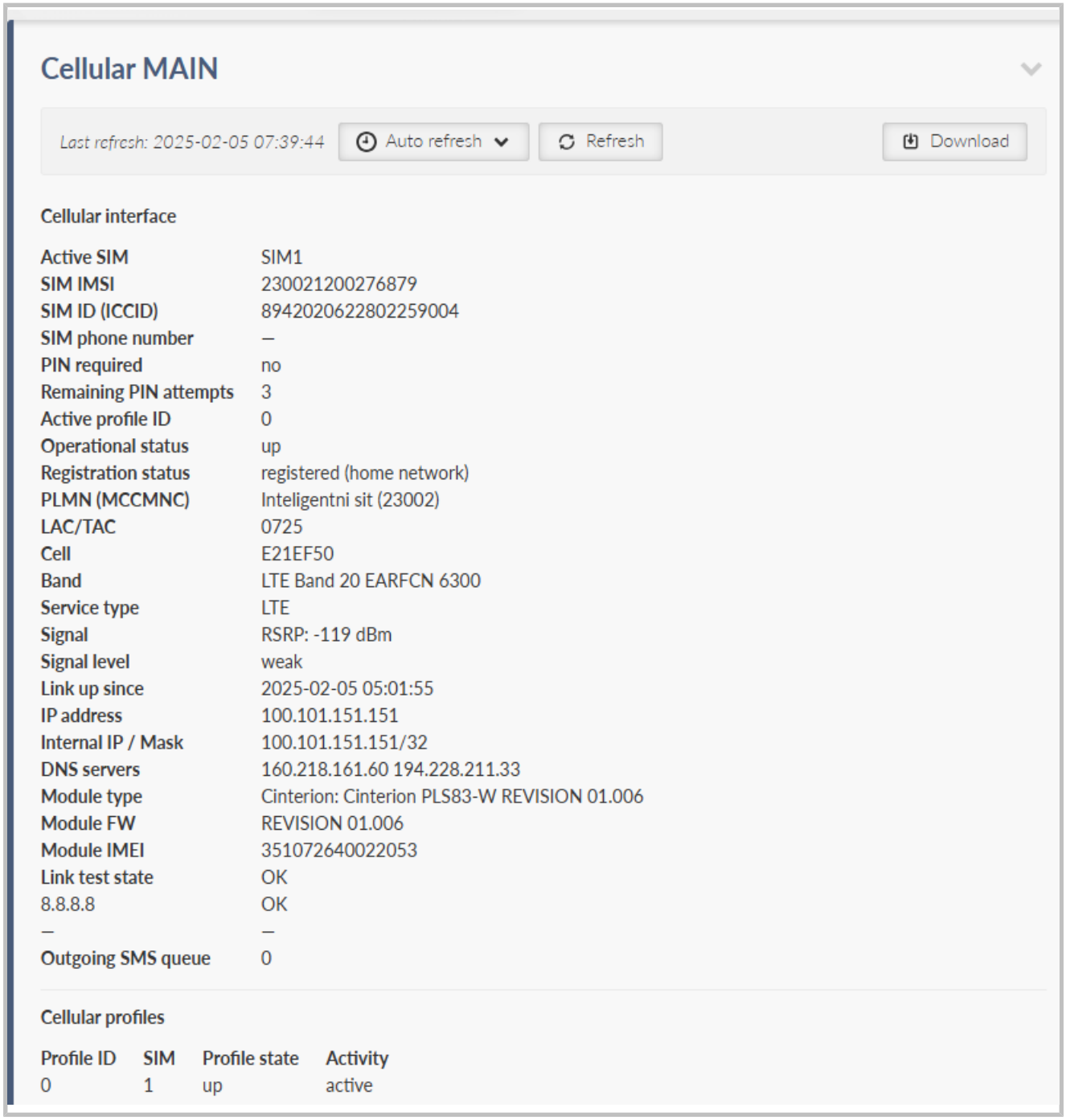


Fig. 8.6: DIAGNOSTICS > Information > Interfaces > Cellular

Active SIM
Currently used SIM

SIM IMSI
International Mobile Station Identity of the active SIM

SIM ID (ICCID)
Integrated Circuit Card ID of the active SIM

SIM phone number
SIM phone number, if it is stored in the SIM

PIN required
Whether the SIM you are currently using requires a PIN

Remaining PIN attempts
Remaining number of attempts to enter the PIN into the SIM

Active profile ID
ID of the SIM profile currently in use

Operational status
Connection status

Registration status
Registration status

PLMN (MCCMNC)
Provider name and PLMN of the connected network

LAC/TAC
LAC (2G, 3G) or TAC (4G, LTE Cat. M/NB) of the location to which the module is connected

Cell
ID of the cell

Band
Band used. Not filled in for 2G
Always added ARFCN (2G), UARFCN (3G) or EARFCN (4G, LTE Cat. M/NB) - channel number

Service type
Connected service

Signal
Current signal strength

Signal level
Current signal strength level

Link up since
The timestamp (with UTC) of the connection opening

IP address
IP address assigned to the interface when it is opened (from APN)

Internal IP / Mask
The IP address assigned to the interface when it is opened (internal, from the module)

DNS servers
IP addresses of DNS servers, separated by a space

Module type
Module name and manufacturer

Module FW
Module firmware version

Module IMEI
International Mobile Equipment Identity of the module

Link test state
Link testing status, if enabled

Outgoing SMS queue
SMS queued, waiting to be sent

Cellular profiles
Status of profiles

Profile ID
Profile ID in the profile table

SIM
SIM used by the profile

Profile state
Latest profile status

Activity
Whether the profile is currently active

8.3.1.6. PPPoE client

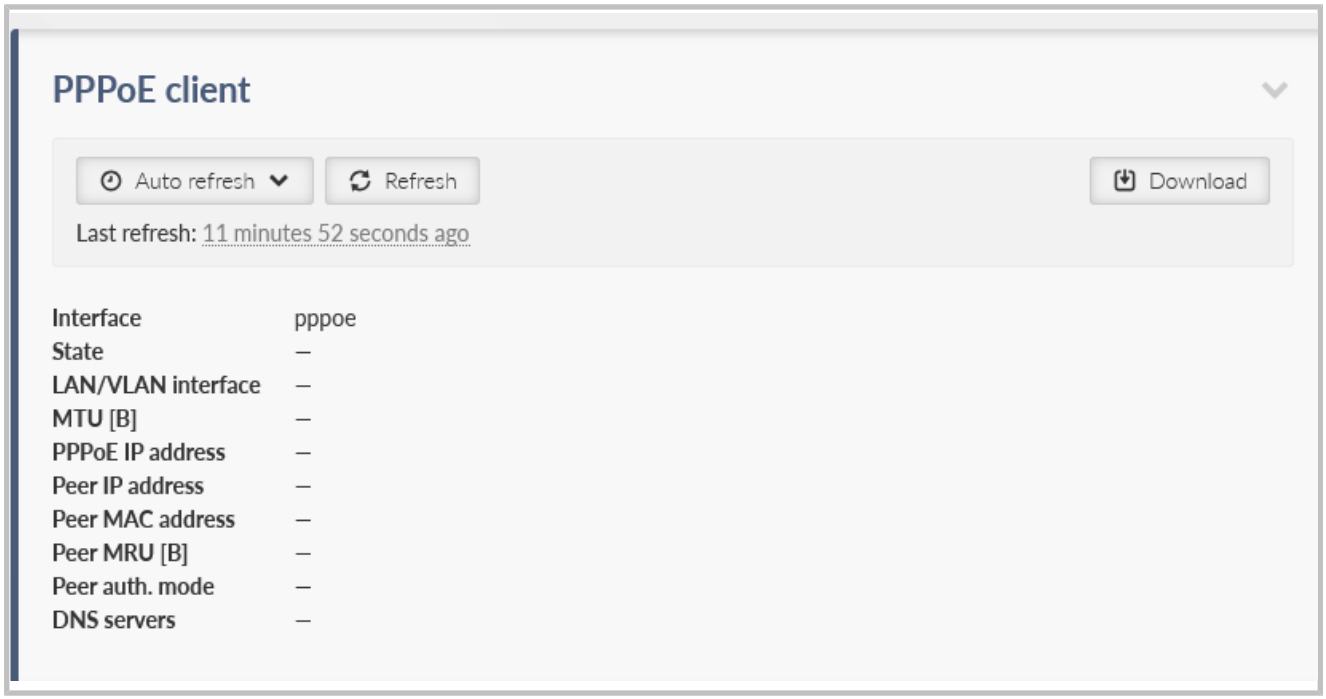


Fig. 8.7: DIAGNOSTICS > Information > Interfaces > PPPoE client

Interface PPPoE interface name

State	Current state of the interface
LAN/VLAN interface	Name of the LAN/VLAN interface on which the PPPoE client is running
MTU [B]	MTU of the LAN/VLAN interface on which the PPPoE client is running
IP address	Assigned IP address
Peer IP address	IP address of the peer (server)
Peer MAC address	MAC address of the peer (server)
Peer MRU [B]	Maximum Receive Unit (MRU) in bytes requested by the negotiating peer
Peer auth. mode	Authentication protocol requested by the peer
DNS servers	IP addresses of DNS servers, separated by a space

8.3.1.7. Wi-Fi

Provides a detailed info about Wi-Fi Access point and connected Wi-Fi clients.

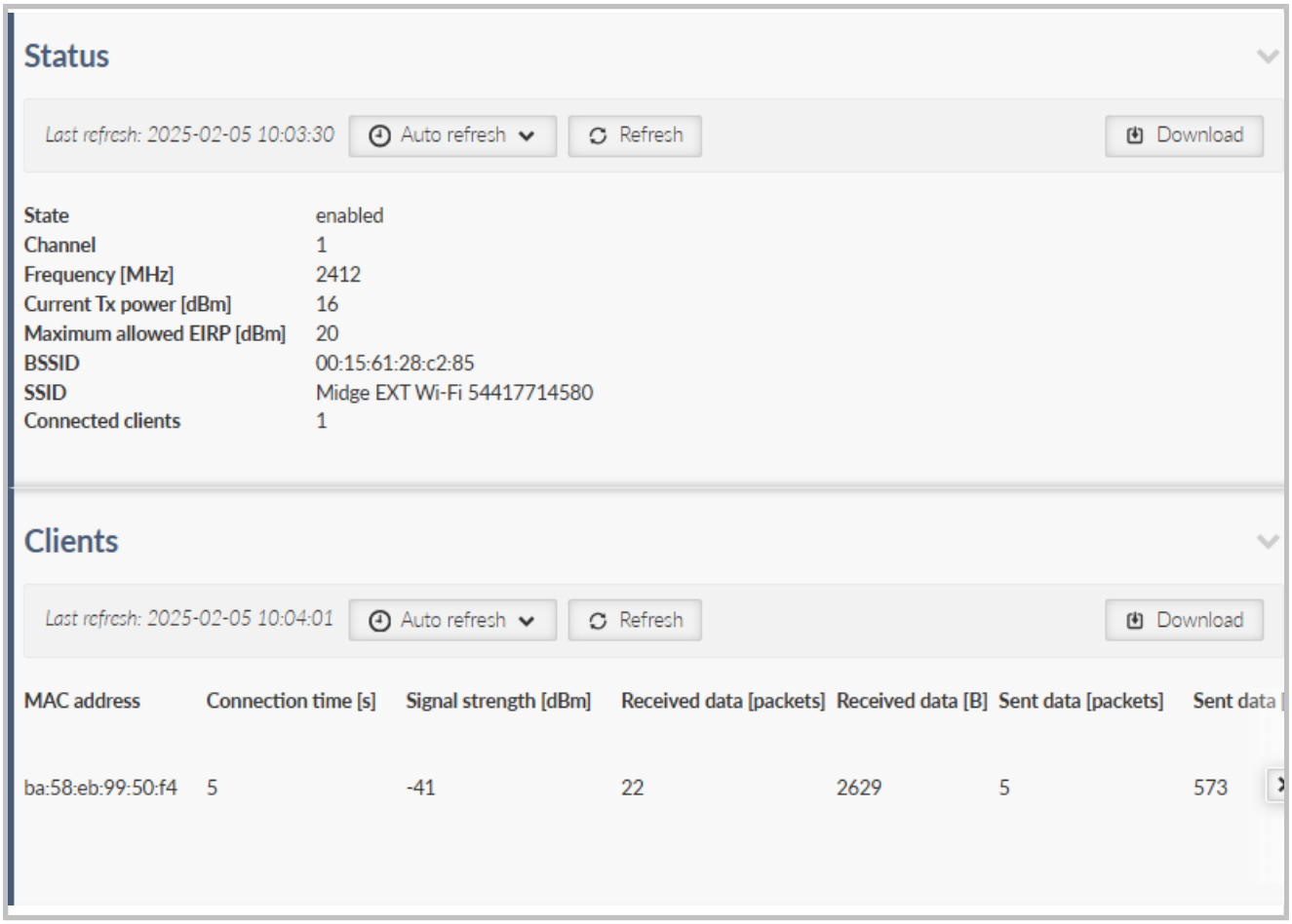


Fig. 8.8: DIAGNOSTICS > Information > Interfaces > Wi-Fi

8.3.2. Routing

Provides information about data extract from section Routing.

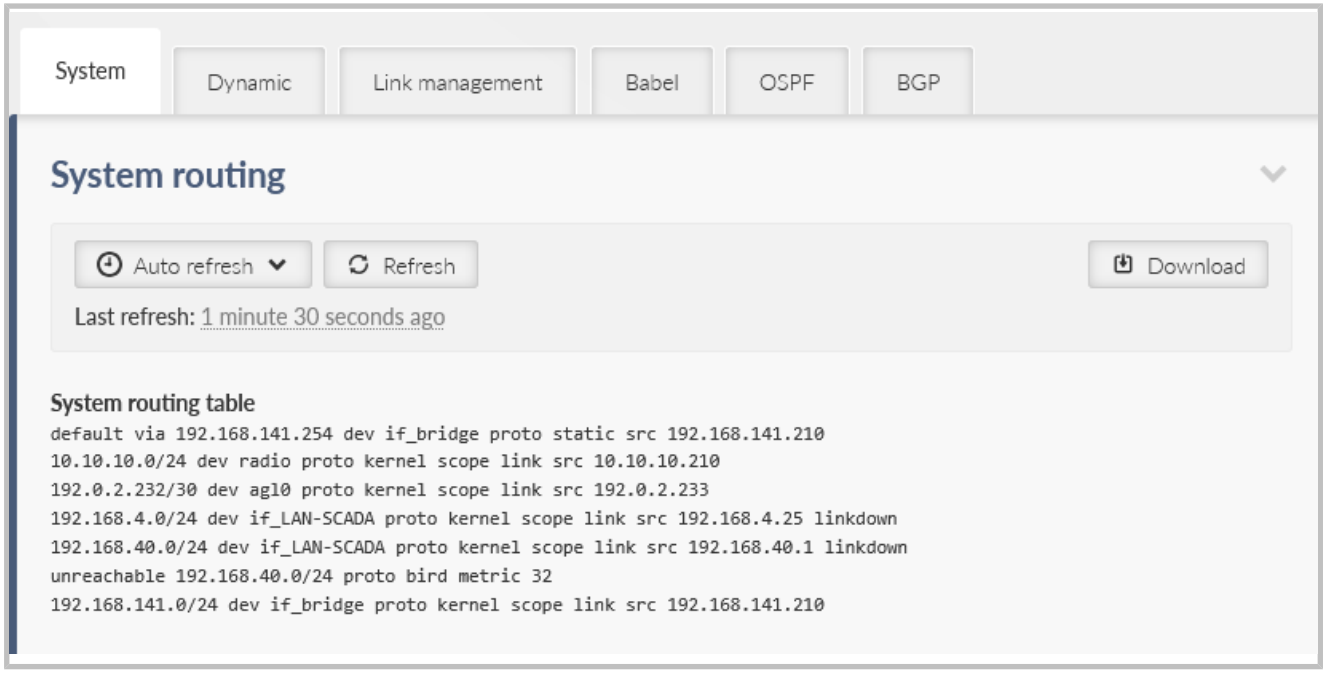


Fig. 8.9: DIAGNOSTICS > Information > Routing

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”.



Fig. 8.10: DIAGNOSTICS > Information > Firewall > L2

8.3.3.2. Firewall L3

Displays data called by following linux commands “iptables -nvL --line-numbers”.

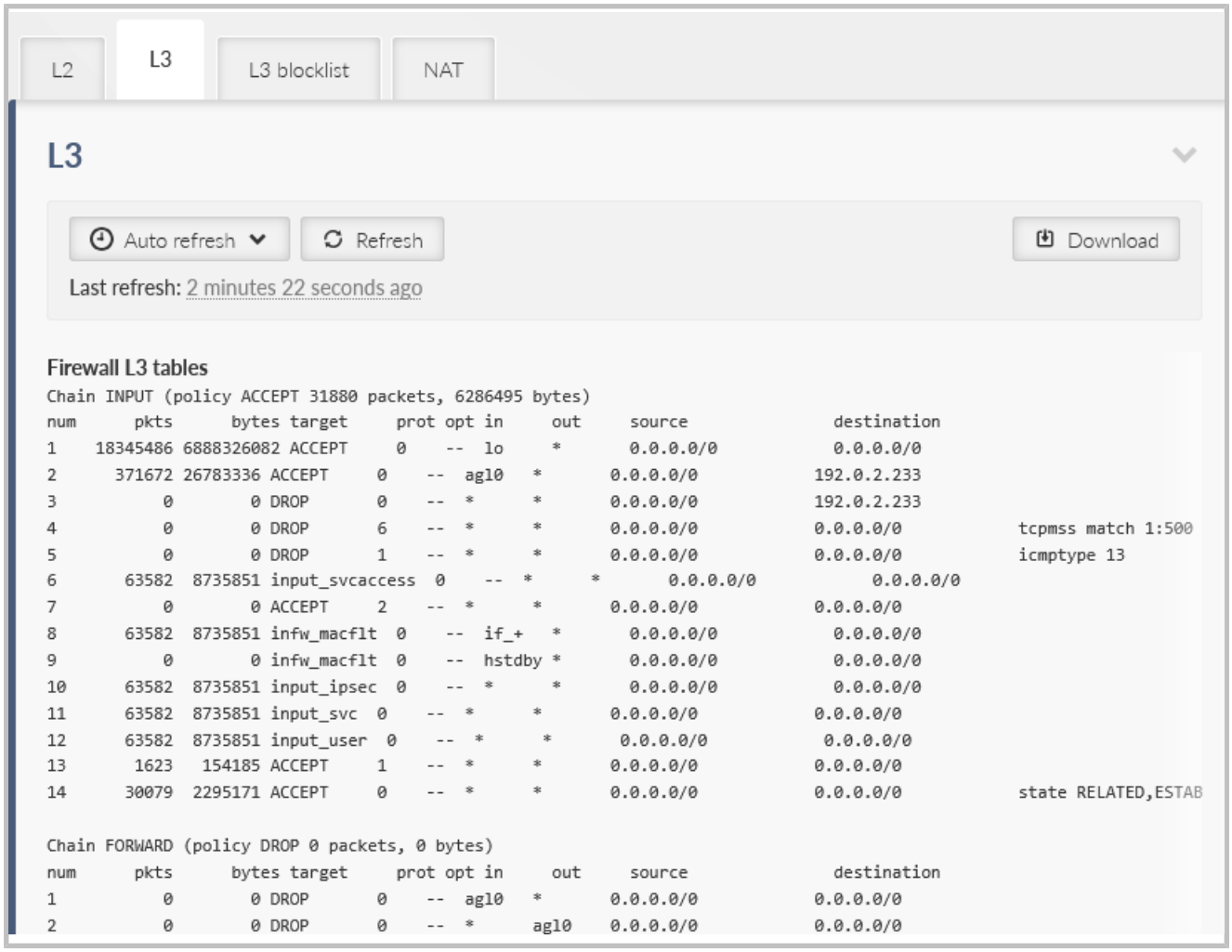


Fig. 8.11: DIAGNOSTICS > Information > Firewall > L3

8.3.3.3. Firewall L3 blocklist

Listing of the list of banned addresses. Addresses are added to the list if the Action: “Deny, Add to Blocklist” (adding the source address of the incoming packet to the banned list) is configured in the Firewall L3 - Input rules

8.3.3.4. 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

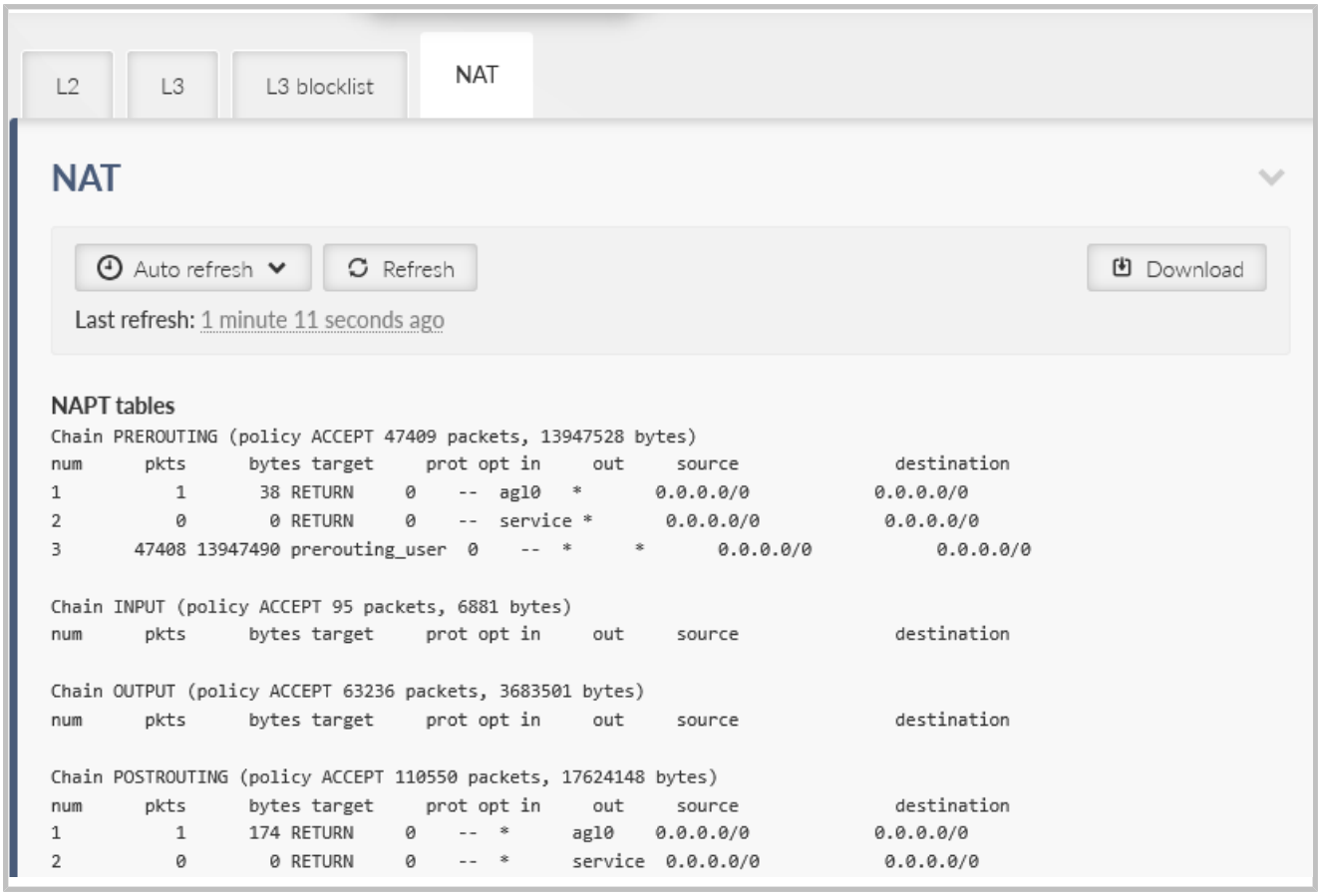


Fig. 8.12: DIAGNOSTICS > Information > Firewall > NAT

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”.

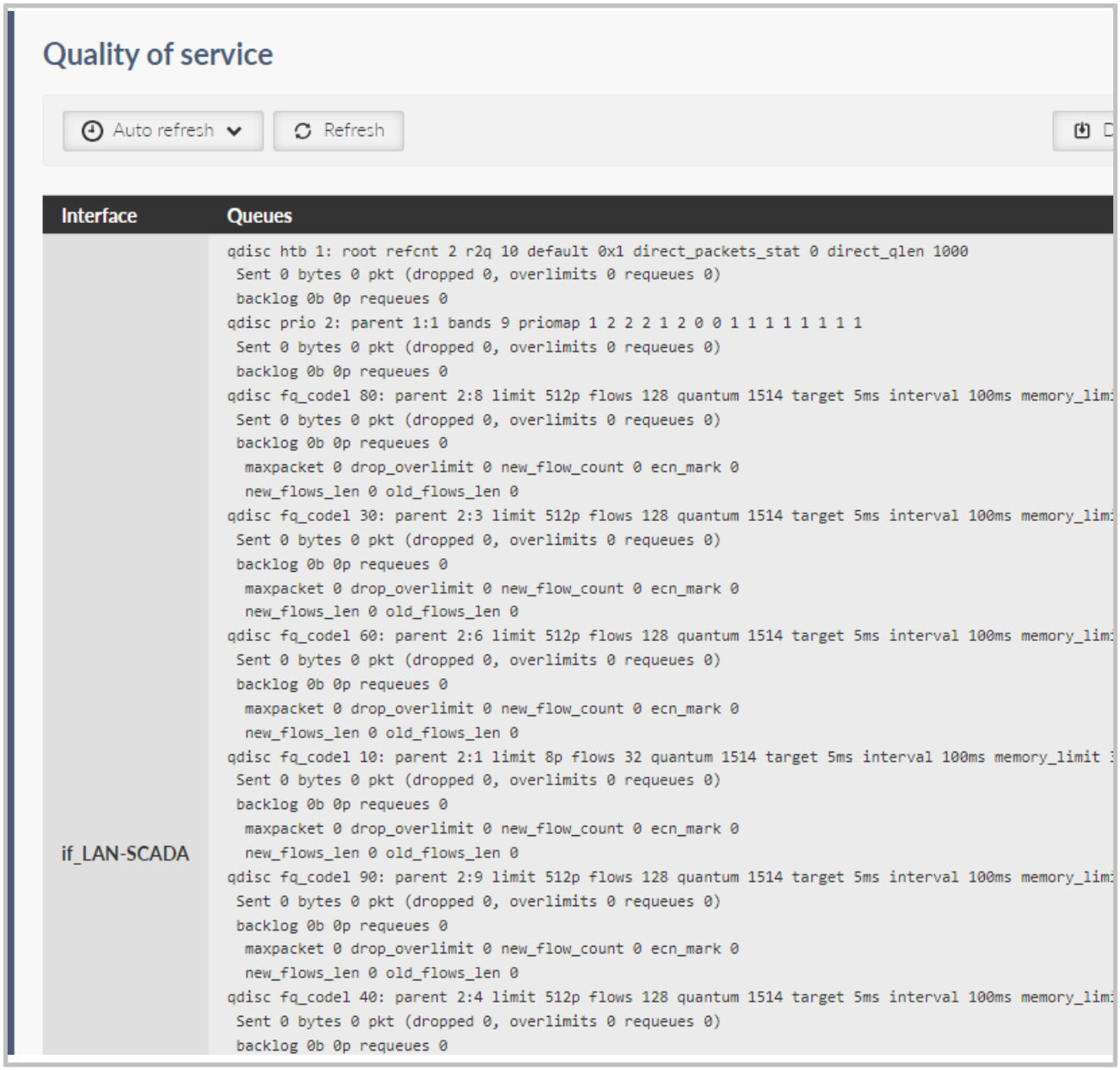


Fig. 8.13: DIAGNOSTICS > Information > Quality of service

8.3.5. DHCP servers

List of addresses assigned by the DHCP server.

IP address The assigned IP address of the client

MAC address MAC address of the client

Lease until The time when the lease expires

8.3.6. SNMP

Listing the Engine ID value. The Engine ID is used to uniquely identify the station when communicating with the SNMP manager.



Fig. 8.14: DIAGNOSTICS > Information > Services > SNMP

8.3.7. Syslog

Listing the message counters to a remote Syslog server.



Fig. 8.15: DIAGNOSTICS > Information > Services > Syslog

8.3.8. SMS

Provides information about sent and received SMS messages.

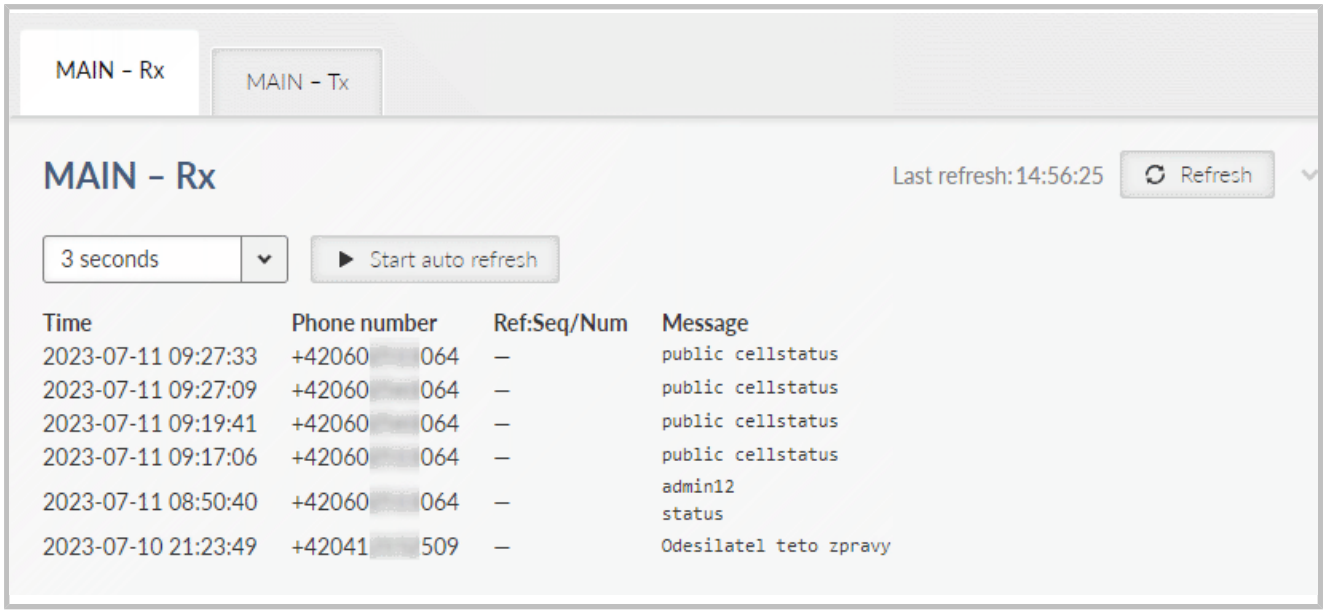


Fig. 8.16: DIAGNOSTICS > Information > SMS > MAIN - Rx

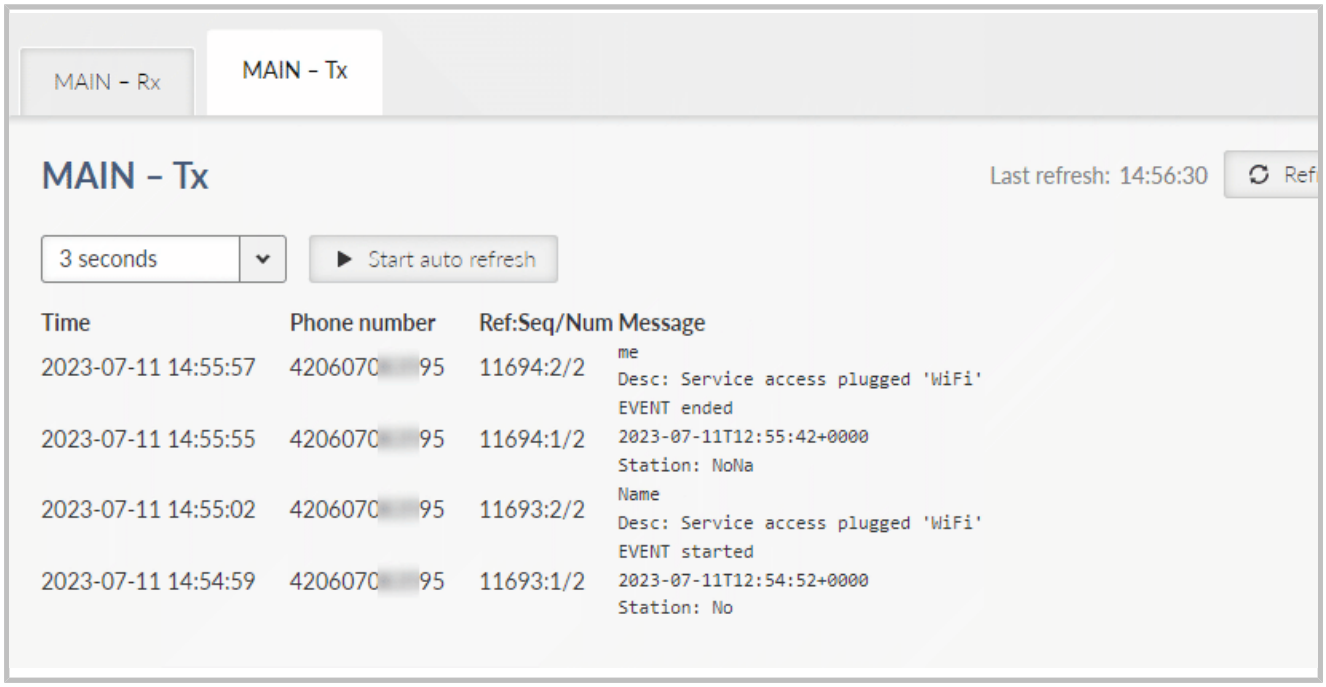


Fig. 8.17: DIAGNOSTICS > Information > SMS > MAIN - Tx

8.3.9. Device

Provides general information about the unit (device).



Fig. 8.18: DIAGNOSTICS > Information > Device

8.3.9.1. 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.

8.3.9.2. Advanced information

Additional unit information is provided which might be requested for advanced diagnostics. Partial description:

- Modem board SN - Modem boards system number.
- Radio board SN - Radio boards system number.
- Radio SW version - Current radio software.
- CNF version - Version of the unit configuration. Configuration version is updated if the new firmware version brings major configuration changes leading to incompatibility with the previous configuration. See *Section 7.6.2, "Configuration"* for more details.
- Web client version - Version of the current web client.
- Region ID - If the unit is delivered with certain limits applied according to a specific Region (specified when ordering a new unit), the specific Region identification is visible here. No limits are applied if the Region ID is empty ("---").

- Region description - Detailed description of the Region (if active).

8.3.10. 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. Maximum size depends on the amount of radio links contained in the statistics. 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.

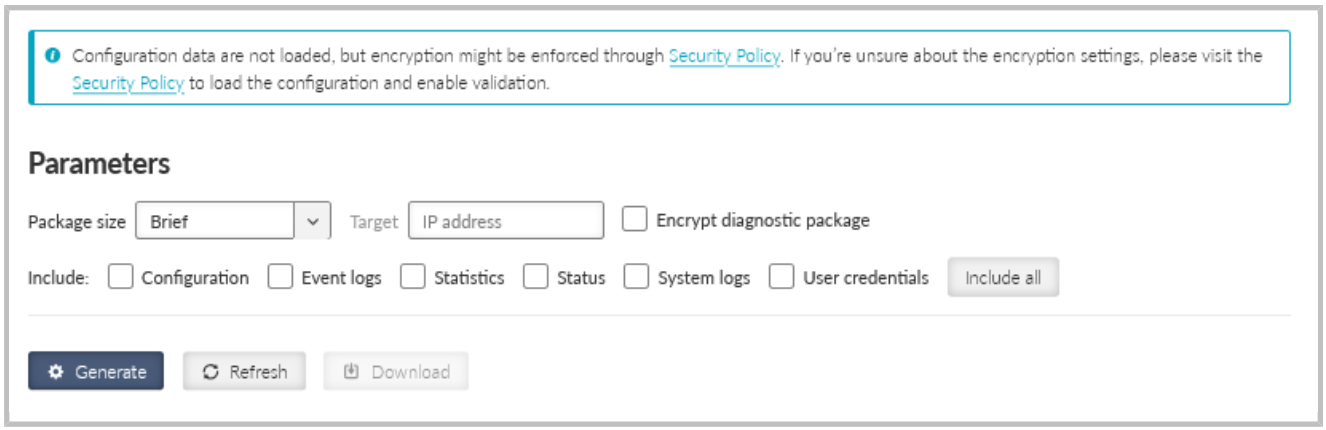


Fig. 8.19: DIAGNOSTICS > Information > Diagnostic package

Package size
List box {Brief; Detailed}, default = "Brief"
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.

Encrypt diagnostic package
Allows generating of the diagnostic package as an encrypted .zip file. The rules for the password complexity are set in the SETTINGS > Security > Policy menu. In the same menu, it is possible to set encryption to always be required.

Note
You cannot use Windows Explorer for extracting the package. You need to use a software that can work with files encrypted with AES-256 algorithm (e.g. WinZip, WinRAR, 7-zip, Total commander).

Include

- Configuration - configuration of the unit is added to the package (json format)
- Event logs - adds a list of events exported to csv

- Brief: Last 50 events
- Detailed: Last 500 events

- Statistics - adds list of statistics exported to csv
  - Interval of frames statistics: 30 min
  - Brief: 10 frames
  - Detailed: 24 frames
- Status - lists detailed status of networks devices and services
- System logs - adds last system logs
  - Brief: 100 of current lines from all logs
  - Detailed: 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.

Part of the event record is also the information about action really triggered by the event. Changing the settings of a requested action or severity of the event (SETTINGS > Device > Events) does not change information about the events that have already occurred.

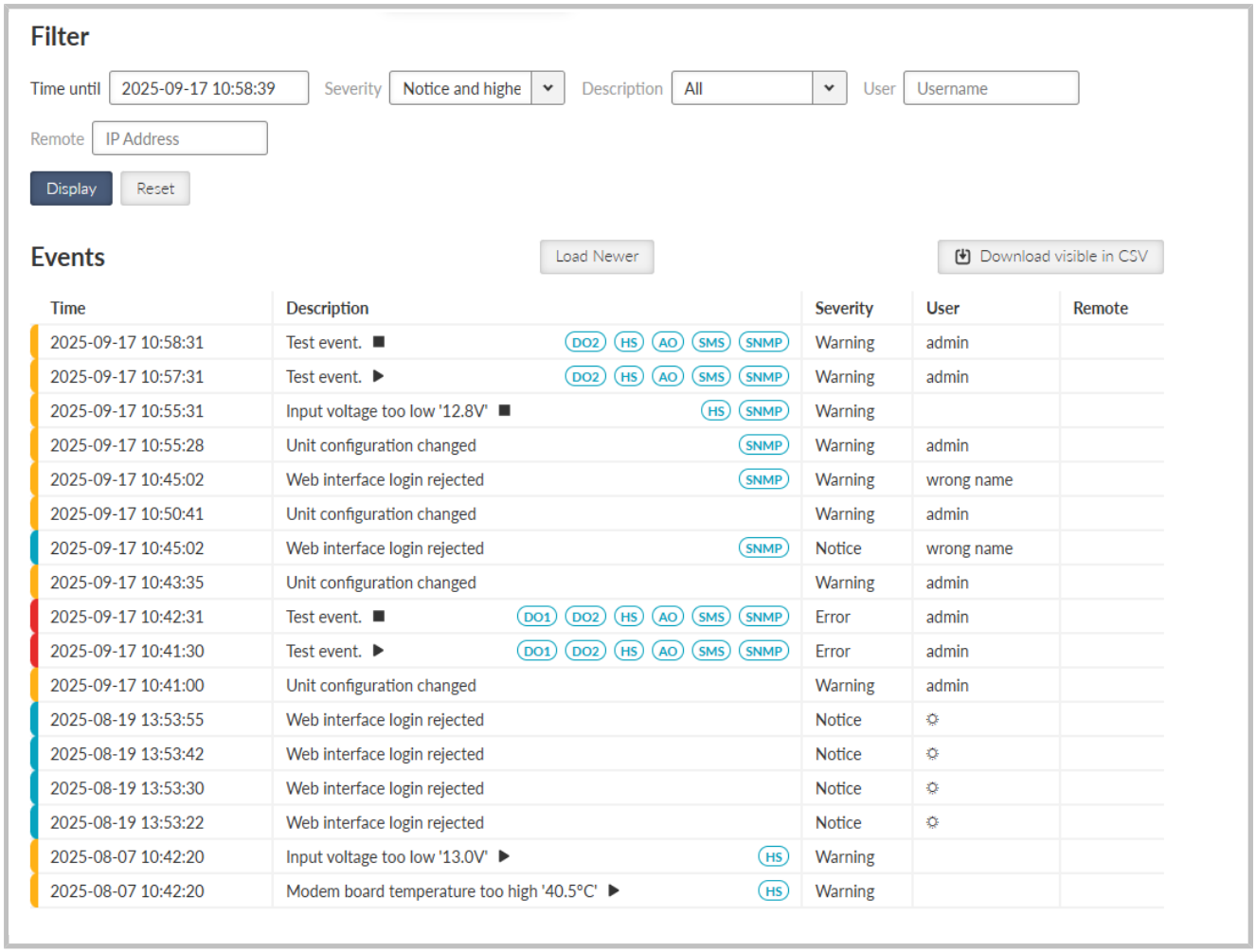


Fig. 8.20: DIAGNOSTICS > Events

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.
	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

RipEX2 unit permanently monitors various system 'channels'. There are several types of those channels: Physical interfaces (Ethernet ports, serial ports, radio interface, 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). What affects the length of available history the most is the number of radio links - how many radio “neighbors” the unit communicates with or how many of the neighboring signals are received. This is different for each unit in the network. For example Base station in a network operating Base driven protocol is the most active unit thus it has the shortest history available.

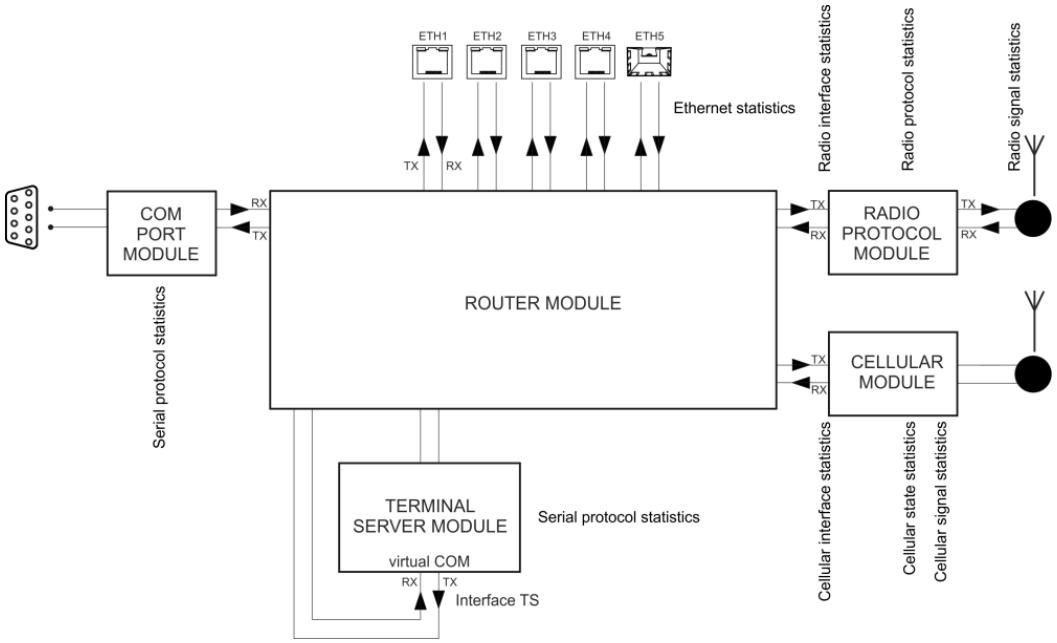


Fig. 8.21: Statistics data in the context of unit interfaces

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:

- Radio interface statistics
- Radio protocol statistics
- Radio protocol non-addressable statistics
- Radio signal statistics
- Radio signal non-addressable statistics
- Serial protocols statistics
- Ethernet statistics
- Cellular statistic (if cellular interface is available)
- Measurements

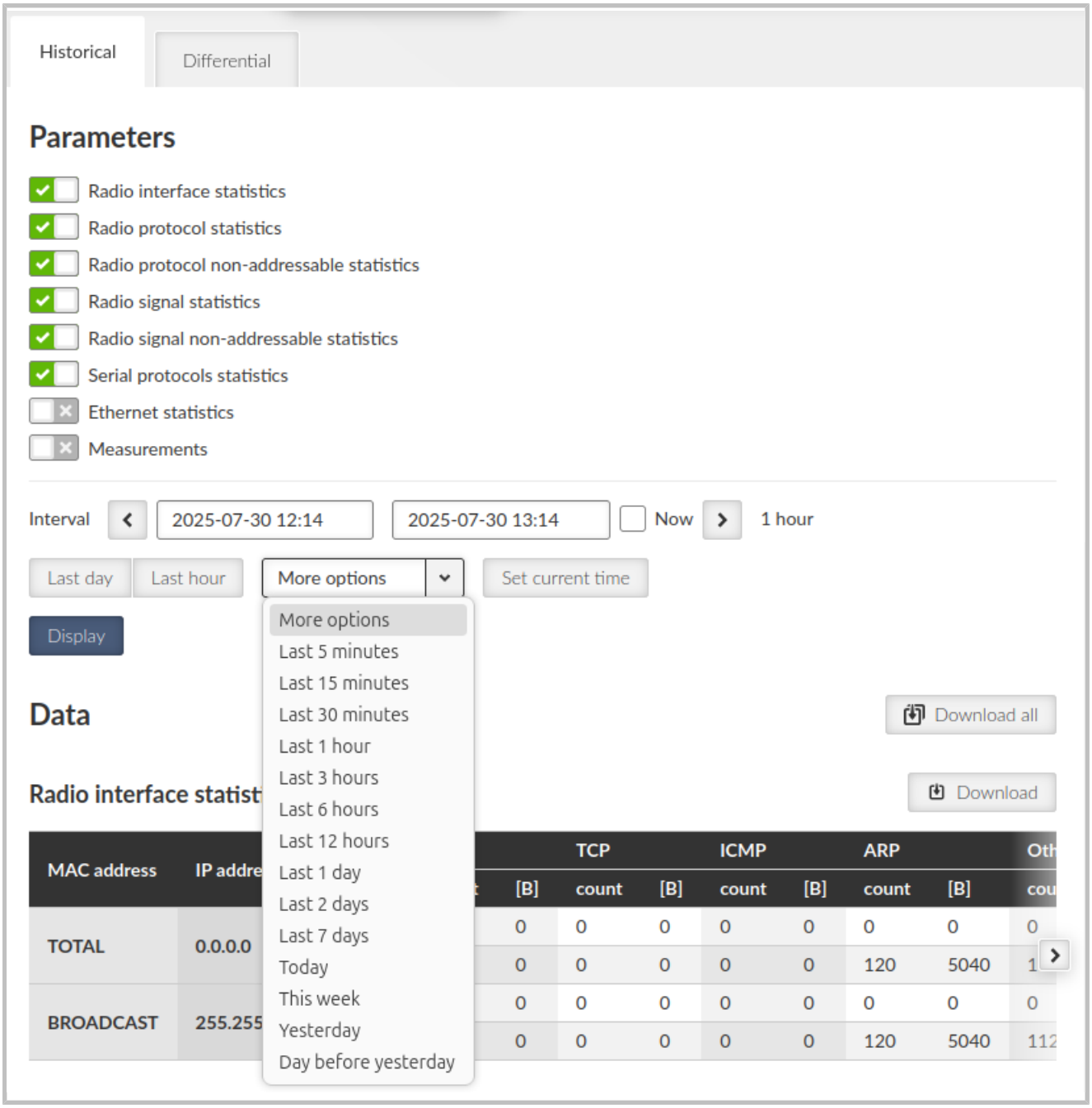


Fig. 8.22: DIAGNOSTICS > Statistics

“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 (over the radio channel) 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. Radio interface statistics

Radio interface statistics provides set of data monitoring the interface between the Router module (IP routing engine in the unit) and the Radio protocol module. It corresponds to monitoring Radio - Router.

Tx direction: from the Router module to the Radio protocol module. Rx direction: from the Radio protocol module to the Router module.

Data

Download all

Radio interface statistics

Download

MAC address	IP address		UDP		TCP		ICMP		ARP		Other
			count	[B]	count	[B]	count	[B]	count	[B]	count
TOTAL	0.0.0.0	Rx	10161	915385	0	0	74	17497	29	1218	14640
		Tx	10229	929507	0	0	15	2665	1823	76566	16987
00:02:a9:20:1b:e9	10.10.10.2	Rx	10161	915385	0	0	74	17497	29	1218	14640
		Tx	10229	929507	0	0	15	2665	10	420	95
BROADCAST	255.255.255.255	Rx	0	0	0	0	0	0	0	0	0
		Tx	0	0	0	0	0	0	1813	76146	16978

MAC address - MAC address of the IP packet. Source for Rx or destination for Tx packets.

IP address – translated MAC address when available. Address 0.0.0.0 is used as a placeholder if the translation is not available. If the Transparent protocol is used, the translation is not available at all.

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).

Other – Packets not handled by the previous counters (e.g. VLAN, services, GRE, IPsec (ESP), ...)

8.5.3. Radio protocol statistics

Radio protocol statistics provides set of data monitoring the radio channel access protocol frames and events. It corresponds to monitoring Radio - Interface.

Frames which are not addressed to/from this unit are not handled (they do not affect any counter).

Rx direction: from the 'air' radio interface to the Radio protocol module. Tx direction: from the Radio protocol module to the radio interface.

Data

Download all

Radio protocol statistics

Download

Link address	IP address		Frame OK	Frame err	Frame dupl		Packet rej	Ctrl frames	Total
			Frame OK	Frame lost	Frame rep	Frame rej	Packet rej		count
TOTAL	0.0.0.0	Rx	156667	0	0	–	0	10332	16699
		Tx	181927	17	103	0	12	10320	19236
:20:1B:E9	10.10.10.2	Rx	156667	0	0	–	0	10332	16699
		Tx	10332	17	103	0	0	10320	207
:FF:FF:FF	255.255.255.255	Rx	0	0	0	–	0	0	0
		Tx	171595	0	0	0	12	0	17159

Link address – Link address of the frame. Source for Rx or destination for Tx frames. This is a Link address assigned at the origin (input) - when entering, or at the target (output) - when leaving the radio network.

In case of Base driven protocol or Transparent protocol, this address pair is not modified when re-translated. As a result of this fact, the whole traffic to a remote station behind the re-translation is counted together in a line assigned to the remote station.

For the Link address:

In case of Base driven protocol - the Protocol address is used

IP address – translated MAC address when available. Address 0.0.0.0 is used as a placeholder if the translation is not available. If the Transparent protocol is used, the translation is not available at all.

Frame OK (Rx) – Correctly received data frames count.

Frame OK (Tx) – Correctly send data frames count. Control frames are not included. When ACK is on, only acknowledged frames are included. Re-translated data frames are not included.

Frame err (Rx) – Received corrupted data frames count (CRC error)

Frame lost (Tx) – Transmitted unacknowledged frames count. It happens when ACK is on and acknowledging frame was not received even when full number of re-transmission attempts was reached.

Frame dupl (Rx) – Received, but dropped, duplicated data frames count. 'Duplicated' frames are repeatedly received acknowledged frames.

Frame rep (Tx) – Repeated frames count (they can appear when ACK is on). Re-translated frames are not included.

Frame rej (Tx) – Rejected frames count (rejected just before transmission) – reason: buffer timeout. In case of Transparent protocol (Bridge mode) it happens when there is a collision during re-translation.

Packet rej (Rx) – Correctly received but rejected packets count - reason: impossible to decrypt or decompress.

Packet rej (Tx) – Rejected packets count (rejected before handed over to the transmitter) – reason: buffer overflow, buffer timeout.

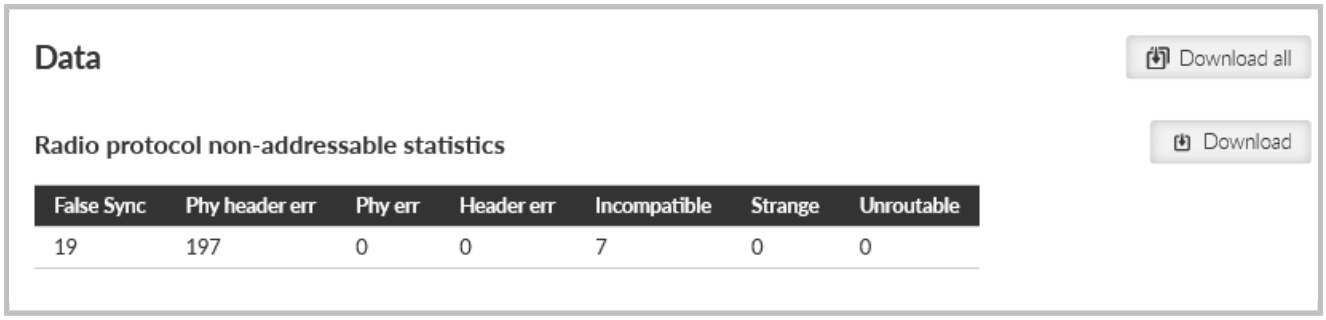
Ctrl frames (Rx, Tx) – Received / transmitted control frames count.

Total (Rx) – Received frames count and amount of data in Bytes. Amount of data - for both Rx and Tx - is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

Total (Tx) – Transmitted frames count and amount of data in Bytes. Re-translated frames are included.

8.5.4. Radio protocol non-addressable statistics

Radio protocol 'non-addressable' statistics provides set of data monitoring the radio channel access protocol frames and events which cannot be linked with any address (e.g. broadcasts). It corresponds to monitoring Radio - Interface.



False Sync – False synchronization incidents count

Phy header err – Packet reception failure count - reason: sub header error

Phy err – Packet reception failure count - reason: physical layer analysis error

Header err - Packet reception failure count - reason: header content error or CRC error.

Incompatible – Received incompatible frames count - reason: different radio protocol

Strange – Received unexpected frames count - reason: wrong addresses, wrong sequence etc. Valid for Base Driven Protocol only.

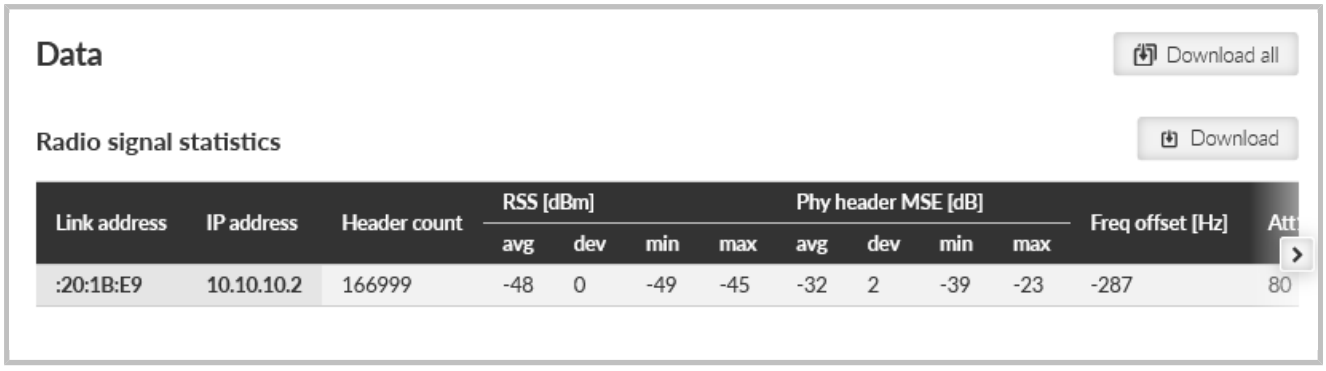
Unroutable – Packets counter which were scheduled for transmission but impossible to be forwarded to the Radio protocol - multiple reasons: e.g. the destination IP address is not known

8.5.5. Radio signal statistics

Radio signal statistics provides set of data monitoring the radio interface quantities and events. It corresponds to monitoring Radio - Interface.

Statistic data are collected by the frame source address - Link address, which is an address of the originating radio transmitter (unlike "Radio protocol statistics" where the Link address is an address of the unit where the packet entered the RipEX2 network).

There is a special address 'RELAY' to indicate frames coming from the re-translation unit in case of Base Driven Protocol operation.



Header count – Received headers count

RSS [dBm] – Radio Signal Strength - measured within the header reception

avg / dev / min / max – average / standard deviation / minimum / maximum

Phy header MSE [dB] – modulation Mean Squared Error - measured within the header reception

Freq offset [Hz] – Averaged frequency offset between the transmitter and the receiver station, measured by the receiver station.

Att1 [%] - First internal attenuator (15 dB) activated. Shown in percents of affected frames.

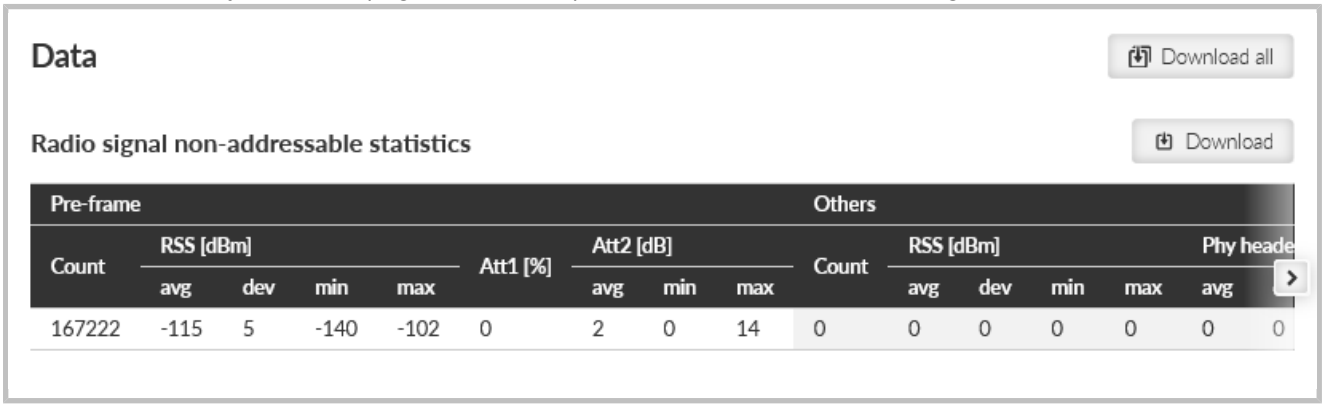
Att2 [dB] – Value of the 2nd internal attenuation applied (0 - 31 dB).

Data count – Received complete frames (including data part) count. Frames with valid header CRC, but wrong data CRC are not counted

Data MSE [dB] - modulation Mean Squared Error - measured within the frame data part reception

8.5.6. Radio signal non-addressable statistics

Radio signal statistics provides set of data monitoring the radio interface quantities and events. This table contains measurements handled before the frame reception and measurements which cannot be linked with any address (e.g. broadcasts). It corresponds to monitoring Radio - Interface.



Pre-frame									Others						
Count	RSS [dBm]				Att1 [%]	Att2 [dB]			Count	RSS [dBm]				Phy heade	
	avg	dev	min	max		avg	min	max		avg	dev	min	max	avg	
167222	-115	5	-140	-102	0	2	0	14	0	0	0	0	0	0	0

Pre-frame – Values based on measurements handled before the frame reception

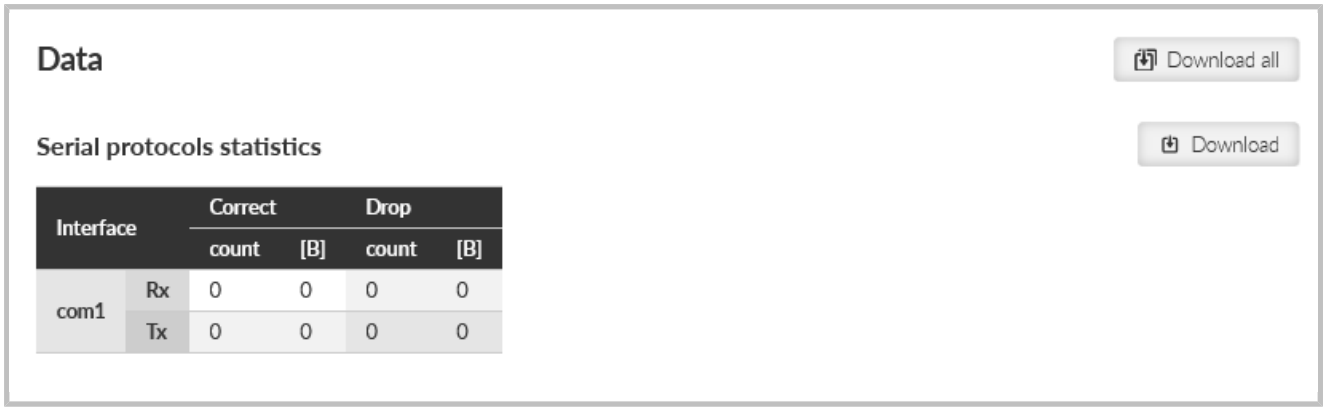
RSS [dBm] – Radio Signal Strength - measured short time just before the frame reception

Others – Values for frames which cannot be linked with any address

8.5.7. 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 RipEX2 unit (i.e. from the COM port module or Terminal server module to the Router module). Tx direction: from the RipEX2 unit to the external device.



Interface		Correct		Drop	
		count	[B]	count	[B]
com1	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).

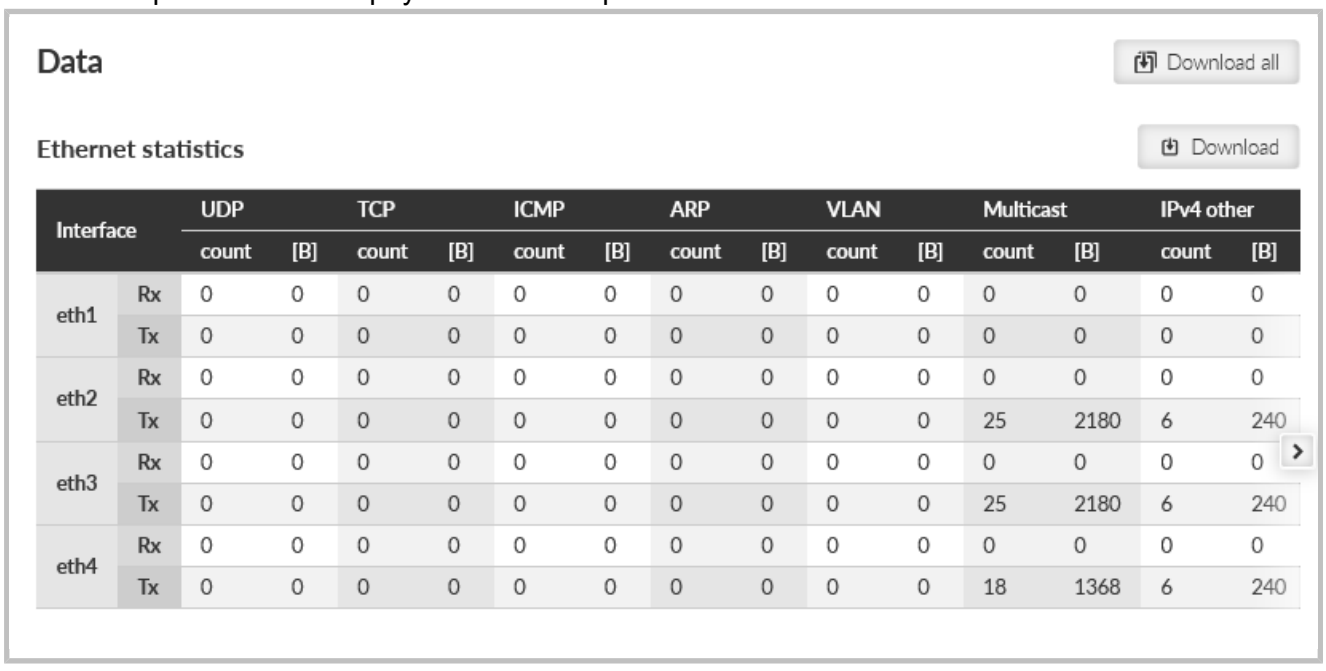
Drop (Rx, Tx) - Dropped received / transmitted packets - reason: corrupted frame, CRC error, wrong protocol message, unsupported protocol message.

8.5.8. 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 RipEX2 unit (i.e. to the Router module). Tx direction: from the RipEX2 unit to the physical Ethernet port.



Interface		UDP		TCP		ICMP		ARP		VLAN		Multicast		IPv4 other	
		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
	Tx	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
	Tx	0	0	0	0	0	0	0	0	0	0	25	2180	6	240
eth3	Rx	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	25	2180	6	240
eth4	Rx	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	18	1368	6	240

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.

8.5.9. Cellular statistics

Cellular statistics are available for optional extension module if used.

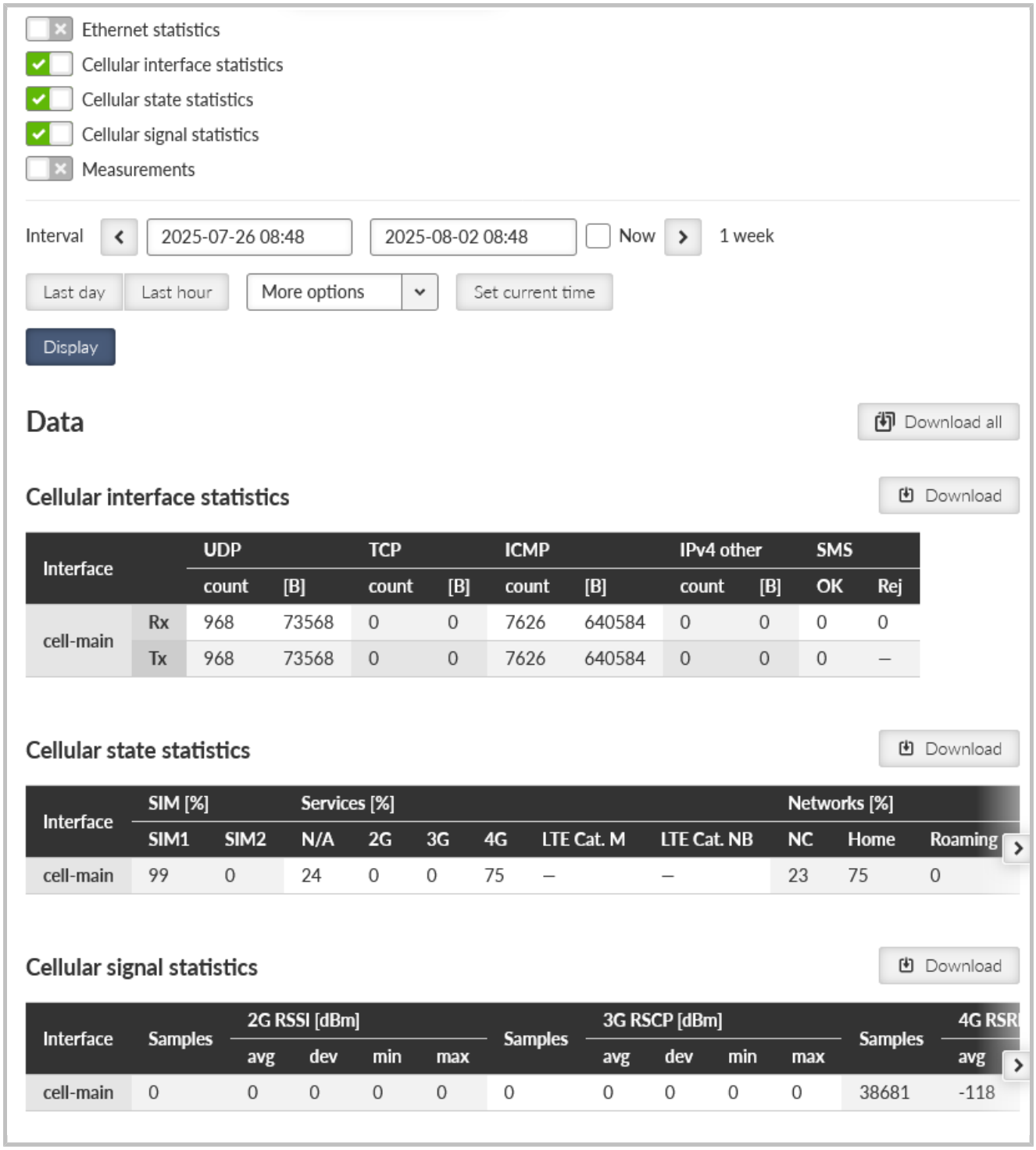
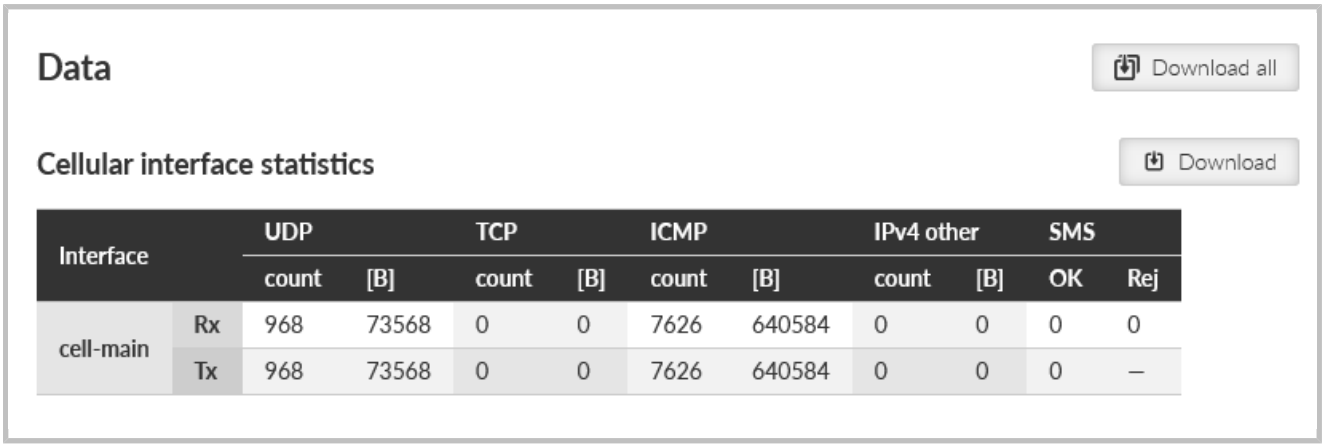


Fig. 8.23: DIAGNOSTICS>Statistics

8.5.9.1. 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.



Interface		UDP		TCP		ICMP		IPv4 other		SMS	
		count	[B]	count	[B]	count	[B]	count	[B]	OK	Rej
cell-main	Rx	968	73568	0	0	7626	640584	0	0	0	0
	Tx	968	73568	0	0	7626	640584	0	0	0	–

Interface

– “cell-ext” interface is used for RipEX2 optional extension cellular module.

UDP, TCP, ICMP

- 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), ...).

SMS

Rx OK

Number of SMS received
SMS with the correct format, passphrase and from the correct number. Invalid commands or wrong parameters are also included here (they are correctly received by the daemon, rejected only in the command execution system).

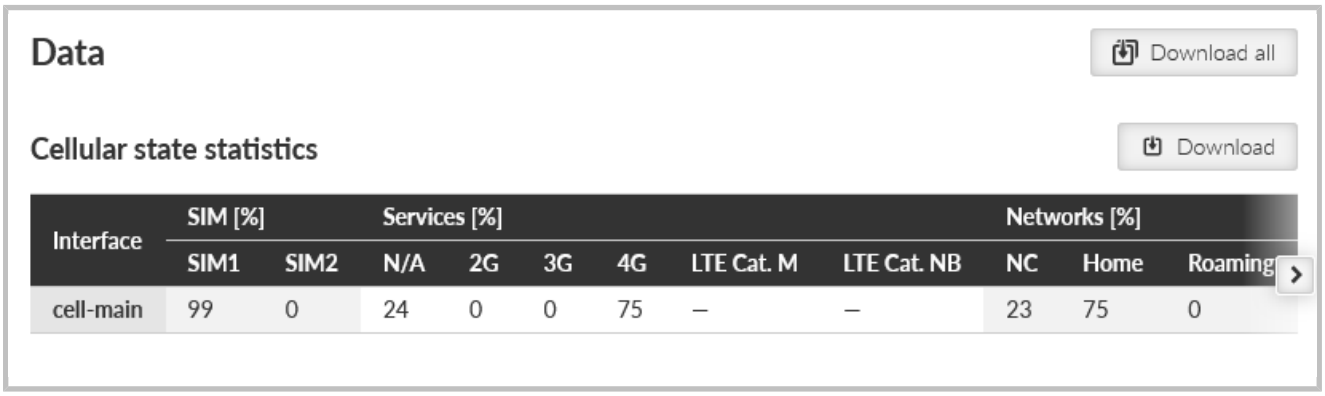
Rx Rej

Number of rejected incoming SMS
SMS. In case of disabling the reception of command SMS, all received SMS are included here.

Tx OK

Number of SMS sent

8.5.9.2. Cellular state statistics



Interface	SIM [%]		Services [%]						Networks [%]		
	SIM1	SIM2	N/A	2G	3G	4G	LTE Cat. M	LTE Cat. NB	NC	Home	Roaming
cell-main	99	0	24	0	0	75	–	–	23	75	0

Interface

– “cell-ext” interface is used for RipEX2 optional extension cellular module.

SIM [%]
– information about using the individual SIM cards during the time displayed in %.

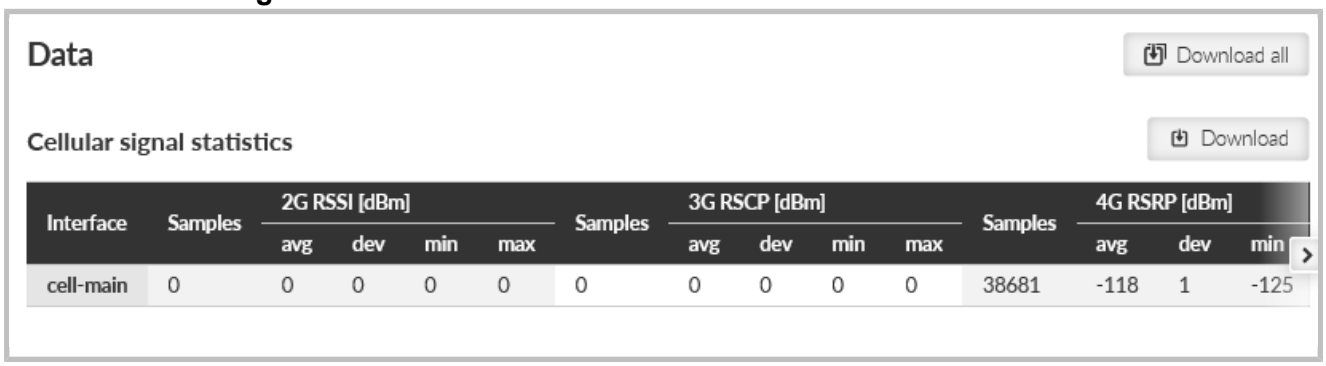
Services [%]
– N/A (not available), 2G (e.g. GPRS, EDGE), 3G (e.g. UMTS), 4G (e.g. LTE), LTE Cat. M, LTE Cat. NB services usage displayed in % of time.

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 %).

8.5.9.3. Cellular signal statistics



Interface	Samples	2G RSSI [dBm]				Samples	3G RSCP [dBm]				Samples	4G RSRP [dBm]		
		avg	dev	min	max		avg	dev	min	max		avg	dev	min
cell-main	0	0	0	0	0	0	0	0	0	0	38681	-118	1	-125

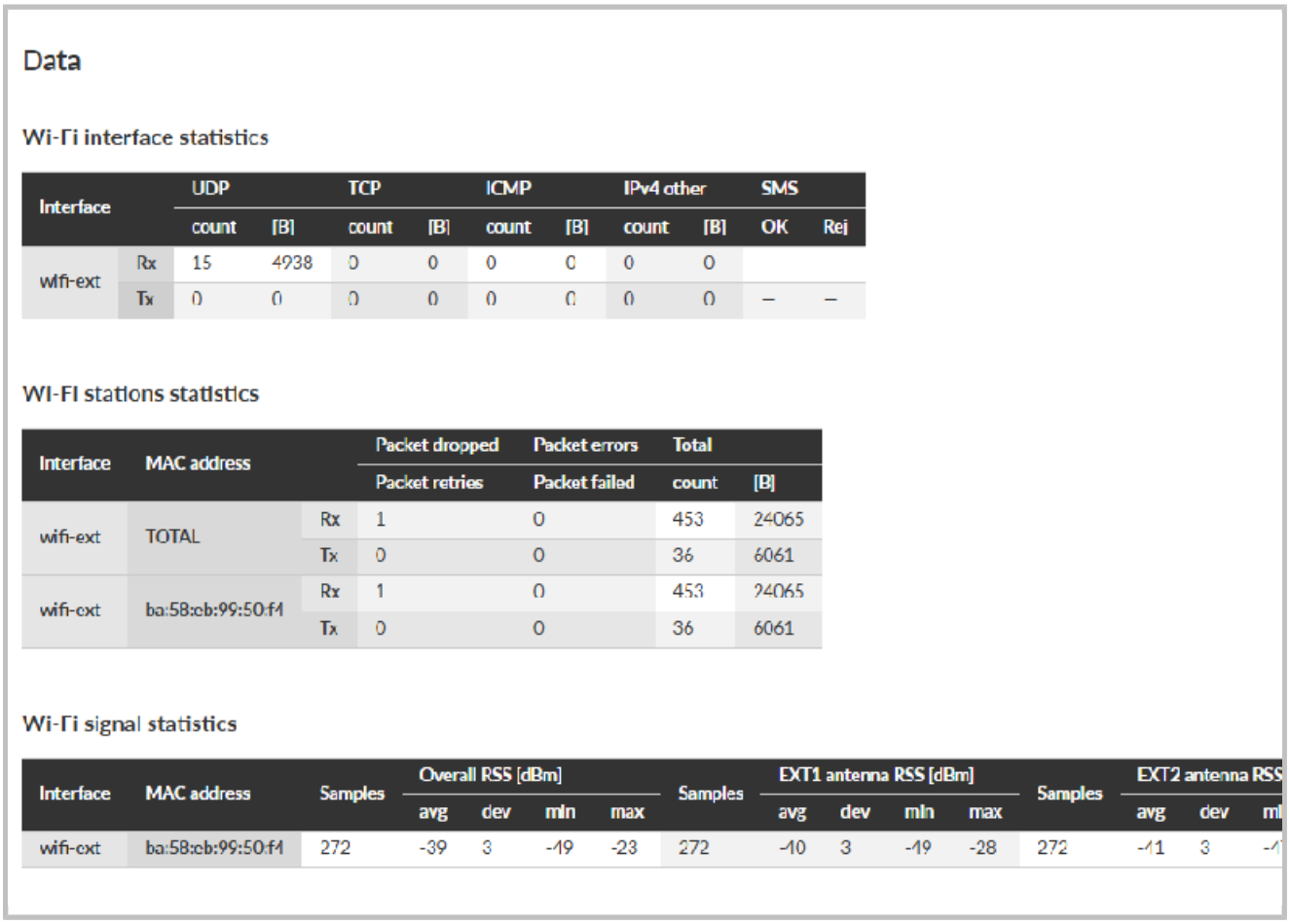
Interface
– “cell-ext” interface is used for RipEX2 optional extension cellular module

2G RSSI / 3G RSCP / 4G RSRP/ LTE Cat. M RSRP/ LTE Cat. NB RSRP
Signal levels in dBm

Samples
Number of samples used for the individual statistics

avg / dev / min / max
Average / standard deviation / minimum / maximum value

8.5.10. Wi-Fi statistics



Data

Wi-Fi interface statistics

Interface		UDP		TCP		ICMP		IPv4 other		SMS	
		count	[B]	count	[B]	count	[B]	count	[B]	OK	Rej
wifi-ext	Rx	15	4938	0	0	0	0	0	0		
	Tx	0	0	0	0	0	0	0	0	–	–

WI-FI stations statistics

Interface	MAC address		Packet dropped	Packet errors	Total	
			Packet retries	Packet failed	count	[B]
wifi-ext	TOTAL	Rx	1	0	453	24065
		Tx	0	0	36	6061
wifi-ext	ba:58:cb:99:50:f4	Rx	1	0	453	24065
		Tx	0	0	36	6061

Wi-Fi signal statistics

Interface	MAC address	Samples	Overall RSS [dBm]				Samples	EXT1 antenna RSS [dBm]				Samples	EXT2 antenna RSS		
			avg	dev	min	max		avg	dev	min	max		avg	dev	mi
wifi-ext	ba:58:cb:99:50:f4	272	-39	3	-49	-23	272	-40	3	-49	-28	272	-41	3	-4

Wi-Fi interface statistics

Interface

“wifi-ext” interface is used for RipEX2 optional extension Wi-Fi module

UDP, TCP, ICMP

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), ...)

SMS

Rx OK

Number of SMS received

SMS with the correct format, passphrase and from the correct number. Invalid commands or wrong parameters are also included here (they are correctly received by the daemon, rejected only in the command execution system)

Rx Rej

Number of rejected incoming SMS

SMS. In case of disabling the reception of command SMS, all received SMS are included here

Tx OK
Number of SMS sent

Wi-Fi stations statistics

Interface
"wifi-ext" interface is used for RipEX2 optional extension Wi-Fi module

MAC address
Statistics available for the ext interface and connected stations (by MAC address)

Packet dropped Rx
Number of packets dropped without specifying the reason

Packet errors Rx
Number of packets with FCS error

Total count Rx
Total number of packets received

Total bytes Rx
Total size of received data in bytes

Packet retries Tx
Number of repeatedly sent packets

Packet failed Tx
Number of packets sent unsuccessfully

Total count Tx
Total number of packets sent

Total bytes Tx
Total size of sent data in bytes

Wi-Fi signal statistics

MAC address
Statistics available for the ext interface and connected stations (by MAC address)

Overall RSS
Signal levels in dBm

avg / dev / min / max
Average / standard deviation / minimum / maximum value

Samples
Number of samples used for the individual statistics

EXT1 antenna RSS
Signal strength at EXT1 antenna in dBm

EXT2 antenna RSS
Signal strength at EXT2 antenna in dBm

8.5.11. Measurements



Sensor	count	avg	min	max
CPU [°C]	59708	51.9	51.2	53.5
Modem board [°C]	59708	42.3	41.9	42.8
Radio board [°C]	252778	41.1	40.7	41.7
Input [V]	59708	13.3	12.6	13.5

Sensor
Measured values on RipEX2.

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 RipEX2 router interfaces. In addition to all the physical interfaces (RADIO, EXT, ETHs, COMs, TSs), some internal interfaces between software modules can be monitored when such advanced diagnostics is needed.

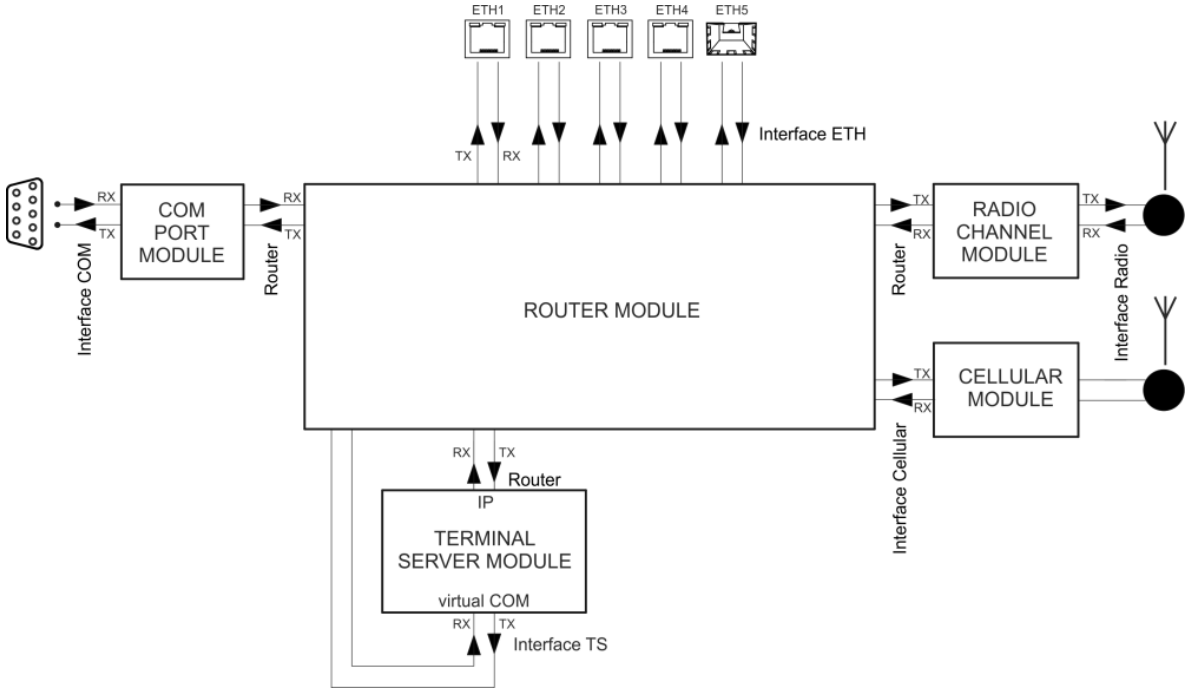


Fig. 8.24: Interfaces in the context of unit monitoring

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

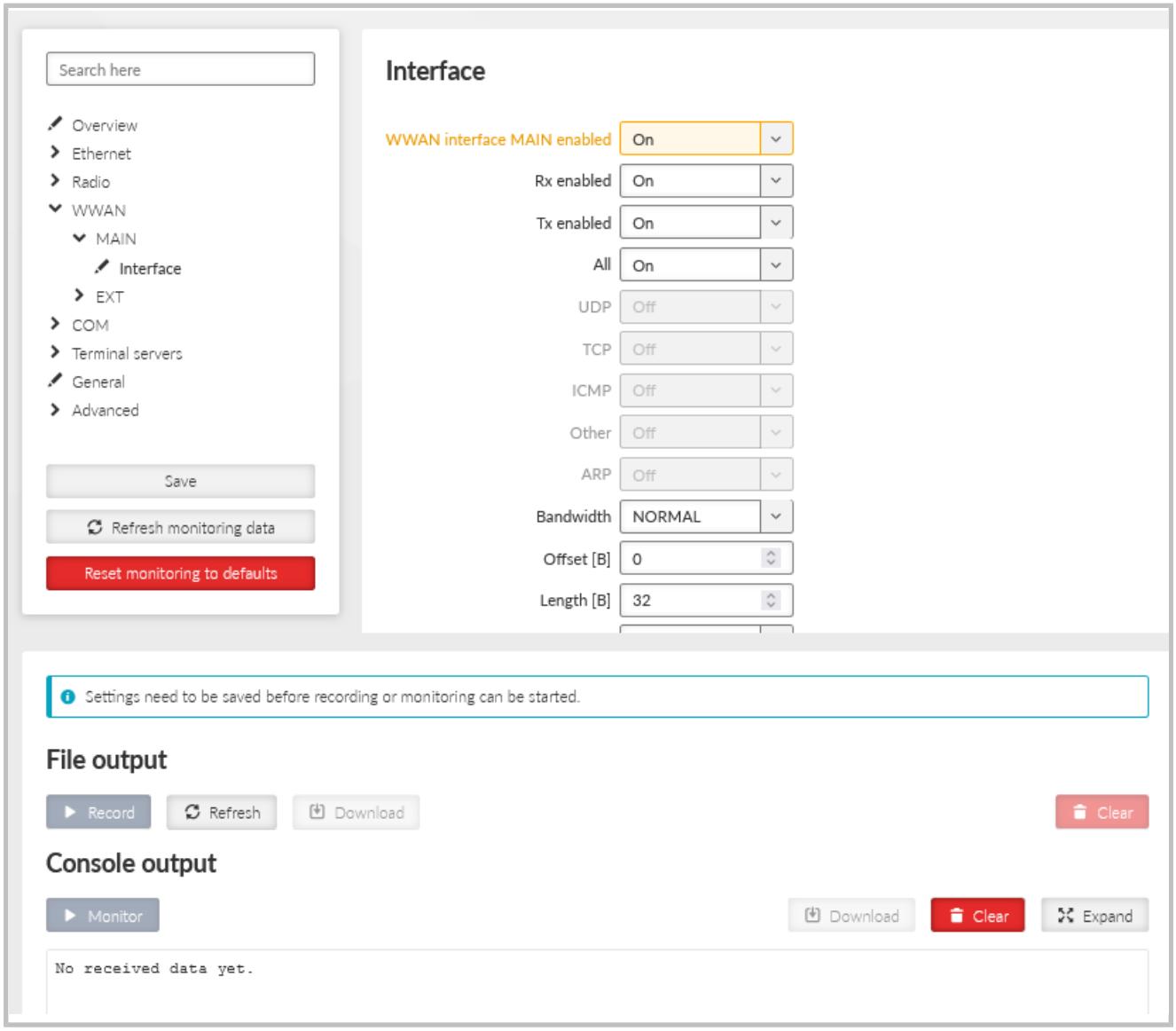


Fig. 8.25: DIAGNOSTICS > Monitoring

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.

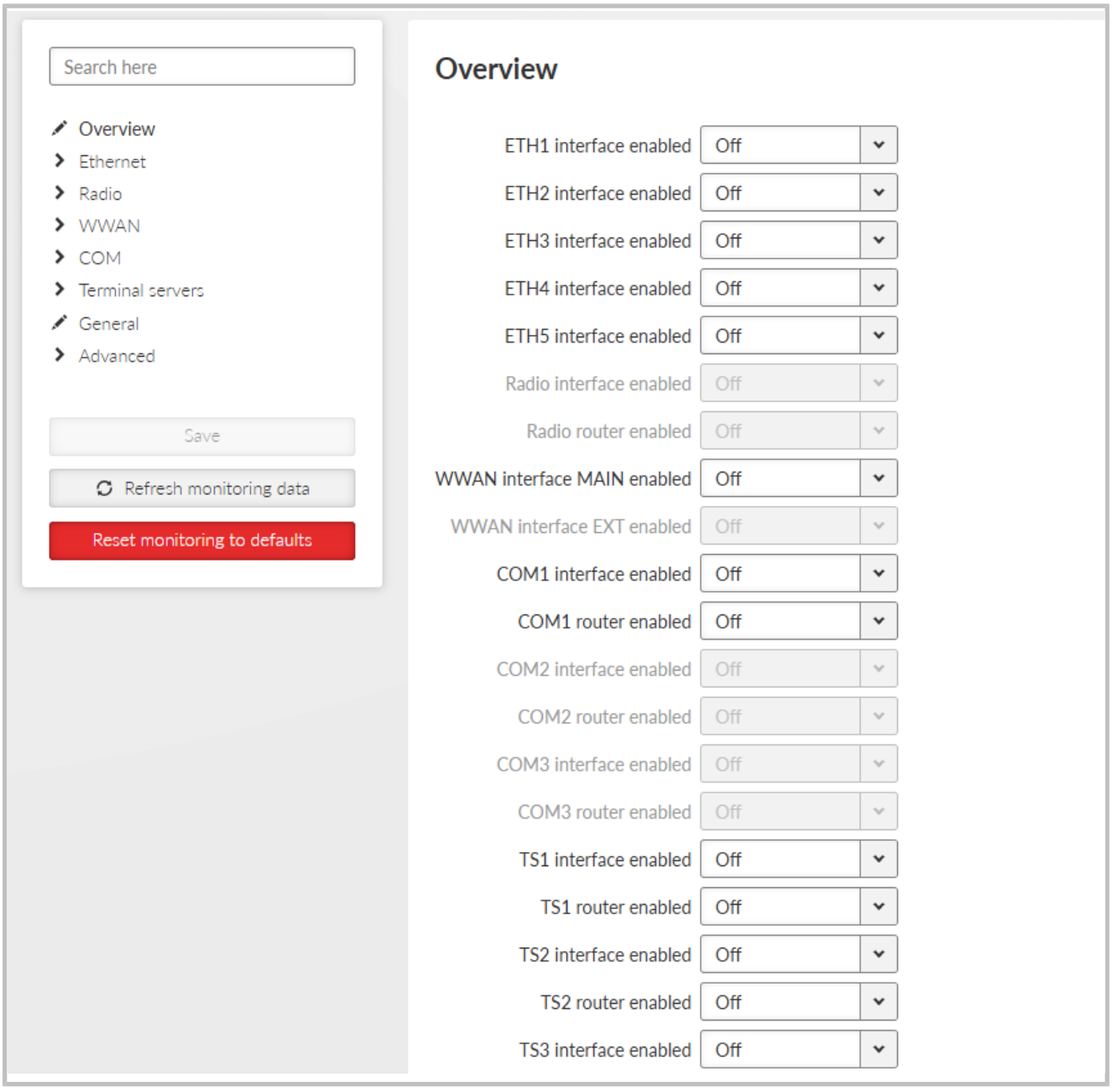


Fig. 8.26: DIAGNOSTICS > Monitoring > Overview

8.6.1.2. Interfaces

This section allows detailed settings of particular monitoring parameters for all interfaces.

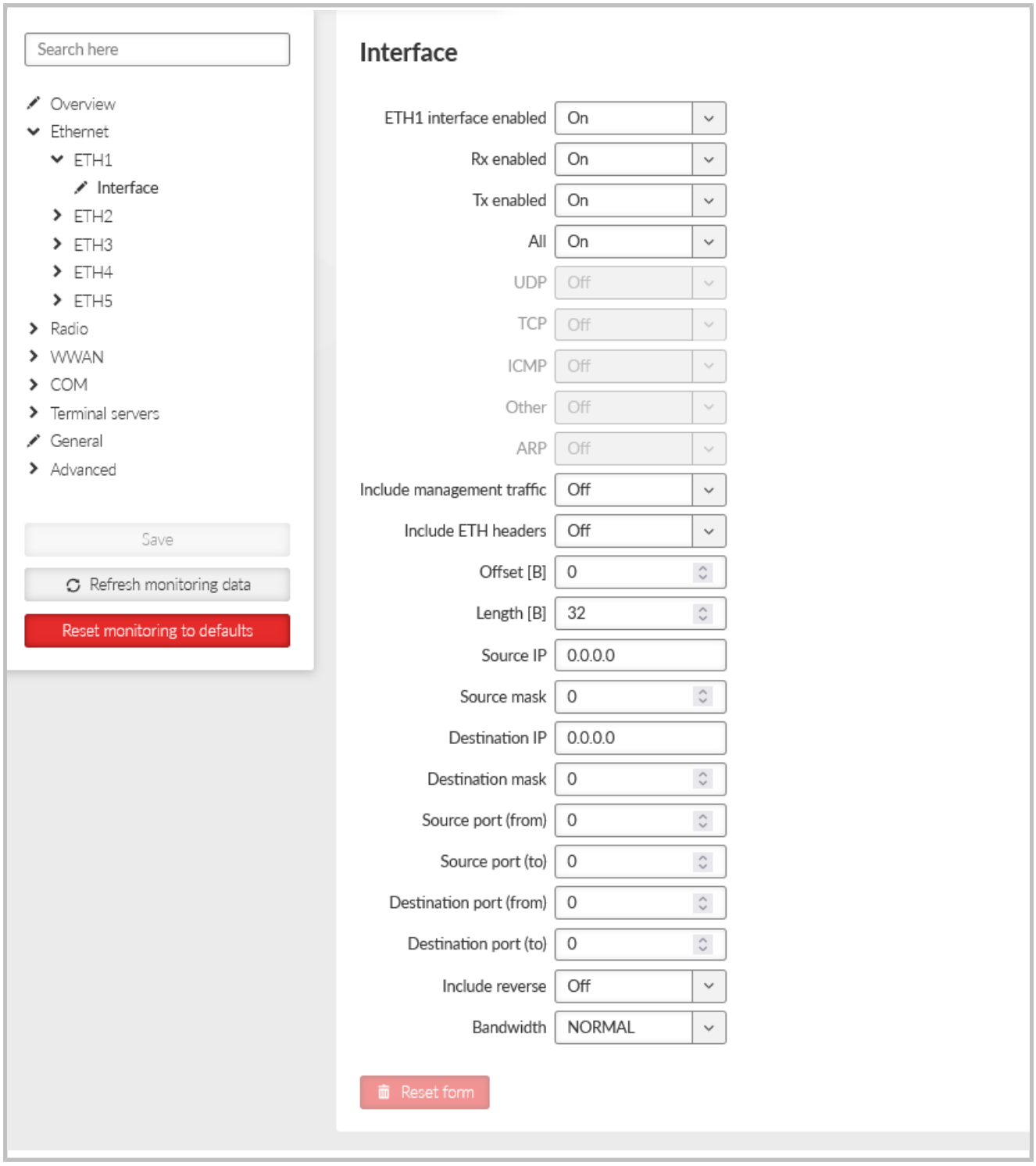


Fig. 8.27: DIAGNOSTICS > Monitoring > Ethernet > ETH1 > Interface

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. RADIO or Terminal Server) and vice versa. When an external interface (e.g. Interface COM) is monitored, the Tx also means packets being transmitted from the RipEX2 over the respective interface (Rx

means "received"). Understanding the directions over the internal interfaces may not be that straightforward, please see *Fig. 8.24, "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 RipEX2 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, ...).

8.6.1.2.1. 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.

8.6.1.2.2. Radio interface

Corrupted frames
List box {On; Off}, default = "On"
Corrupted ("header CRC error", "data CRC error", etc.) received frames monitoring output can be suppressed. This can be useful when the communication in the channel is heavily disturbed by interference or noise, resulting in „garbage" messages which can make the monitoring output difficult to read.

Other modes
List box {On; Off}, default = "Off"
When Promiscuous mode is enabled, the unit is capable to monitor (receive) frames from the other RipEX2 units even if the other unit(s) is(are) working in the other Unit mode (Bridge versus Router). Frames transmitted under another Unit mode may not be properly 'analyzed'. In such a case frames are displayed in raw data format.

Include headers (Router)
List box {None; Packet (IP); Frame (ETH)}, default = "None"

- None – Only the payload (L4) is displayed, e.g. the data part of a UDP datagram.
- Packet (IP) – Headers up to a Network layer (L3) are included, i.e. the full IP packet is displayed.
- Frame (ETH) – The full Ethernet frame (L2) is displayed, i.e. including the ETH header.

Include headers (Interface)
List box {None; Radio link; Data coding; Both}, default = "None"

- None - no headers will be displayed
- Radio link – radio link headers will be included into the monitoring output
- Data coding – data coding header will be included, where C: type of compression, E: type of encryption
- Both – both Radio link and data coding headers will be included

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

- Off – only frames which are normally received by this unit, i.e. frames whose Radio IP destination equals to Radio IP address of this RipEX2 unit and broadcast frames are available for the monitoring. Monitoring filters are applied afterwards.
- On – all frames detected on the Radio channel are available for the monitoring. Monitoring filters are applied afterwards.

Link Control Frames

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

- Off – Radio Link Control Frames (e.g. ACK frames) are never displayed.
- On – Radio Link Control Frames are processed by monitoring. Monitoring filters are applied.

Source IP / mask, Destination IP / mask (router)

Monitoring output can also be limited to a specific address range - Internal (router) Source and Destination IP address and mask can be used to define the required range.

Source IP / mask, Destination IP / mask (radio)

Monitoring output can also be limited to a specific address range - Radio interface Source and Destination IP address and mask can be used to define the required range.

Include reverse / Include Radio reverse

Includes reverse traffic for source / destination settings.

Menu DIAGNOSTICS > Monitoring > Advanced groups together all setting across all monitoring web pages, mentioned above, in one web page.

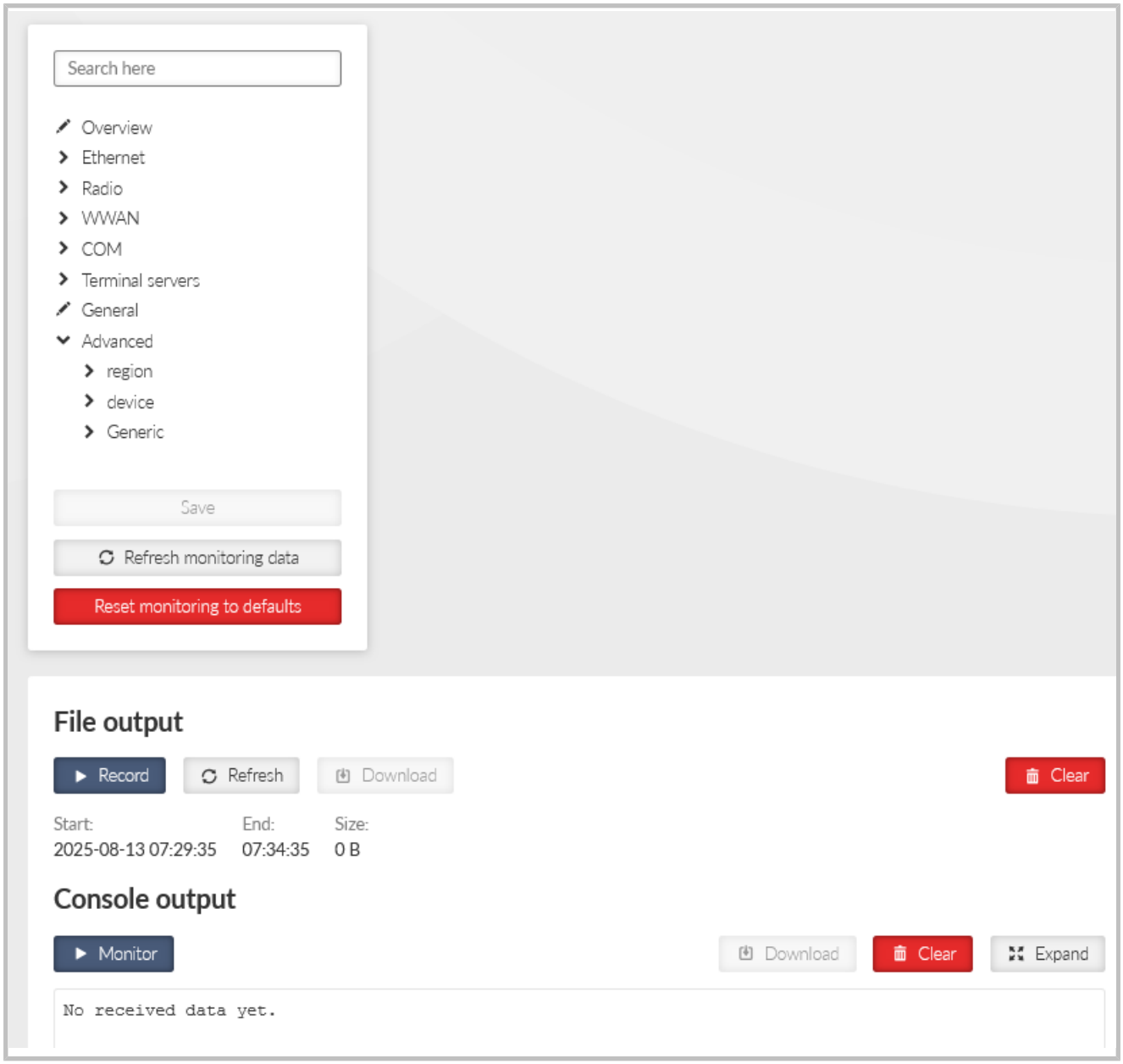


Fig. 8.28: DIAGNOSTICS > Monitoring > Advanced

Extended measurement

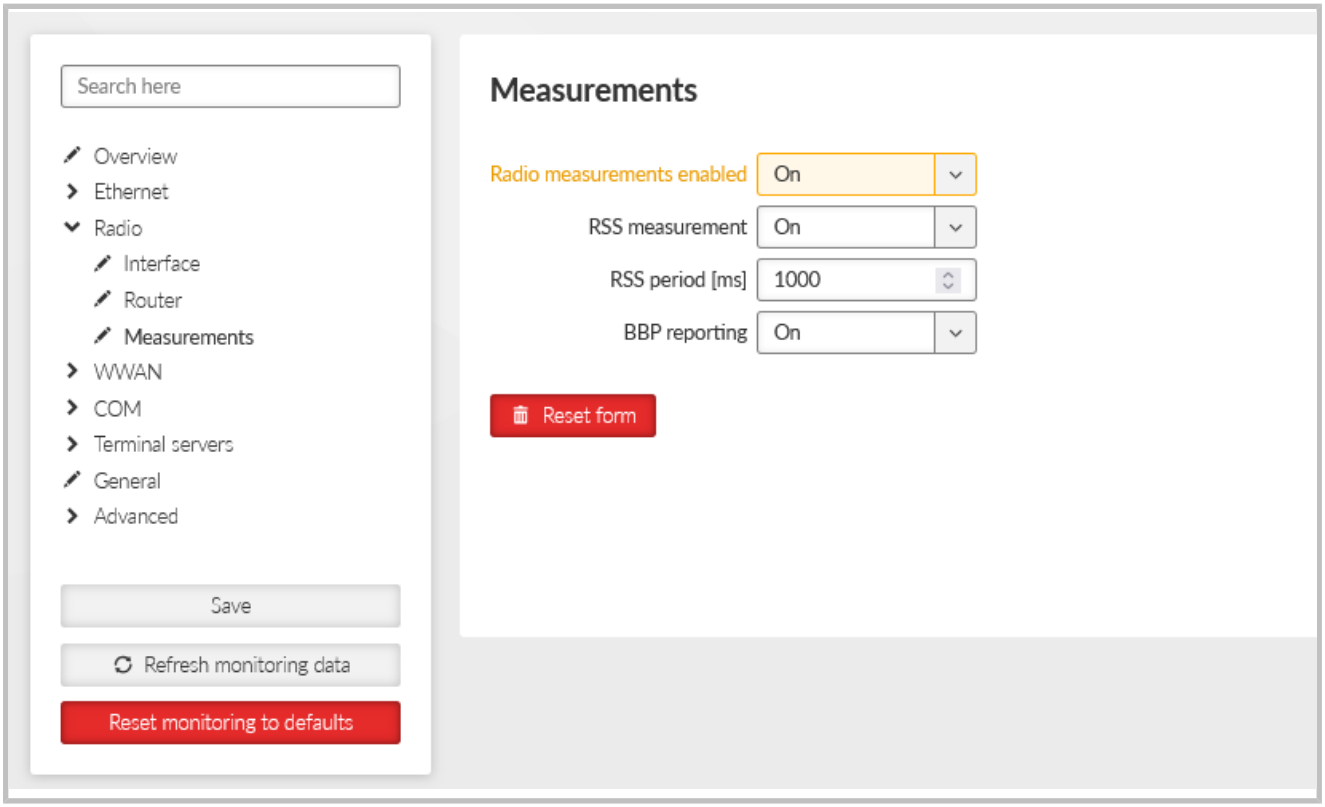


Fig. 8.29: Diagnostics > Monitoring > Radio > Measurements

Monitoring now includes additional parameters such as modulation type, FEC code, RF power, and temperature for TX, as well as modulation type, FEC code, frequency offset, and pre-packet RSS for RX.

Monitors regular measurements of radio channel and HW variables.

Individual measurements can be switched on and off, or the measurement period can be modified.

The signal strength is measured at the receiver at the set interval, regardless of any ongoing activity—even during transmission.

The BBP reporting function is included, providing the measured integrated power level across the entire bandwidth.

8.6.1.2.3. 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 EXT enabled (EXT)
List box {On; Off}, default = "Off"

8.6.1.3. General

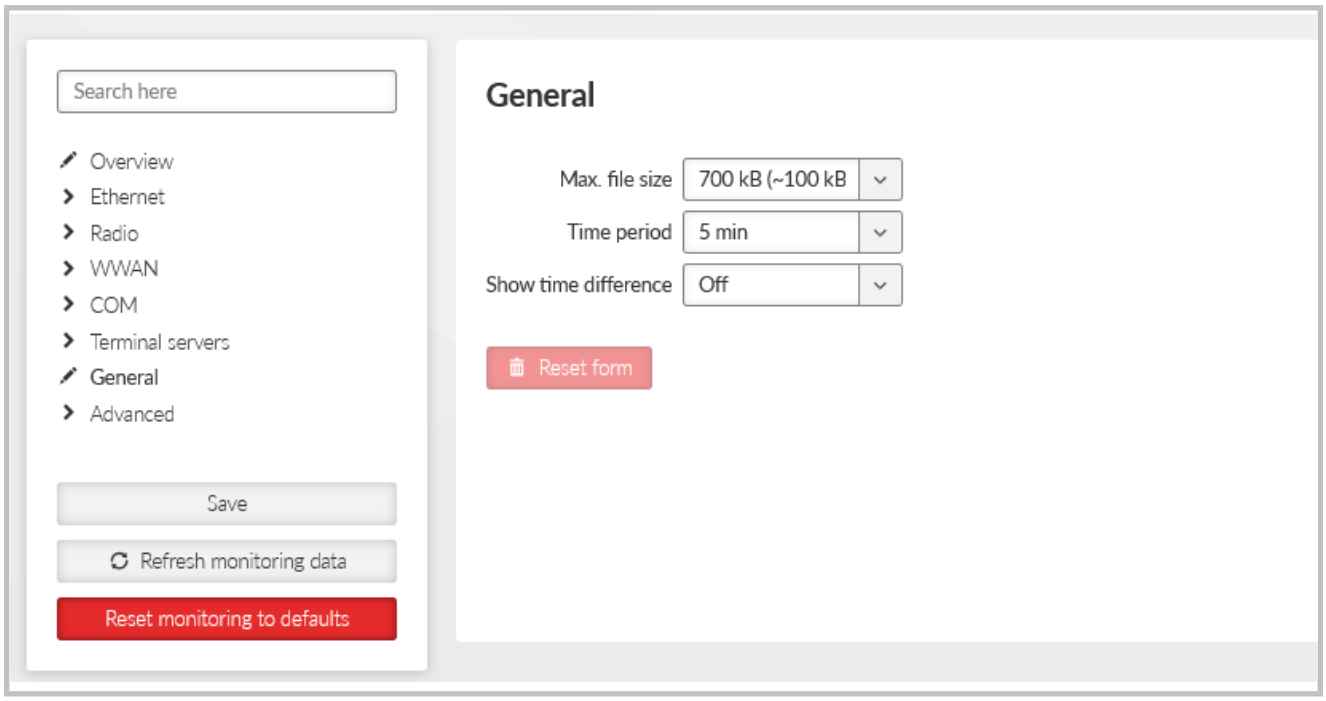


Fig. 8.30: DIAGNOSTICS > Monitoring

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 omited 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

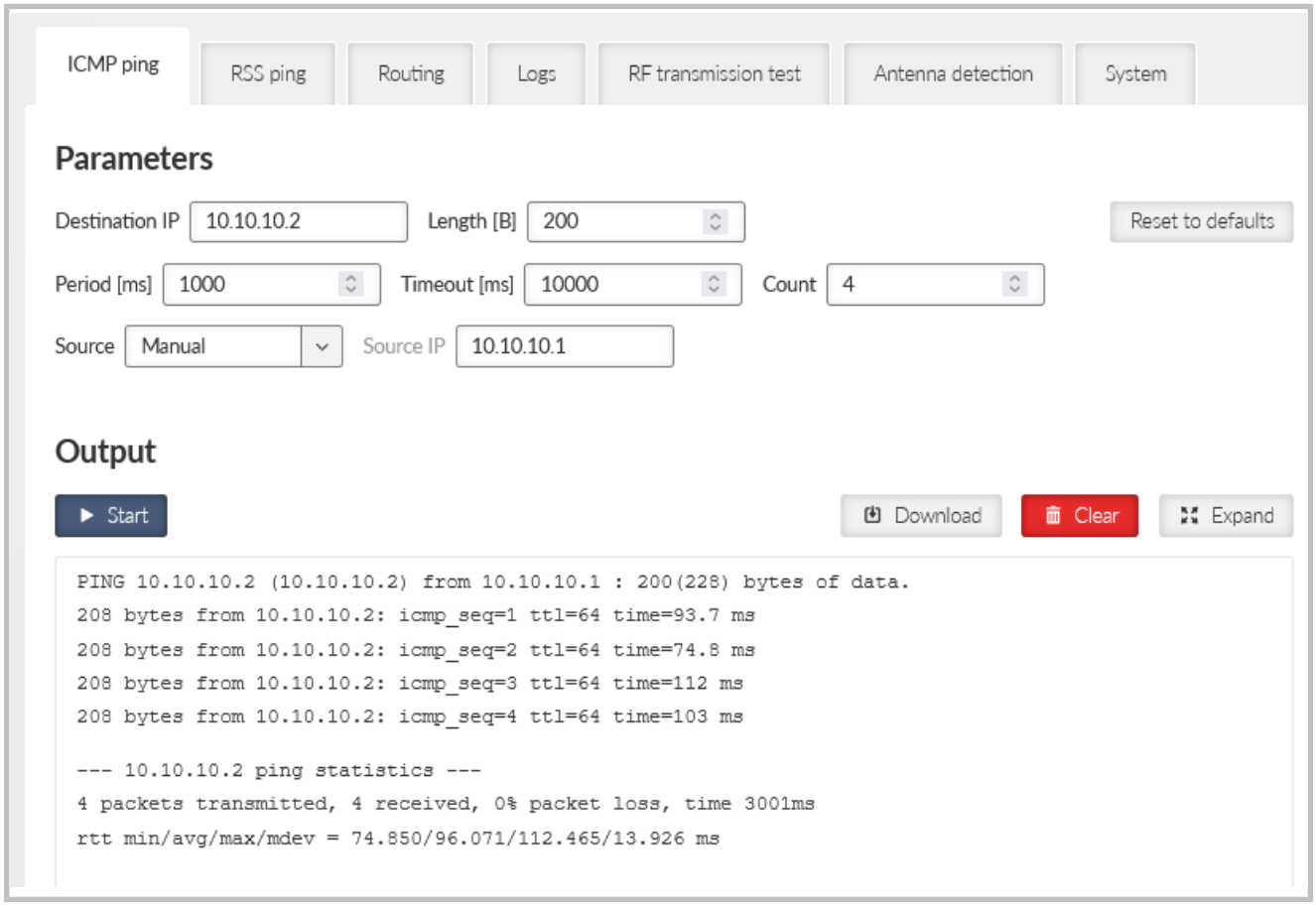


Fig. 8.31: DIAGNOSTICS > Tools > ICMP ping

All parameters used by standard ICMP ping are available. Start / Stop button starts / stops pinging.

8.7.2. RSS ping

(RipEX2 / RipEX2 combination)

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 RipEX2 network. Hybrid networks are supported. Output format of different type (other than radio) of hops is similar to ICMP ping.

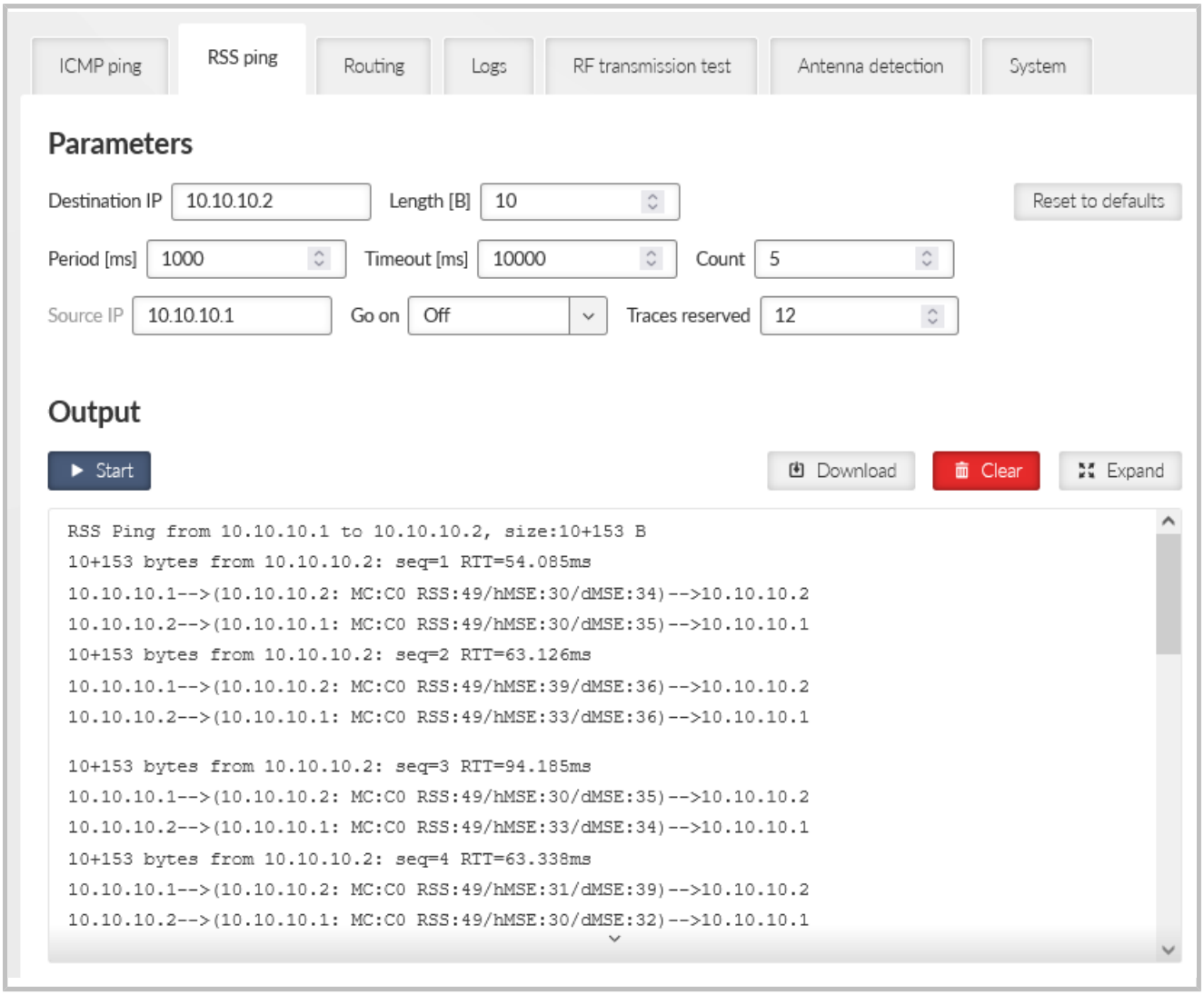


Fig. 8.32: DIAGNOSTICS > Tools > RSS ping

Destination IP

Destination IP address. This address must belong to a RipEX2 unit as the RSS ping can be initiated only between two RipEX2 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 RipEX2 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

	Modulation	**FEC**
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

	Modulation	FEC
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.



Fig. 8.33: DIAGNOSTICS > Tools > Routing

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. Logs

This tool provides a real-time display of process logs for active device operations. These logs are designed for live station diagnostics and do not offer historical data retrieval. For retrospective analysis, please utilize an alternative method, such as the *Diagnostic package*.

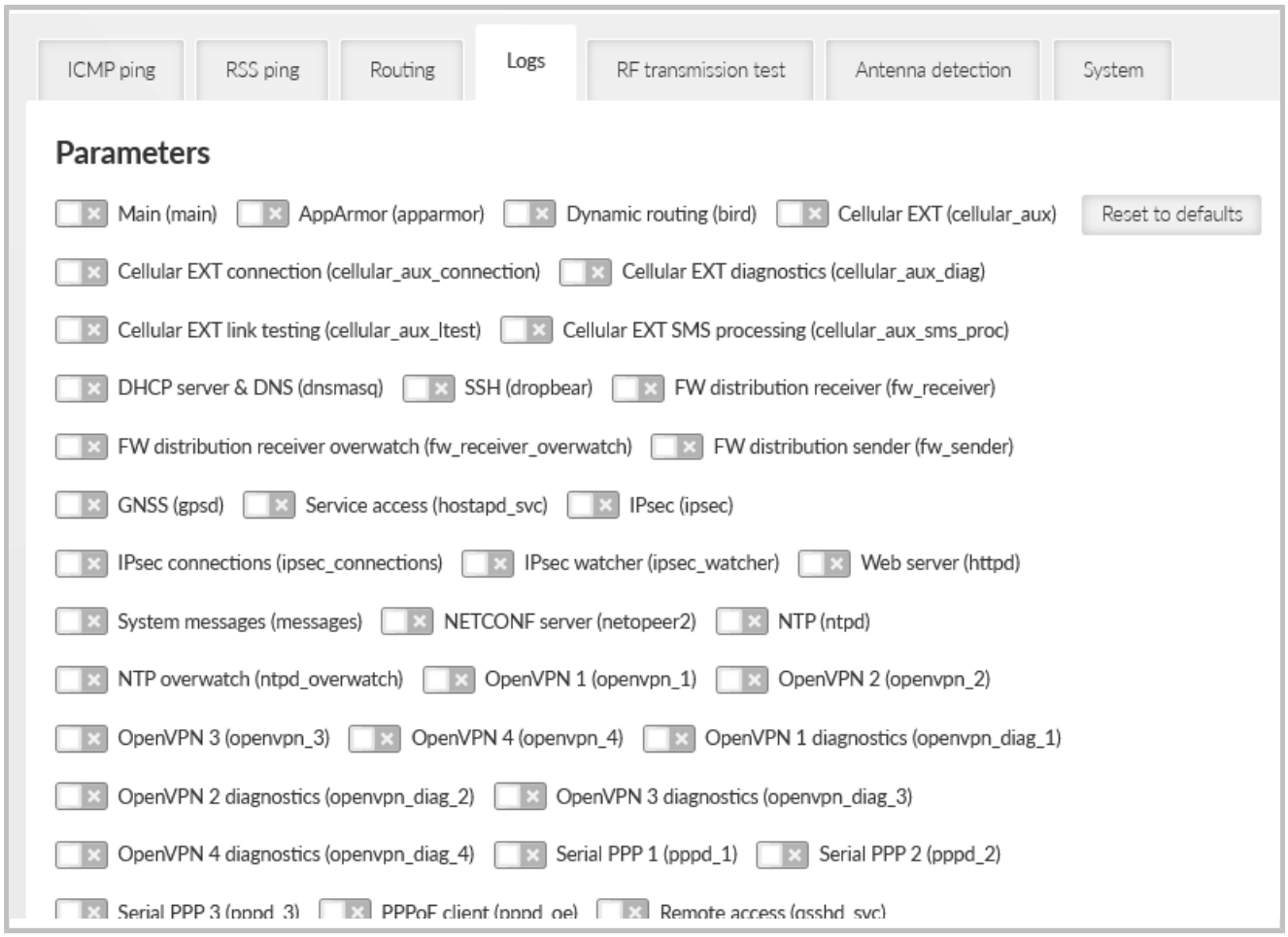


Fig. 8.34: DIAGNOSTICS > Tools > Logs

The core functionalities of this tool include:

- Real-time record display.
- Support for multiple independent instances (up to 10).
- Consolidated display of records from any number of processes within a single instance.
- Record filtering based on specified severity levels.
- Record length limitation to 1024 characters, with truncation of longer entries.

8.7.5. RF Transmission test

RF transmission test
Pre-defined type of RF signal can be transmitted for a specific purpose.

- **Type**

List box {Random data; Carrier wave; Single tone}, default = "Random data"
Type of transmitted signal during the test. In case of Single tone a frequency with an offset from the central frequency is transmitted.

- **Period [s]**
  Number {1 – 120 s}
  Transmission test pre-set duration.

- **Start** button
  Starts the transmission test. If "Start" is requested during running test, it will not be launched again, but an error value will return. Currently running test will finish its time period.

- **Stop** button
  Allows to stop the test before the pre-set time. If "Stop" is requested and there is no running test, and error value will return.

Note

Testing is only allowed without standard radio protocol. Please set "Radio protocol" to "None" in Radio Settings before using this feature.

8.7.6. Antenna detection

The RipEX2 is equipped with circuits and algorithms that make it possible to monitor the state of its output transmission circuits, including the antenna and its cable. To evaluate the situation, the data from the output directional coupling, which is contained in the output port of the transmitter's final stage, and the current of the final amplifier, which is always measured at the beginning of each transmitted packet, are used.

To take full advantage of these monitoring values, it is necessary to calibrate the system that monitors the transmitter output circuits and the antenna. The individual calibration steps are simple and straightforward, the help is fully available via the web interface, and it is necessary to go through them in the mode that will be used operationally.

The first step is to measure the relevant quantities with the working antenna of the installed unit. The second step is to disconnect the antenna cable from the RipEX2 or RipEX2-HS. The thresholds of the monitored quantities corresponding to the fault condition are then calibrated. The final, third step is to reconnect the antenna cable correctly and complete the calibration process according to the instructions provided by the web interface.

When calibration is complete, the result is automatically evaluated. If the calibration process reports the result as 'unreliable', this means that the system for monitoring the status of the transmitter output circuits do not have valid information for their operation and will not be fully functional. However, the calibration procedure that ends with a "mediocre" or "distinctive" result can be used for the system to monitor the state of the transmitter's output circuits, with the "distinctive" resultensuring greater robustness of the system.

Detector needs to be calibrated first to operate correctly:

Calibrate button initiates the calibration process. Following steps need to be done:

1. Set the Radio protocol to ‘None’. The Calibrate button can be pressed afterwards.

2. Disconnect the Tx antenna. It is recommended to disconnect the antenna cable as far from the radio unit (closer to the antenna) as possible – to get better detection sensitivity.

3. Connect the antenna. The antenna should not be disconnected any more after the calibration is finished – to ensure proper Detector sensitivity. If the antenna needs to be disconnected for a reason, it is recommended to repeat the calibration process afterwards.

Calibration limits:

- Calibration is valid for the given values of Tx frequency and RF Power. If those values need to be changed, it is necessary to re-calibrate the Detector after such change.

- The calibrated parameters are specific for the given radio unit and antenna connection. This is the reason, why the calibration parameters cannot be backed up for the eventual transfer to a backup unit. In case the radio unit needs to be replaced, the Detector must be re-calibrated.

Reset button initiates the Detector status reset. Such a reset is needed when the unit is operated as a Hot standby unit (see below) and the Detector caused the Hot standby units' switchover: the passive (repaired) station needs to be reset after the repair.

The "Radio TX or antenna degraded" *event* is triggered in case the Detector detects a problem.

8.7.6.1. Hot standby operation

The Detector Event can be used as one of the triggers for the Hot standby units' switchover. There are several conditions for the Hot standby operation:

- Both Hot standby units need to be calibrated separately

- In case of shared Tx antenna, each unit must be calibrated as active – in order to have the antenna connected.

- In case of separated Tx antennas, it is possible to run the calibration both on active and passive unit independently. Unit repair or replacement does not interrupt the user data traffic. The calibration process (of the eventually replaced station) causes a short (up to 10 seconds) interference of the active station.

- The Detector needs to be reset after the passive station repair (see above).

8.7.6.1.1. Degradation detector status

The **Antenna disconnected** and **Antenna connected** lines provide information about the calibration – when it was finished, what is the frequency and RF power for which the calibration is valid.

Detector can be one of the following: {offline; running; not calibrated}

Quality of calibration informs about calibration process result – how reliable the failure detection can be expected:

- unreliable: low quality, unreliable failure detection

- mediocre: reasonable quality

- distinctive: good quality

8.7.7. System

Reboot button
Performs unit cold restart (power cycle equivalent).

8.8. Syslog

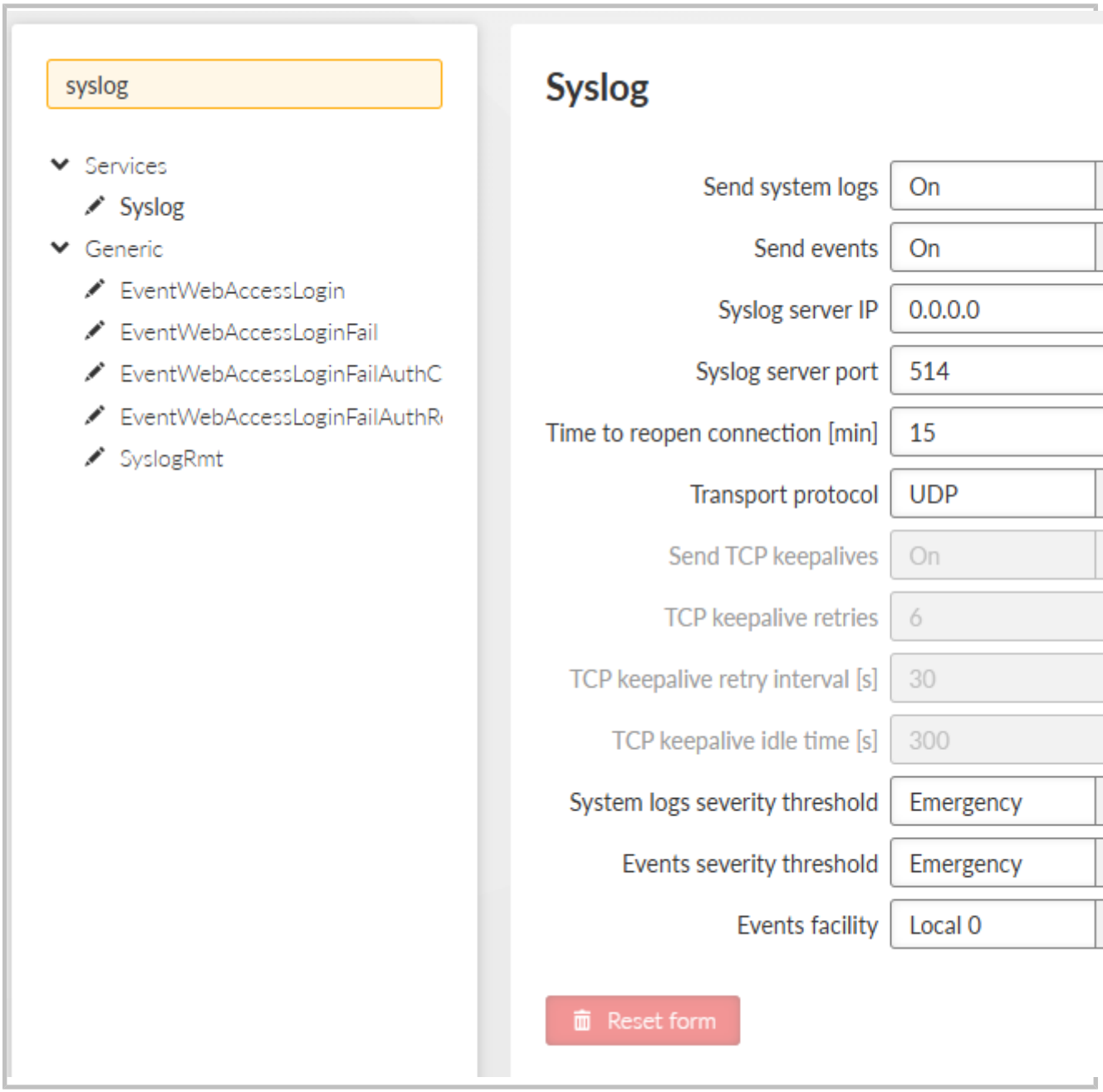


Fig. 8.35: ADVANCED > Services > Syslog

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

Tab. 9.1: Technical parameters

Radio parameters	**RipEX2**		**RipEX2e**	
Frequency bands	135 - 175; 215 - 240 MHz 285 – 335; 335 – 400 MHz 400 – 470; 450 – 520 MHz 803 – 897; 860 – 960 MHz			
Channel spacing	6.25; 12.5; 25; 50; 100; 150; 200; 250; 300 kHz		6.25; 12.5; 25; 50 kHz	
Frequency stability	±0.5 ppm *see details*			
Modulation	QAM: 256QAM; 64QAM; 16DEQAM; D8PSK; π/4DQPSK; DPSK FSK: 4CPFSK; 2CPFSK, *see details*		QAM: 64QAM; 16DEQAM; D8PSK; π/4DQPSK; DPSK FSK: 4CPFSK; 2CPFSK, *see details*	
ACM (Adaptive coding and modulation)	For each individual radio link according to real-time signal and channel conditions			
FEC (Forward Error Correction)	2/3; 3/4; 5/6; Off Trellis code with Viterbi soft-decoder			
Gross data rate (data speed) [1)]	Channel spacing [kHz]	Gross data rate (modulation rate) [kb/s]	Channel spacing [kHz]	Gross data rate (modulation rate) [kb/s]
	6.25	35	6.25	26
	12.5	83	12.5	63
	25	167	25	125
	50	333	50	250
	100	555		
	150	925		
	200	1111		
	250 [2)]	1389		
	300 [2)]	1736		
Transmitter				
RF Output power	QAM: 0.1 – 5.0 W (20 – 37 dBm) RMS in 1dB step [3)] FSK: 0.1 – 10 W (20 – 40 dBm) in 1dB step *see details*			
Duty cycle	Continuous			
Rx to Tx Time	< 2 ms @ 6.25 kHz channel < 1.0 ms @ 12.5 kHz channel < 0.7 ms @ 25 kHz channel			
Spurious Emissions (Conducted)	< -36 dBm			
Radiated Spurious Emissions	< -36 dBm			

Adjacent channel power	< -60 dBc	
Transient adjacent channel power	< -60 dBc	
Receiver		
Anti-aliasing Selectivity	56 kHz @ -3 dB BW applicable for 6.25; 12.5; 25 kHz 500 kHz @ -3 dB BW applicable for 50; 100; 150; 200; 250; 300 kHz	56 kHz @ -3 dB BW applicable for 6.25; 12.5; 25 kHz 500 kHz @ -3 dB BW applicable for 50 kHz
Tx to Rx Time	< 2 ms @ 6.25 kHz channel < 1.0 ms @ 12.5 kHz channel < 0.7 ms @ 25 kHz channel	
Maximum Receiver Input Power	20 dBm (100 mW)	
Rx Spurious Emissions (Conducted)	< -57 dBm	
Radiated Spurious Emissions	< -57 dBm	
Blocking or desensitization	> -23 dBm @ 1 MHz > -19 dBm @ 2 MHz > -15 dBm @ 5 MHz > -13 dBm @ 10 MHz	
Spurious response rejection	> 70 dB	

Technical parameters are subject to change without prior notification.

[1] Network throughput varies and depends heavily on the data structure, optimization effectivity, protocol on Radio channel, network topology, signal budgets and many other parameters of the network. Practical tests are recommended.

[2] Available only in Bridge mode.

[3] Max peak envelope power (PEP) 10 W (40 dBm) .

Electrical	**RipEX2**	**RipEX2e**
Primary power	10 to 30 VDC, negative GND	
Rx	8.3 W @ 24 V, *see details*	
Tx	12 – 55 W @ 24 V, *see details*	
Sleep mode	0.01 W	
Interfaces		
Ethernet	10/100/1000Base-T Auto MDI/MDIX 4× RJ45	10/100/1000Base-T Auto MDI/MDIX 2× RJ45
SFP	10/100/1000Base-T or 1000Base-SX or 1000Base-LX user exchangeable SFP with max. power consumption 1.25 W 1× SFP	No SFP

COM	RS232 / RS485 SW configurable	DB9F		
	600 b/s – 2 Mb/s			
COM2 RipEX2e, RipEX2 var. F and O	RS232	DB9F (COM1, COM2)		
	600 b/s – 2 Mb/s			
COM2, COM3 *Extension module 'C'*: Not available for RipEX2e, RipEX2 var. F and O	2× RS232	RJ45		
	COM2: 300 b/s – 2 Mb/s; COM3: 2.4 kb/s – 921.6 kb/s			
USB	USB 3.0	Host A		
Antenna	50 Ω SW configurable 1× Tx / Rx or 1× Rx + 1× Tx	2× TNC female	50 Ω 1× Tx / Rx	1× TNC female
Inputs/Outputs	1× HW alarm input 1× HW alarm output 1× Sleep input	Power connector		
	2× DI, 2× DO, 1× diffDI not available when Extension module 'C' (COM ports) is used	RJ45	Not available	

Indication LEDs	
LED panel	5× tri-color status LEDs (SYS, EXT, RX, TX, COM)
ETH	4× RJ45 (Link and Activity LEDs), 1× SFP (Status LED)
Environmental	
IP Code (Ingress Protection)	IP41, IP42, IP52 - *see details*
MTBF (Mean Time Between Failure)	> 900 000 hours (> 100 years)
Operating temperature	−40 to +70 °C (−40 to +158 °F) *4)*
Operating humidity	5 to 95 % non-condensing
Storage	−40 to +85 °C (−40 to +185 °F) / 5 to 95 % non-condensing
Mechanical	
Casing	Rugged die-cast aluminium
Dimensions	H×W×D: 60×185×125.5 mm (2.34×7.2×4.94 in)
Weight	1.55 kg (3.4 lbs)
Mounting	DIN rail, L-bracket, Flat-bracket, 19" Rack chassis *see details*[1]
SW	
Operating modes	Bridge / Router
Radio channel protocols	Transparent @ Bridge Base driven, Flexible @ Router (RipEX2e does not support Base station in Base driven) *see details*[2]
User protocols on COM	DNP3, DF1, IEC101, Modbus RTU, PR2000, RDS, Siemens 3964(R), COMLI, SAIA S-bus, Mars-A, PPP, 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
Routing (both, Radio and Ethernet)	Static, Dynamic - Babel, OSPF, BGP, Link management
QoS	8 levels on all interfaces
Protocol on Radio channel	
Multi master applications	Yes
Report by exception	Yes
Collision Avoidance Capability	Yes
Remote to Remote communication	Yes
Repeaters	Store-and-forward Every unit Unlimited number
Data integrity control	CRC 32
Optimization	Intelligent payload data and header (Eth / IP / TCP / UDP) compression
Security	

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting
[2] https://www.racom.eu/eng/products/radio-modem-ripex.html#radio_protocols

Management	HTTPS (Web Interface or Application Programming Interface)
Role-based access control (RBAC)	4 levels (Guest, Tech, SecTech, Admin)
Wi-Fi management access	WPA2-PSK secured
Encryption	AES256-CCM
VPN	IPsec, OpenVPN, GRE
VLAN	IEEE 802.1Q (tagging), Q-in-Q for Transparent mode
AAA protocol	RADIUS
Firewall	Layer 2 - MAC, Layer 3 - IP, Layer 4 - TCP/UDP
FW	Digitally signed
HW tamper	Case opening evidence

[4)] When full-duplex with full power (40 dBm PEP) and the surrounding temperature above + 60 °C the external passive cooler should be used (e.g. *RipEX2-RS 19" Rack chassis*[3]).

Diagnostic and Management	
Link testing	ICMP ping, RSS ping
Status information	User interfaces
Statistics	Historical and differential statistics for Rx / Tx Packets on all user interfaces (ETH 1-5, COM 1-3, TS 1-5) and Radio interface - for individual connections. Radio protocol statistics (frame error, replied, duplicated, lost etc.) for individual radio links. Advanced statistics for Radio channel (RSS levels, MSE, Pre-frame RSS, Repeats, etc.)
Statistics history	Several weeks
Event log	Events filtered by time, severity, user, remote IP address and type of event
SNMP	SNMPv1, SNMPv2c, SNMPv3 Trap / Inform alarms generation as per settings
NTP	Client / Server
Monitoring	Real time analysis of all interfaces (RADIO, ETH 1-5 , COM 1-3, TS 1-5) and internal interfaces between software modules, *see details*

[3] https://www.racom.eu/eng/products/m/ripex2-hs/product.html#rip2rs

Standards	
CE	*RED, RoHS, WEEE*
FCC, IC	*FCC Part 90, IC RSS-119*
Spectrum	ETSI EN 302 561 V2.1.1 ETSI EN 300 113 V2.2.1
EMC (electromagnetic compatibility)	ETSI EN 301 489-1 V2.2.3 ETSI EN 301 489-5 V3.2.1 EN 61850-3:2014
Product safety	EN 62368-1:2014 + A11:2017
Cybersecurity	EN 18031-1:2024 IEC 62443-4-2:2019
RF health safety	EN 62311:2008
Electric power substations environment	IEEE 1613:2009 IEEE 1613.1:2013 EN 61850-3:2014
Hazardous locations	EN 60079-0:2012 EN 60079-11:2012
Environmental	EN 61850-3: 2014
Vibration & shock	EN 60068-2-6:2008 ETS 300 019-2-3:1994, Class 3.4 EN 61850-3:2014
Seismic qualification	EN 60068-2-27:2010
IP rating	EN 60529:1993 + A1:2001 + A2:2014

Optional interfaces (not applicable for RipEX2e)	
Extension module 'G' GNSS (GPS)	Active antenna 3.3 VDC SMA female (EXT on front panel)
	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' COM ports	COM2: RS232 - 5 pin (RxD, TxD, GND, RTS, CTS) 300 b/s to 2 Mb/s COM3: RS232 - 3 pin (RxD, TxD, GND) 2.4 kb/s to 921.6 kb/s RJ45 (DI/DO on front panel)
Extension module 'W', 'R', 'S' Cellular	*see details*
Extension module 'F' Wi-Fi	IEEE 802.11a/b/g/n/ac 2×2 MIMO 20 MHz / 40 MHz for 2.4 GHz 20 MHz / 40 MHz / 80 MHz for 5 GHz WPA/WPA2 PSK WPA3-SAE AES/TKIP hardware encryption Output power up to 16 dBm EmWicon WMX6218 - FCC ID 2A3G3-WMX6218

Tab. 9.2: Maximal power for individual modulations

RipEX2			
Modulation	**PEP [dBm]**	**RMS [dBm]**	**RMS [W]**
2CPFSK	20 – 40	20 – 40	0.1 – 10
4CPFSK	20 – 40	20 – 40	0.1 – 10
DPSK	20 – 40	20 – 37	0.1 – 5
π/4-DQPSK	20 – 40	20 – 37	0.1 – 5
D8PSK	20 – 40	20 – 36	0.1 – 4
16DEQAM	20 – 40	20 – 35	0.1 – 3.2
64QAM	20 – 40	20 – 34	0.1 – 2.5
256QAM	20 – 40	20 – 33	0.1 – 2
SW configurable [PEP, dBm] FSK, QAM: 1 dB step			
PEP vs. RMS application note[4]			

Tab. 9.3: List of connected cables

Input / Output	Specified length	Shielded / Nonshielded	Recommended cable type
DC power supply 10 – 30 V	As needed	N	V03VH-H 2×0,5

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

Input / Output	Specified length	Shielded / Nonshielded	Recommended cable type
GPIO (Sleep Input, HW Alarm Input, HW Alarm Output)	As needed	S	LiYCY 6×0,14
Antenna connection Rx, Rx/Tx	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
EXT (used for GNSS)	As needed	S	Coaxial
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. 3 m	S	USB3
DI / DO	As needed	S	STP CAT 5e
Ex Check the maximum voltage, current and minimal cross sections in *Table 10.4, "Maximum voltage and current of individual interfaces"* for hazardous location conditions.			

Tab. 9.4: Power consumption for 24 Vdc

Tx Power consumption @24Vdc	**RipEX2-1**			**RipEX2-3, RipEX2-4**		
	Min.	Typ.	Max.	Min.	Typ.	Max.
FSK 20 dBm RMS	12	14	15	12	14	15
FSK 40 dBm RMS	27	33	40	31	40	55
QAM 24 dBm PEP	12	13	14	12	13	14
QAM 40 dBm PEP	24	26	30	24	29	40

Rx Power consumption @24Vdc	**RipEX2**
RipEX2	8.3 W
+Ethernet	+0.1 W @ 10BaseT +0.12 W @ 100BaseT +0.5 W @ 1000BaseT per Eth interface with connected equipment
+1st COM	+0.2 W
+GNSS	+0.15 W
+2nd COM	+0.1 W
+LTE	Rx +0.3, Tx +3.0 W
+SFP module typ.	+1.0 W
+Wi-Fi	+3.0 W Max

Tab. 9.5: Cellular interface (optional)

Cellular interface (optional)	
Frequency bands for extension module 'W' Cellular	4G LTE (also 5G NSA) Rel.10 Band 1 (2100 MHz), Band 2 (1900 MHz), Band 3 (1800 MHz), Band 4 (1700/2100 MHz), Band 5 (850 MHz), Band 7 (2600 MHz), Band 8 (900 MHz), Band 12 (700 MHz), Band 13 (700 MHz)*, Band 14 (700 MHz), Band 17 (700 MHz), Band 18 (850 MHz), Band 19 (850 MHz), Band 20 (800 MHz), Band 25 (1900 MHz), Band 26 (850 MHz), Band 28 (700 MHz), Band 38 (2600 MHz), Band 40 (2300 MHz), Band 41 (2500 MHz)**, Band 66 (1700/2100 MHz), Band 71 (600 MHz) * a sensitivity issue will occur in GNSS when transmitting in Band 13 ** for Band 41 (LTE-TDD), the frequency range are partially supported (2535 MHz...2675 MHz)
	3G UMTS/HSDPA/HSUPA Rel.7: Band 1 (2100 MHz), Band 2 (1900 MHz), Band 3 (1800 MHz), Band 4 (1700/2100 MHz), Band 5 (850 MHz), Band 6 (850 MHz), Band 8 (900 MHz), Band 19 (850 MHz))
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
	Cinterion PLS83-W FCC ID QIPPLS83-W TAC 35107264
Specification for module 'W' Cellular	Antenna: 2× SMA female – receiver diversity (2×2 MIMO)
	4G LTE (also 5G NSA) 3GPP Rel.10 Long Term Evolution (LTE) Evolved Uni. Terrestrial Radio Access (E-UTRA) Frequency Division Duplex (FDD) DL Multi-Input Multi-Output (MIMO) 2×2 Data throughput: Cat.4, DL 150 Mb/s, UL 50 Mb/s
	3G UMTS/HSDPA/HSUPA 3GPP Rel.7 Dual-Cell HS Packet Access (DC-HSPA+) UMTS Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD) DL Rx diversity Data throughput: Cat.14: HSPA+ DL 21 Mbps HSUPA UL 5.7 Mbps
	2G GSM/GPRS/EDGE 3GPP Rel.4 Enhanced Data rate GSM Evolution (EDGE) GSM EGPRS Radio Access (GERA) Time Division Multiple Access (TDMA) DL Advanced Rx Performance Phase 1 Data throughput: Class 12, DL 237 kb/s, UL 237kb/s

Frequency bands for extension module 'R'Cellular	4G LTE Cat M1, NB2 3GPP Rel.14: Band 1 (2100 MHz), Band 3 (1800 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 20 (800 MHz), Band 28 (700 MHz), Band 31 (450 MHz), Band 72 (450 MHz), Band 87 (410 MHz), Band 88 (410 MHz)	
	Telit ME310G1-W2	EU RED, UK UKCA, ANATEL
Frequency bands for extension module 'S' Cellular	4G LTE Cat M1, NB2 3GPP Rel.14: Band 1 (2100 MHz), Band 2 (1900 MHz), Band 3 (1800 MHz), Band 4 (1700/2100 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 8 (900 MHz) (39d), Band 12 (700 MHz), Band 13 (700 MHz), Band 18 (850 MHz), Band 19 (850 MHz), Band 20 (800 MHz), Band 25 (1900 MHz), Band 26 (850 MHz), Band 27 (800 MHz), Band 28 (700 MHz), Band 66 (1700/2100 MHz), Band 71 (600 MHz), Band 85 (700 MHz)	
	Telit ME310G1-WW	EU RED, UK UKCA, CA ISED, MX IFETEL, AU RCM, CH CCC, JP JRL/JTBL, KR, KCC, SG IMDA, TW NCC FCC ID RI7ME310G1WW
Specification for extension cellular module 'R' and 'S'	1× SMA Antenna	
	4G LTE Cat M1, NB2	
	3GPP Release 14	
	Data throughput: M1 - DL 588 kb/s, UL 1 Mb/s NB2 - DL 120 kb/s, UL 160 kb/s	
	Only 1.8 V simcard are supported.	
Frequency bands for extension module 'E' Cellular**	4G LTE Band 20 (800 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)	
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz	
	Ublox TOBY L-210	FCC ID XPYTOBYL210 TAC 35225506
Frequency bands for extension module 'P' Cellular**	4G LTE Band 28 (750 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)	
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz,	

	PCS 1900 MHz	
	Ublox TOBY L-280	FCC ID XPYTOBYL280 TAC 35850306
Frequency bands for extension module 'A' Cellular**	4G LTE Band 17 (700 MHz), Band 5 (850 MHz), Band 4 (1700 MHz), Band 2 (1900 MHz), Band 7 (2600 MHz)	
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 4 (AWS, i.e. 1700 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz	
	Ublox TOBY L-200	FCC ID XPYTOBYL200 TAC 35225406

** E, P, A cellular modules were under production until XI/2021

Tab. 9.6: Sensitivity

Modulation	2CPFSK	4CPFSK	DPSK	π/4DQPSK	D8PSK	16DEQAM	64QAM	256QAM
Channel spacing	Sensitivity [dbm] @ BER 10^{-6}, FEC 3/4 (2/3 QAM64 and QAM256)							
6.25	-119	-116	-116	-115	-111	-106	-104	-100
12.5	-117	-114	-114	-113	-108	-103	-101	-97
25	-115	-112	-112	-111	-106	-101	-99	-95
50	x	x	-109	-108	-103	-98	-96	-92
100	x	x	-106	-105	-100	-95	-93	-89
150	x	x	-104	-103	-98	-93	-91	-87
200	x	x	-103	-102	-97	-92	-90	-86
250	x	x	-102	-101	-96	-93	-89	-85
300	x	x	-100	-99	-94	-91	-87	-83
	Sensitivity [dbm] @ BER 10^{-2} (ETSI 80% PSR eqv.), FEC 3/4 (2/3 QAM64 and QAM256)							
6.25	-123	-121	-122	-121	-119	-116	-116	-109
12.5	-120	-119	-119	-118	-116	-112	-112	-106
25	-118	-117	-117	-116	-113	-110	-110	-104
50	x	x	-114	-113	-110	-107	-107	-101
100	x	x	-112	-111	-108	-104	-104	-99
150	x	x	-110	-109	-106	-102	-102	-97
200	x	x	-109	-108	-105	-101	-101	-96
250	x	x	-107	-106	-103	-100	-100	-94
300	x	x	-106	-105	-101	-98	-98	-93

Note

Consider the proper fade margin for the radio link design. The larger the fade margin the higher link availability. The fade margin of 20 dB is considered acceptable for most installations with availability 99% or less. The fade margin of 25 dB or higher shall be used for highly reliable systems (99.9% availability).

9.1. Detailed radio channel parameters

Tab. 9.7: Channel spacing 5 kHz

Channel spacing [kHz]	**5**	
Occupied BW limit [kHz]	4	4
Modulation type	FSK	QAM
RipEX 1 "Mode"	-	-
Baudrate [kBaud]	2.17	3.26
RipEX2 Compliance	FCC, ISED (pending)	FCC, ISED (pending)

5 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 2.17 kBaud				
2.17	2CPFSK	3K00F1DBN	3.00	4
4.34	4CPFSK	3K00F1DBN	3.00	4
Baudrate 3.26 kBaud				
3.26	DPSK	3K60G1DBN	3.60	4
6.52	π/4-DQPSK	3K60G1DBN	3.60	4
9.78	D8PSK	3K60G1DEN	3.60	4
13.04	16DEQAM	3K60G1DEN	3.60	4
19.56	64QAM	3K60G1DEN	3.60	4
26.08	256QAM	3K60G1DEN	3.60	4

Tab. 9.8: Channel spacing 6.25 kHz

Channel spacing [kHz]	**6.25**	
Occupied BW limit [kHz]	5	5
Modulation type	FSK	QAM
RipEX 1 "Mode"	FCC, CE	FCC
Baudrate [kBaud]	2.60	4.34
RipEX2 Compliance	FCC, ISED	FCC, ISED

6.25 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 2.60 kBaud				
2.60	2CPFSK	3K60F1DBN	3.60	5
5.21	4CPFSK	3K60F1DBN	3.60	5
Baudrate 4.34 kBaud				
4.34	DPSK	5K00G1DBN	5.00	5
8.68	π/4-DQPSK	5K00G1DDN	5.00	5
13.02	D8PSK	5K00G1DEN	5.00	5
17.36	16DEQAM	5K00G1DEN	5.00	5
26.04	64QAM	5K00G1DEN	5.00	5
34.72	256QAM	5K00G1DEN	5.00	5

5 kHz						
Classification				Sensitivity [dBm]		
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}
RX sensitivity, Baudrate 2.17 kBaud						
2.17	1.95	3/4	2CPFSK	-123.0	-121.5	-119.5
2.17	2.60	Off	2CPFSK	-122.5	-120.5	-117.5
4.34	3.91	3/4	4CPFSK	-121.5	-119.5	-116.5
4.34	5.21	Off	4CPFSK	-120.5	-118.0	-114.5
RX sensitivity, Baudrate 3.26 kBaud						
3.26	2.46	3/4	DPSK	-122.5	-121.0	-116.5
3.26	3.26	Off	DPSK	-122.0	-120.0	-114.5
6.52	4.69	3/4	π/4-DQPSK	-121.5	-120.0	-115.5
6.52	6.52	Off	π/4-DQPSK	-120.5	-118.5	-112.5
9.78	7.34	3/4	D8PSK	-119.5	-116.5	-111.0
9.78	9.78	Off	D8PSK	-116.0	-112.5	-106.0
13.04	9.78	3/4	16DEQAM	-116.0	-112.5	-106.5
13.04	13.04	Off	16DEQAM	-113.0	-110.0	-103.0
19.56	13.04	2/3	64QAM	-116.0	-112.0	-104.0
19.56	14.67	3/4	64QAM	-113.0	-109.5	-102.5
19.56	16.30	5/6	64QAM	-112.0	-107.0	-100.0
19.56	19.56	Off	64QAM	-109.0	-104.5	-97.0
26.08	17.38	2/3	256QAM	-109.5	-106.5	-100.5
26.08	19.56	3/4	256QAM	-108.5	-105.0	-98.5
26.08	21.73	5/6	256QAM	-106.5	-103.5	-96.5
26.08	26.08	Off	256QAM	-104.5	-100.5	-95.0

6.25 kHz						
Classification				Sensitivity [dBm]		
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}
RX sensitivity, Baudrate 2.60 kBaud						
2.60	1.95	3/4	2CPFSK	-122.5	-121.0	-119.0
2.60	2.60	Off	2CPFSK	-122.0	-120.0	-117.0
5.21	3.91	3/4	4CPFSK	-121.0	-119.0	-116.0
5.21	5.21	Off	4CPFSK	-120.0	-117.5	-114.0
RX sensitivity, Baudrate 4.34 kBaud						
4.34	3.26	3/4	DPSK	-122.0	-120.5	-116.0
4.34	4.34	Off	DPSK	-121.5	-119.5	-114.0
8.68	6.51	3/4	π/4-DQPSK	-121.0	-119.5	-115.0
8.68	8.68	Off	π/4-DQPSK	-120.0	-118.0	-112.0
13.02	9.77	3/4	D8PSK	-118.5	-116.0	-110.5
13.02	13.02	Off	D8PSK	-115.5	-112.0	-105.5
17.36	13.02	3/4	16DEQAM	-115.5	-112.0	-106.0
17.36	17.36	Off	16DEQAM	-112.5	-109.5	-102.5
26.04	17.36	2/3	64QAM	-115.5	-111.5	-103.5
26.04	19.53	3/4	64QAM	-112.5	-109.0	-102.0
26.04	21.70	5/6	64QAM	-111.5	-106.5	-99.5
26.04	26.04	Off	64QAM	-108.5	-104.0	-96.5
34.72	23.15	2/3	256QAM	-109.0	-106.0	-100.0
34.72	26.04	3/4	256QAM	-108.0	-104.5	-98.0
34.72	28.94	5/6	256QAM	-106.0	-103.0	-96.0
34.72	34.72	Off	256QAM	-104.0	-100.0	-94.5

Tab. 9.9: Channel spacing 12.5 kHz

Channel spacing [kHz]	**12.5**		
Occupied BW limit [kHz]	11	11	12.5
Modulation type	FSK	QAM	
RipEX 1 "Mode"	FCC, CE	FCC	CE
Baudrate [kBaud]	5.21	8.68	10.42
RipEX2 Compliance	RED FCC, ISED	RED FCC, ISED	RED

12.5 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 5.21 kBaud				
5.21	2CPFSK	7K50F1DBN	7.0	11.0
10.42	4CPFSK	7K50F1DDN	7.0	11.0
Baudrate 8.68 kBaud				
8.68	DPSK	10K0G1DBN	10.0	11.0
17.36	π/4-DQPSK	10K0G1DDN	10.0	11.0
26.04	D8PSK	10K0G1DEN	10.0	11.0
34.72	16DEQAM	10K0G1DEN	10.0	11.0
52.08	64QAM	10K0G1DEN	10.0	11.0
69.44	256QAM	10K0G1DEN	10.0	11.0
Baudrate 10.42 kBaud				
10.42	DPSK	11K9G1DBN	11.9	12.5
20.83	π/4-DQPSK	11K9G1DDN	11.9	12.5
31.25	D8PSK	11K9G1DEN	11.9	12.5
41.67	16DEQAM	11K9G1DEN	11.9	12.5
62.50	64QAM	11K9G1DEN	11.9	12.5
83.33	256QAM	11K9G1DEN	11.9	12.5

12.5 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
RX sensitivity, Baudrate 5.21 kBaud							
5.21	3.91	3/4	2CPFSK	-120	-119	-117	-7
5.21	5.21	Off	2CPFSK	-120	-118	-115	-10
10.42	7.81	3/4	4CPFSK	-119	-117	-114	-11
10.42	10.42	Off	4CPFSK	-118	-115	-112	-6
RX sensitivity, Baudrate 10.42 kBaud							
10.42	7.81	3/4	DPSK	-119	-118	-114	-6.5
10.42	10.42	Off	DPSK	-119	-117	-112	-5
20.83	15.62	3/4	π/4-DQPSK	-118	-117	-113	-9
20.83	20.83	Off	π/4-DQPSK	-117	-115	-110	-10
31.25	23.44	3/4	D8PSK	-116	-113	-108	-12
31.25	31.25	Off	D8PSK	-113	-109	-103	-14
41.67	31.25	3/4	16DEQAM	-112	-109	-103	-16
41.67	41.67	Off	16DEQAM	-109	-106	-99	-18.5
62.50	41.67	2/3	64QAM	-112	-108	-101	-16
62.50	46.88	3/4	64QAM	-110	-106	-99	-19
62.50	52.08	5/6	64QAM	-109	-104	-97	-20
62.50	62.50	Off	64QAM	-105	-101	-94	-22.5
83.33	55.56	2/3	256QAM	-106	-103	-97	-21
83.33	62.50	3/4	256QAM	-105	-102	-95	-22
83.33	69.44	5/6	256QAM	-103	-100	-93	-24
83.33	83.33	Off	256QAM	-100	-97	-90	-28.5

Tab. 9.10: Channel spacing 25 kHz

Channel spacing[kHz]	**25**				
Occupied BW limit[kHz]	14	16	16	20	25
Modulation type	FSK		QAM		
RipEX 1 "Mode"		CE	Narrow	FCC	CE
Baudrate [kBaud]	8.68	10.42	13.89	17.36	20.83
RipEX2 Compliance	RED FCC, ISED	RED FCC, ISED	RED FCC, ISED	RED FCC, ISED	RED

25 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 8.68 kBaud				
8.68	2CPFSK	13K5F1DBN	13.5	14
17.36	4CPFSK	12K2F1DDN	12.2	14
Baudrate 10.42 kBaud				
10.42	2CPFSK	15K5F1DBN	15.5	16
20.83	4CPFSK	15K5F1DDN	15.5	16
Baudrate 13.89 kBaud				
13.89	DPSK	15K9G1DBN	15.9	16
27.78	π/4-DQPSK	15K9G1DDN	15.9	16
41.67	D8PSK	15K9G1DEN	15.9	16
55.56	16DEQAM	15K9G1DEN	15.9	16
83.33	64QAM	15K9G1DEN	15.9	16
111.11	256QAM	15K9G1DEN	15.9	16
Baudrate 17.36 kBaud				
17.36	DPSK	19K8G1DBN	19.8	20
34.72	π/4-DQPSK	19K8G1DDN	19.8	20
52.08	D8PSK	19K8G1DEN	19.8	20
69.44	16DEQAM	19K8G1DEN	19.8	20
104.17	64QAM	19K8G1DEN	19.8	20
138.89	256QAM	19K8G1DEN	19.8	20
Baudrate 20.83 kBaud				
20.83	DPSK	24K0G1DBN	24.0	25
41.67	π/4-DQPSK	24K0G1DDN	24.0	25
62.50	D8PSK	24K0G1DEN	24.0	25
83.33	16DEQAM	24K0G1DEN	24.0	25
125.00	64QAM	24K0G1DEN	24.0	25
166.67	256QAM	24K0G1DEN	24.0	25

25 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
Rx sensitivity Baudrate 10.42							
10.42	7.81	3/4	2CPFSK	-118	-117	-115	-6
10.42	10.42	Off	2CPFSK	-118	-116	-113	-7
20.83	15.63	3/4	4CPFSK	-117	-115	-112	-10
20.83	20.83	Off	4CPFSK	-115	-113	-109	-6
Rx sensitivity Baudrate 20.83							
20.83	15.62	3/4	DPSK	-117	-116	-112	-6
20.83	20.83	Off	DPSK	-117	-115	-110	-6
41.66	31.25	3/4	π/4-DQPSK	-116	-115	-111	-9
41.66	41.66	Off	π/4-DQPSK	-115	-113	-108	-10
62.49	46.87	3/4	D8PSK	-113	-111	-106	-12
62.49	62.49	Off	D8PSK	-110	-107	-101	-14.5
83.33	62.49	3/4	16DEQAM	-110	-107	-101	-16
83.33	83.33	Off	16DEQAM	-108	-105	-98	-18.5
125.00	83.33	2/3	64QAM	-110	-106	-99	-16
125.00	93.75	3/4	64QAM	-108	-104	-97	-19
125.00	104.17	5/6	64QAM	-107	-102	-95	-20
125.00	125.00	Off	64QAM	-104	-99	-92	-22.5
166.67	111.11	2/3	256QAM	-104	-101	-95	-21
166.67	125.00	3/4	256QAM	-103	-100	-93	-22
166.67	138.89	5/6	256QAM	-101	-98	-91	-24
166.67	166.67	Off	256QAM	-98	-95	-88	-28.5

Tab. 9.11: Channel spacing 50 kHz

Channel spacing [kHz]	**50**	
Occupied BW limit [kHz]	40	50
Modulation type	QAM	
RipEX 1 "Mode"	CE	Unlimited
Baudrate [kBaud]	34.72	41.67
RipEX2 Compliance	RED	RED

50 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 34.72 kBaud				
34.72	DPSK	40K0G1DBN	40.0	40
69.44	π/4-DQPSK	40K0G1DDN	40.0	40
104.17	D8PSK	40K0G1DEN	40.0	40
138.89	16DEQAM	40K0G1DEN	40.0	40
208.33	64QAM	40K0G1DEN	40.0	40
277.78	256QAM	40K0G1DEN	40.0	40
Baudrate 41.67 kBaud				
41.67	DPSK	45K0G1DBN	45.0	50
83.33	π/4-DQPSK	45K0G1DDN	45.0	50
125.00	D8PSK	45K0G1DEN	45.0	50
166.67	16DEQAM	45K0G1DEN	45.0	50
250.00	64QAM	45K0G1DEN	45.0	50
333.33	256QAM	45K0G1DEN	45.0	50

50 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
Baudrate 41.67 kBaud							
41.67	31.25	3/4	DPSK	-114	-113	-109	-7
41.67	41.67	Off	DPSK	-114	-112	-107	-7
83.33	62.50	3/4	π/4-DQPSK	-113	-112	-108	-10
83.33	83.33	Off	π/4-DQPSK	-112	-110	-105	-11
125.00	93.75	3/4	D8PSK	-110	-108	-103	-13
125.00	125.00	Off	D8PSK	-107	-104	-98	-15
166.67	125.00	3/4	16DEQAM	-107	-104	-98	-17
166.67	166.67	Off	16DEQAM	-105	-102	-95	-19
250.00	166.67	2/3	64QAM	-107	-103	-96	-17
250.00	187.50	3/4	64QAM	-105	-101	-94	-20
250.00	208.33	5/6	64QAM	-104	-99	-92	-21
250.00	250.00	Off	64QAM	-101	-96	-89	-23
333.33	222.22	2/3	256QAM	-101	-98	-92	-22
333.33	250.00	3/4	256QAM	-100	-97	-90	-23
333.33	277.78	5/6	256QAM	-98	-95	-88	-25
333.33	333.33	Off	256QAM	-95	-92	-85	-31

Tab. 9.12: Channel spacing 100 kHz

Channel spacing [kHz]	**100**	
Occupied BW limit [kHz]	80	100
Modulation type	QAM	
Baudrate [kBaud]	69.44	83.3
RipEX2 Compliance	RED	

100 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 69.44 kBaud				
69.44	DPSK	80K0G1DBN	80.0	80
138.89	π/4-DQPSK	80K0G1DDN	80.0	80
208.33	D8PSK	80K0G1DEN	80.0	80
277.78	16DEQAM	80K0G1DEN	80.0	80
416.66	64QAM	80K0G1DEN	80.0	80
555.55	256QAM	80K0G1DEN	80.0	80

100 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
Baudrate 69.44 kBaud							
69.44	52.08	3/4	DPSK	-112	-110	-106	-7
69.44	69.44	Off	DPSK	-111	-109	-104	-7
138.89	104.17	3/4	π/4-DQPSK	-111	-109	-105	-10
138.89	138.89	Off	π/4-DQPSK	-110	-108	-102	-11
208.33	156.25	3/4	D8PSK	-108	-105	-100	-13
208.33	208.33	Off	D8PSK	-105	-101	-95	-15
277.78	208.33	3/4	16DEQAM	-104	-101	-95	-17
277.78	277.78	Off	16DEQAM	-102	-99	-92	-19
416.66	277.78	2/3	64QAM	-104	-100	-93	-17
416.66	312.50	3/4	64QAM	-102	-98	-91	-20
416.66	347.22	5/6	64QAM	-101	-96	-89	-21
416.66	416.66	Off	64QAM	-98	-93	-86	-23
555.55	370.37	2/3	256QAM	-99	-95	-89	-22
555.55	416.66	3/4	256QAM	-98	-94	-86	-23
555.55	462.96	5/6	256QAM	-96	-92	-85	-25
555.55	555.55	Off	256QAM	-93	-89	-83	-31

Tab. 9.13: Channel spacing 150 kHz

Channel spacing [kHz]	**150**	
Occupied BW limit [kHz]	125	150
Modulation type	QAM	
Baudrate [kBaud]	115.74	124.01
RipEX2 Compliance	RED	

150 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 115.74 kBaud				
115.74	DPSK	125KG1DBN	125.0	125
231.48	π/4-DQPSK	125KG1DDN	125.0	125
347.22	D8PSK	125KG1DEN	125.0	125
462.96	16DEQAM	125KG1DEN	125.0	125
694.45	64QAM	125KG1DEN	125.0	125
925.93	256QAM	125KG1DEN	125.0	125

150 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
Baudrate 115.74 kBaud							
115.74	86.71	3/4	DPSK	-110	-108	-104	-7
115.74	115.74	Off	DPSK	-109	-107	-102	-7
231.48	173.61	3/4	π/4-DQPSK	-109	-107	-103	-10
231.48	231.48	Off	π/4-DQPSK	-108	-106	-100	-11
347.22	260.42	3/4	D8PSK	-106	-103	-98	-13
347.22	347.22	Off	D8PSK	-103	-99	-93	-15
462.96	347.22	3/4	16DEQAM	-102	-99	-93	-17
462.96	462.96	Off	16DEQAM	-100	-97	-90	-19
694.45	462.96	2/3	64QAM	-102	-98	-91	-17
694.45	520.83	3/4	64QAM	-100	-96	-89	-20
694.45	587.71	5/6	64QAM	-99	-94	-87	-21
694.45	694.45	Off	64QAM	-96	-91	-84	-23
925.93	617.29	2/3	256QAM	-97	-93	-87	-22
925.93	694.45	3/4	256QAM	-96	-92	-84	-23
925.93	771.61	5/6	256QAM	-94	-90	-83	-25
925.93	925.93	Off	256QAM	-91	-87	-81	-31

Tab. 9.14: Channel spacing 200 kHz

Channel spacing [kHz]	**200**
Occupied BW limit [kHz]	175
Modulation type	QAM
Baudrate [kBaud]	138.89
RipEX2 Compliance	RED

200 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 138.89 kBaud				
138.89	DPSK	150KG1DBN	150.0	175
277.78	π/4-DQPSK	150KG1DDN	150.0	175
416.67	D8PSK	150KG1DEN	150.0	175
555.56	16DEQAM	150KG1DEN	150.0	175
833.33	64QAM	150KG1DEN	150.0	175
1111.11	256QAM	150KG1DEN	150.0	175

200 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
Baudrate 138.89 kBaud							
138.89	104.17	3/4	DPSK	-109	-107	-103	-7
138.89	138.89	Off	DPSK	-108	-106	-101	-7
277.78	208.33	3/4	π/4-DQPSK	-108	-106	-102	-10
277.78	277.78	Off	π/4-DQPSK	-107	-105	-99	-11
416.67	312.50	3/4	D8PSK	-105	-102	-97	-13
416.67	416.67	Off	D8PSK	-102	-98	-92	-15
555.55	416.67	3/4	16DEQAM	-101	-98	-92	-17
555.55	555.55	Off	16DEQAM	-99	-96	-89	-19
833.33	555.55	2/3	64QAM	-101	-97	-90	-17
833.33	625.00	3/4	64QAM	-99	-95	-88	-20
833.33	694.45	5/6	64QAM	-98	-93	-86	-21
833.33	833.33	Off	64QAM	-95	-90	-83	-23
1111.11	740.74	2/3	256QAM	-96	-92	-86	-22
1111.11	833.33	3/4	256QAM	-95	-91	-83	-23
1111.11	925.93	5/6	256QAM	-93	-89	-82	-25
1111.11	1111.11	Off	256QAM	-90	-86	-80	-31

Tab. 9.15: Channel spacing 250 kHz

Channel spacing [kHz]	**250**
Occupied BW limit [kHz]	250
Modulation type	QAM
Baudrate [kBaud]	208.33

250 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 208.33 kBaud				
208.33	DPSK	225KG1DBN	225.0	250
416.67	π/4-DQPSK	225KG1DDN	225.0	250
625.00	D8PSK	225KG1DEN	225.0	250
833.33	16DEQAM	225KG1DEN	225.0	250
1250.00	64QAM	225KG1DEN	225.0	250
1388.89	256QAM	225KG1DEN	225.0	250

250 kHz							
Classification				**Sensitivity [dBm]**			**Co-Channel Rejection Ratio**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-2}**	**BER 10^{-3}**	**BER 10^{-6}**	**[dB]**
Baudrate 208.33 kBaud							
208.33	156.25	3/4	DPSK	-107	-106	-102	-7
208.33	208.33	Off	DPSK	-107	-105	-100	-7
416.67	312.50	3/4	π/4-DQPSK	-106	-105	-101	-10
416.67	416.67	Off	π/4-DQPSK	-105	-103	-98	-11
625.00	468.75	3/4	D8PSK	-103	-101	-96	-13
625.00	625.00	Off	D8PSK	-100	-97	-91	-15
833.33	625.00	3/4	16DEQAM	-100	-97	-93	-17
833.33	833.33	Off	16DEQAM	-98	-95	-88	-19
1250.00	833.33	2/3	64QAM	-100	-96	-89	-17
1250.00	937.50	3/4	64QAM	-98	-94	-88	-20
1250.00	1041.67	5/6	64QAM	-97	-92	-86	-21
1250.00	1250.00	Off	64QAM	-96	-91	-84	-23
1666,67	1111.11	2/3	256QAM	-94	-91	-85	-22
1666,67	1250.00	3/4	256QAM	-93	-90	-83	-23
1666,67	1388.89	5/6	256QAM	-91	-88	-81	-25

Tab. 9.16: Channel spacing 300 kHz

Channel spacing [kHz]	**300**
Occupied BW limit [kHz]	300
Modulation type	QAM
Baudrate [kBaud]	260.42

300 kHz				
Modulation rate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 260.42 kBaud				
260.42	DPSK	280KG1DBN	280.0	300
520.83	π/4-DQPSK	280KG1DDN	280.0	300
781.25	D8PSK	280KG1DEN	280.0	300
1041.67	16DEQAM	280KG1DEN	280.0	300
1562.50	64QAM	280KG1DEN	280.0	300
1736.11	256QAM	280KG1DEN	280.0	300

300 kHz							
Classification				**Sensitivity [dBm]**			**Co-Channel Rejection Ratio**
Modulation rate [kb/s]	**Bitrate [kb/s]**	**FEC**	**Modulation**	**BER 10^{-2}**	**BER 10^{-3}**	**BER 10^{-6}**	**[dB]**
Baudrate 260.42 kBaud							
260.42	195.31	3/4	DPSK	-106	-104	-100	-7
260.42	260.42	Off	DPSK	-105	-103	-98	-7
520.83	390.63	3/4	π/4-DQPSK	-105	-103	-99	-10
520.83	520.83	Off	π/4-DQPSK	-104	-102	-96	-11
781.25	585.94	3/4	D8PSK	-101	-99	-94	-13
781.25	781.25	Off	D8PSK	-99	-95	-89	-15
1041.67	781.25	3/4	16DEQAM	-98	-95	-91	-17
1041.67	1041.67	Off	16DEQAM	-96	-93	-86	-19
1562.50	1041.67	2/3	64QAM	-98	-94	-87	-17
1562.50	1171.88	3/4	64QAM	-96	-92	-86	-20
1562.50	1302.09	5/6	64QAM	-95	-90	-84	-21
1562.50	1562.50	Off	64QAM	-92	-87	-81	-23
2083,34	1388.89	2/3	256QAM	-93	-89	-83	-22
2083,34	1562.50	3/4	256QAM	-91	-88	-81	-23
2083,34	1736.11	5/6	256QAM	-90	-86	-79	-25

9.2. Recommended MSE thresholds

Tab. 9.17: MSE

Recommended MSE thresholds		
Modulation	**FEC**	**Mean MSE [dB]**
2CPFSK	3/4	-10
2CPFSK	Off	-11
4CPFSK	3/4	-12
4CPFSK	Off	-15
DPSK	3/4	-10
DPSK	Off	-11
π/4-DQPSK	3/4	-12
π/4-DQPSK	Off	-14
8DPSK	3/4	-17
8DPSK	Off	-20
16DEQAM	3/4	-19
16DEQAM	Off	-22
64QAM	3/4	-24
64QAM	Off	-27
256QAM	3/4	-30
256QAM	Off	-33

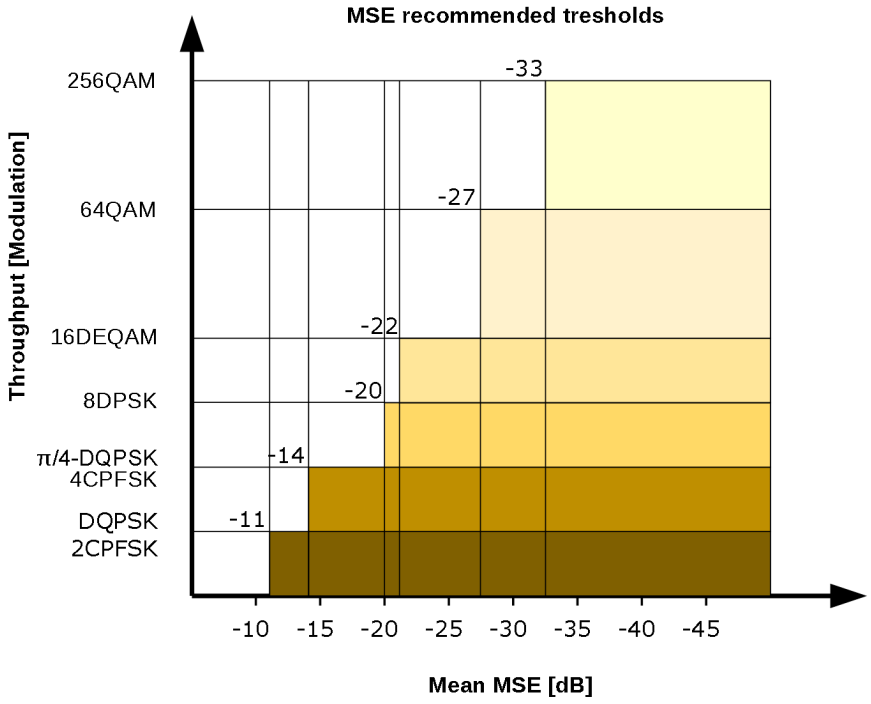


Fig. 9.1: MSE recommended tresholds

10. Safety, regulations, warranty

10.1. Frequency

The radio modem must be operated only in accordance with the valid frequency license issued by national frequency authority and all radio parameters have to be set exactly as listed.

Important

Use of frequencies between 406.0 and 406.1 MHz is worldwide-allocated only for International Satellite Search and Rescue System. These frequencies are used for distress beacons and are incessantly monitored by the ground and satellite Cospas-Sarsat system. Other use of these frequencies is forbidden.

Important

The radio operator is responsible for setting the radio parameters of the radio modem exactly in accordance with the valid frequency license issued by national frequency authority, and all radio parameters to be set exactly as listed.

10.2. Safety distance



Concentrated energy from a directional antenna may pose a health hazard to humans.Do not allow people to come closer to the antenna than the distances listed in the tablebelow when the transmitter is operating. More information on RF exposure can be found online at the following website (OET Bulletin No. 65):
http://www.fcc.gov/oet/info/documents/bulletins



Concentré d'énergie à partir d'une antenne directionnelle peut poser un risque pour lasanté humaine. Ne pas permettre aux gens de se rapprocher de l'antenne que les distancesindiquées dans le tableau ci-dessous lorsque l'émetteur est en marche. Plusd'informations sur l'exposition aux RF peut être trouvé en ligne à l'adresse suivante (OET Bulletin No. 65): *www.fcc.gov/oet/info/documents/bulletins*[1]

The minimal safe distance is typically ensured by the antenna position on a mast. When special installation is required, the conditions of the standard EN 50385: 2002 have to be met. The distance between the persons and antenna shown in the table below comply with all applicable standards for human exposure of general public to RF electromagnetic fields.

Tab. 10.1: Minimum Safety Distance 300–470 MHz

300–470 MHz/70 cm band – 10 W RF power					
Antenna code	Antenna description	Gain G [dBi]	Gain G [–]	Dist. where the FCC limits are met for	
				General Population / Uncontrolled Exposure [cm]	General Population / Controlled Exposure [cm]
OV380.1	single dipole	4.6	2.9	130	60
OV380.2	stacked double dipole	7.6	5.8	180	80
SA380.3	3 element directional Yagi	7.6	5.8	180	80

[1] http://www.fcc.gov/oet/info/documents/bulletins

300–470 MHz/70 cm band – 10 W RF power					
SA380.5	5 element directional Yagi	8.7	7.4	200	90
SA380.9	9 element directional Yagi	12.5	17.8	310	140

Tab. 10.2: Minimum Safety Distance 135–175 MHz

135 - 175 MHz / 2 m band – 10 W RF power					
Antenna code	**Antenna description**	**Gain G [dBi]**	**Gain G [–]**	**Dist. where the FCC limits are met for**	
				General Population / Uncontrolled Exposure [cm]	**General Population / Controlled Exposure [cm]**
OV138.1	single dipole	4.6	2.9	155	55
OV138.2	stacked double dipole	7.6	5.8	215	75
SA138.3	3 element directional Yagi	8.0	6.3	225	80
SA138.5	5 element directional Yagi	10.0	10.0	285	100

Tab. 10.3: Minimum Safety Distance 135–175 MHz according to RSS-102

135 - 175 MHz / 2 m band – 10 W RF power					
Antenna code	**Antenna description**	**Gain G [dBi]**	**Gain G [–]**	**Dist. where the limits are met for**	
				General Population / Uncontrolled Exposure [cm]	**General Population / Controlled Exposure [cm]**
OV138.1	single dipole	4.6	2.9	170	70
OV138.2	stacked double dipole	7.6	5.8	240	95
SA138.3	3 element directional Yagi	8.0	6.3	250	100
SA138.5	5 element directional Yagi	10.0	10.0	315	125

10.3. High temperature



If the RipEX2 is operated in an environment where the ambient temperature exceeds 55 °C, the RipEX2 must be installed within a restricted access location to prevent human contact with the enclosure heatsink.

10.4. 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.

10.5. Explosive atmospheres



RipEX2 unit shall be used in hazardous locations with following specification:
Ⓔx II 3G Ex ic IIA T4 Gc
according to IEC 60079-0 standard under following conditions:

- Installation has to be done with conformity to standard EN 60079-25 Explosive atmospheres - Intrinsically safe electrical systems, with special attention to lightning protection.
- The device does not meet the requirements of Chapter 6.3.13. Dielectric strength requirement of the EN 60079-11: 2012, this must be taken into account during installing the device (connectors - or their individual pins - are connected to the housing).
- The unit must be powered with an intrinsically safe power source.
- The antenna has to be installed outside the hazardous zone.
- Do not manipulate the RipEX2 (e.g. plug or unplug connectors) unless powered down or the area is known to be non-hazardous.
- Only USB equipment dedicated for hazardous locations shall remain connected permanently.
- Repairs, including exchange of internal battery, shall only be undertaken by an authorized repair shop.
- This equipment is not intended to withstand particularly adverse service conditions (for example, rough handling, humidity effects, ambient temperature variations, effects of chemical agents, corrosion) in combination with an explosive atmosphere.



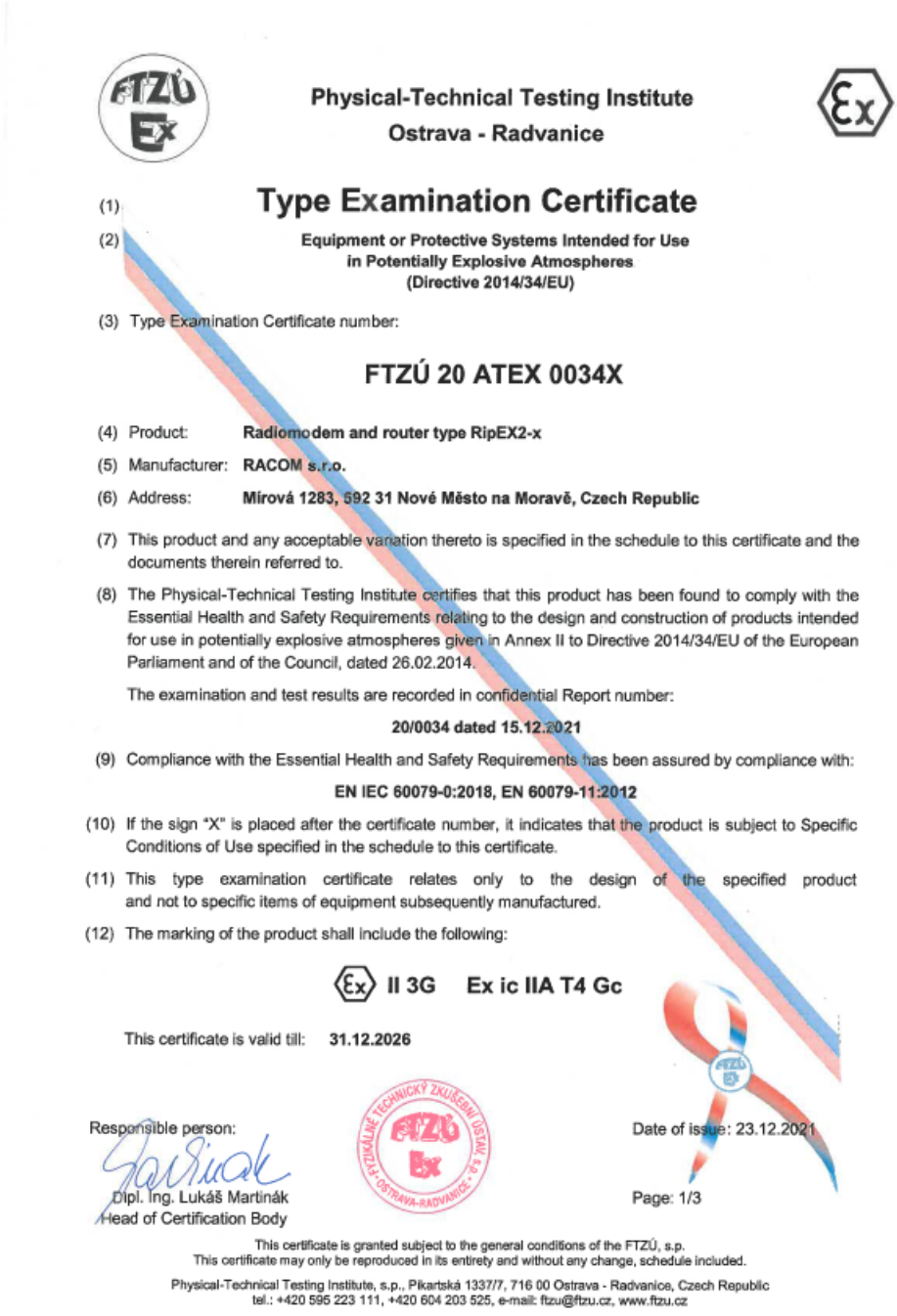
Important

DO NOT HANDLE UNLESS THE AREA IS KNOWN TO BE NON-HAZARDOUS

For individual interface maximum voltage and current see the following table:

Tab. 10.4: Maximum voltage and current of individual interfaces

IN/OUT	Max. voltage	Max. current	Min. cross section of Cu wire	Recommended
DC power	13.6 VDC	6 A	0.5 mm^2	V03VH-H 2×0.5
SI	13.6 VDC	10 mA	0.5 mm^2	V03VH-H 1×0.5
Alarm input	13.6 VDC	10 mA	0.5 mm^2	V03VH-H 1×0.5
Alarm output	DC power	0.2 A	0.5 mm^2	V03VH-H 1×0.5
Digital output	DC power	0.2 A	0.5 mm^2	V03VH-H 1×0.5
RS232	±15 VDC	60 mA	0.14 mm^2	LiYCY 4×0.14
RS485	±15 VDC	60 mA	0.14 mm^2	LiYCY 4×0.14
USB	5 VDC	0.5 A	0.5 mm^2	
Ethernet RJ45	±2.5 VDC			STP CAT 5E



Physical-Technical Testing Institute
Ostrava - Radvanice

Type Examination Certificate

(1)

(2) Equipment or Protective Systems Intended for Use in Potentially Explosive Atmospheres (Directive 2014/34/EU)

(3) Type Examination Certificate number:

FTZÚ 20 ATEX 0034X

(4) Product: **Radiomodem and router type RipEX2-x**

(5) Manufacturer: **RACOM s.r.o.**

(6) Address: **Mírová 1283, 592 31 Nové Město na Moravě, Czech Republic**

(7) This product and any acceptable variation thereto is specified in the schedule to this certificate and the documents therein referred to.

(8) The Physical-Technical Testing Institute certifies that this product has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of products intended for use in potentially explosive atmospheres given in Annex II to Directive 2014/34/EU of the European Parliament and of the Council, dated 26.02.2014.

The examination and test results are recorded in confidential Report number:

20/0034 dated 15.12.2021

(9) Compliance with the Essential Health and Safety Requirements has been assured by compliance with:

EN IEC 60079-0:2018, EN 60079-11:2012

(10) If the sign "X" is placed after the certificate number, it indicates that the product is subject to Specific Conditions of Use specified in the schedule to this certificate.

(11) This type examination certificate relates only to the design of the specified product and not to specific items of equipment subsequently manufactured.

(12) The marking of the product shall include the following:

Ex II 3G Ex ic IIA T4 Gc

This certificate is valid till: **31.12.2026**

Responsible person:
Dipl. Ing. Lukáš Martinák
Head of Certification Body

Date of issue: 23.12.2021

Page: 1/3

This certificate is granted subject to the general conditions of the FTZÚ, s.p.
This certificate may only be reproduced in its entirety and without any change, schedule included.

Physical-Technical Testing Institute, s.p., Pikartská 1337/7, 716 00 Ostrava - Radvanice, Czech Republic
tel.: +420 595 223 111, +420 604 203 525, e-mail: ftzu@ftzu.cz, www.ftzu.cz

Fig. 10.1: ATEX type examination certificate 1/3

Physical-Technical Testing Institute
Ostrava - Radvanice

(13) **Schedule**

(14) **Type Examination Certificate No. FTZÚ 20 ATEX 0034X**

(15) Description of Product:

The apparatus Radiomodem and router type RipEX2-x is widely configured compact radio modem and IP router.

The electronics are on PCBs placed inside aluminum enclosure.

Intrinsically safe parameters:

Power supply DC Power:
U_i =13.6 V, I_i = 6 A, P_i = 60 W, C_i = 4.9 µF, L_i = 0

Interface SI:
U_i = 13.6 V, Ii = 10 mA, C_i = 120 nF, L_i = 0

Interface Alarm IN:
U_i = 13.6 V, Ii = 10 mA, C_i = 120 nF, L_i = 0

Interface Alarm OUT:
U_i = 13.6 V, I_i = 0.2 A, P_i = 0.9 W, C_i = 2 nF, L_i = 0

Interface RS232:
U_i = ±15 V, I_i = 60 mA, C_i = 1 µF, L_i = 0
U_o = ±15 V, I_o = 60 mA, C_o = 99 µF, L_o = 1 mH

Interface RS485
U_i = ±15 V, I_i = 60 mA, C_i = 1 µF, L_i = 0
Uo = ±15 V, Io = 60 mA, C_o = 99 µF, Lo = 1 mH

Interface Eth:
U_i = ±2.5 V, I_i = 40 mA, C_i = 400 nF, L_i = 0
U_o = ±2.5 V, I_o = 40 mA, C_o = 100 µF, Li = 40 mH

Interface USB:
U_i = 5 V, I_i = 0.5 A, C_i = 400 nF, L_i = 0, C_o = 68 µF, L_i = 0
U_o = 5 V, I_o = 0.5 A, C_o = 100 µF, Li = 2 mH

Interface DI:
U_i = 13.6 V, C_i = 10 nF, L_i = 0

Interface differential DI (P,N):
U_{IPN} = 13.6 V, I_{IPN} = 25 mA, C_i = 10 nF, L_i = 0

Interface DO:
U_i = 13.6V, I_i = 0.2 A, P_i = 0.9 W, C_i = 2 nF, L_i = 0

Interface AUX:
U_i = 5 V, C_i = 6 µF, L_i = 0, C_o = 99 µF, L_o = 2 mH

Ambient temperature:
Ta = -40°C to +70°C

Responsible person:
Dipl. Ing. Lukáš Martinák
Head of Certification Body

Date of issue: 23.12.2021

Page: 2/3

This certificate is granted subject to the general conditions of the FTZÚ, s.p.
This certificate may only be reproduced in its entirety and without any change, schedule included.

Physical-Technical Testing Institute, s.p., Pikartská 1337/7, 716 00 Ostrava - Radvanice, Czech Republic
tel.: +420 595 223 111, +420 604 203 525, e-mail: ftzu@ftzu.cz, www.ftzu.cz

Fig. 10.2: ATEX type examination certificate 2/3

Physical-Technical Testing Institute
Ostrava - Radvanice

(13) **Schedule**

(14) **Type Examination Certificate No. FTZÚ 20 ATEX 0034X**

(16) Report Number: 20/0034

(17) Specific Conditions of Use:

1. Instruction manual must be taken into account during installation.
2. The antenna has to be installed outside of hazardous atmosphere.
3. The apparatus cannot only be manipulated when explosive atmosphere is present and the apparatus is not disconnected from power supply.
4. Only USB devices dedicated for Zone 2, 1 or 0 can be connected permanently.
5. SFP modules have to be dedicated for explosive atmosphere.

(18) Essential Health and Safety Requirements:

Compliance with the Essential Health and Safety Requirements is covered by standards mentioned in clause (9) of this certificate.

(19) Drawings and Documents:

Document/Drawings:	*Rev./Ver.:*	*Date:*	*No. of Pages:*
User manual	1.11	03.05.2021	189
ATEX manual	2.0	19.12.2021	9
Label	--	05.10.2021	1
BLOKDIAGRAMRIPEX2	--	22.07.2019	1
MBM7_aescpu_V2	v2	25.10.2019	26
mbr7_400-470MHz	7.7	17.10.2014	17
mbm7_noaescpu list of component	v2	12.11.2019	27
mbr7_400-470MHz list of component	v7	9.6.2020	26
MBM7_noaescpu PCB layout	-	10.11.2020	2
mbr7_400-470MHz PCB layout	3	9.6.2020	2

Responsible person:
Dipl. Ing. Lukáš Martinák
Head of Certification Body

Date of issue: 23.12.2021

Page: 3/3

This certificate is granted subject to the general conditions of the FTZÚ, s.p.
This certificate may only be reproduced in its entirety and without any change, schedule included.

Physical-Technical Testing Institute, s.p., Pikartská 1337/7, 716 00 Ostrava - Radvanice, Czech Republic
tel.: +420 595 223 111, +420 604 203 525, e-mail: ftzu@ftzu.cz, www.ftzu.cz

Fig. 10.3: ATEX type examination certificate 3/3

10.6. 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 radio modem and other terminal equipment the supply must always be disconnected upon connecting or disconnecting the cable to the radio modem 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.

10.7. 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.

10.8. EU Compliance

10.8.1. RoHS, WEEE and WFD



RACOM
www.racom.eu

EU DECLARATION OF CONFORMITY

Equipment	RipEX, RipEX2 RAy2, RAy3 M!DGE2, M!DGE3 RipEX-HS, RipEX2-HS
Manufacturer	RACOM s.r.o. Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The equipment described above is in conformity with the Directive 2011/65/EU of the European Parliament and of the Council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS), as amended by Directive (EU) 2015/863, Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) and Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH).

REACH: Equipment mentioned above do not contain any substances from the "Candidate List of Substances of Very High Concern" with more than 0.1% of the global weight of the delivered item (without packaging of the item)

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, 3rd May 2024
Marek Bobula, Technical director

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. 1.4

Fig. 10.4: 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.

10.8.2. EU restrictions or requirements notice

Radio equipment used within the EU countries listed below:

- there are restrictions on putting into service or
- any requirements for authorisation of use.

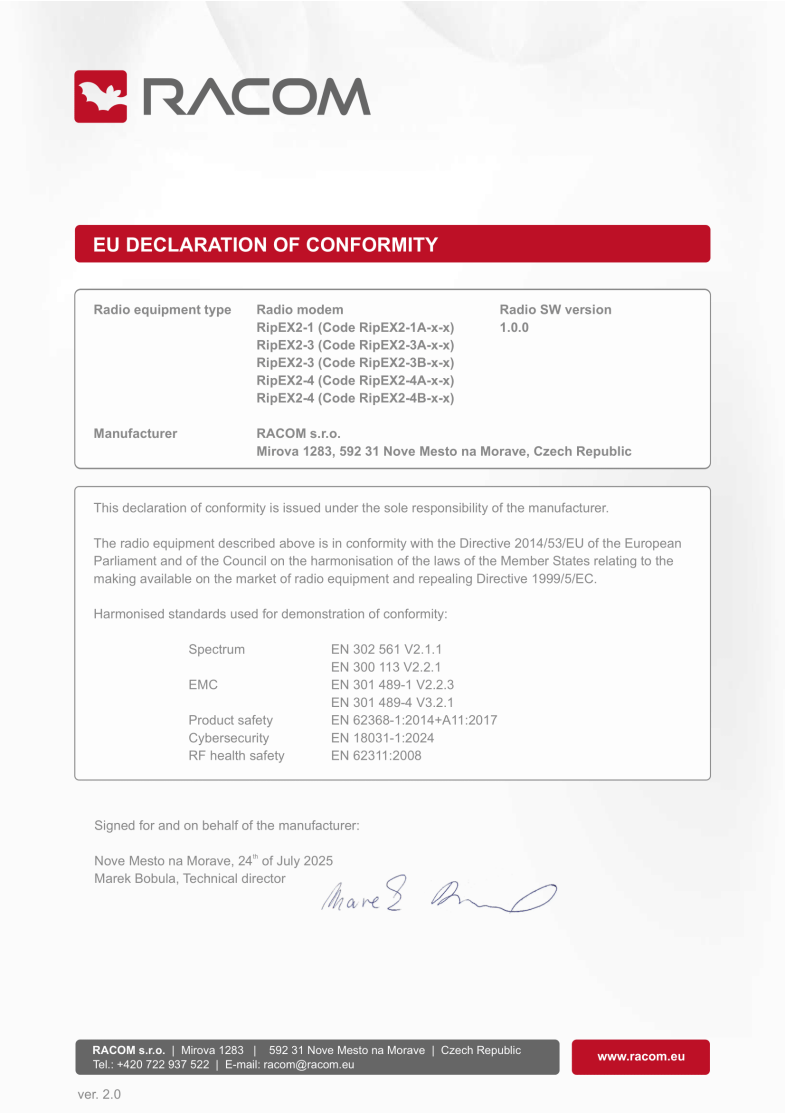


BE	BG	CZ	DK	DE	EE	IE
EL	ES	FR	HR	IT	CY	LV
LT	LU	HU	MT	NL	AT	PL
PT	RO	SI	SK	FI	SE	UK

Fig. 10.5: EU restrictions or requirements

The RipEX2 radio modem predominantly operates within frequency bands that require a site license be issued by the radio regulatory authority with jurisdiction over the territory in which the equipment is being operated.

10.8.3. EU Declaration of Conformity RED



RACOM

EU DECLARATION OF CONFORMITY

Radio equipment type	Radio modem	Radio SW version
	RipEX2-1 (Code RipEX2-1A-x-x)	1.0.0
	RipEX2-3 (Code RipEX2-3A-x-x)	
	RipEX2-3 (Code RipEX2-3B-x-x)	
	RipEX2-4 (Code RipEX2-4A-x-x)	
	RipEX2-4 (Code RipEX2-4B-x-x)	
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:

Spectrum	EN 302 561 V2.1.1
	EN 300 113 V2.2.1
EMC	EN 301 489-1 V2.2.3
	EN 301 489-4 V3.2.1
Product safety	EN 62368-1:2014+A11:2017
Cybersecurity	EN 18031-1:2024
RF health safety	EN 62311:2008

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 24th of July 2025
Marek Bobula, Technical director

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. 2.0

Fig. 10.6: EU Declaration of Conformity RED

10.9. Compliance Federal Communications Commission and Innovation, Science and Economic Development Canada

Installation and usage of RipEX2 radio modems must be done by qualified and experienced person with proper training and technical knowledge such as path planning, licensing and regulatory requirements.

FCC Part 15.19(a):

“This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause undesired operation.”

FCC Part 15 Clause 15.21:

“Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment”

Tab. 10.5: Compliance FCC and ISED

Code	FCC part	FCC ID	ISED	IC number
RipEX2-1A	90	SQT-RIPEX2-1A	RSS-102	24993-RIPEX21A
RipEX2-3A	90	pending	RSS-102	pending
RipEX2-3B	90	pending	RSS-102	pending
RipEX2-4A	90	SQT-RipEX2-4A	RSS-102	24993-RIPEX24A
RipEX2-9A	90	pending	RSS-102	pending

Possible values for channels, channel spacing and occupied bandwidth fulfilling FCC rules are shown in *Chapter 9, Technical parameters*.



Important

The radio operator is responsible for setting the radio parameters of the radio modem exactly in accordance with the valid frequency license issued by national frequency authority, and all radio parameters to be set exactly as listed.

TCB **TCB**

GRANT OF EQUIPMENT AUTHORIZATION

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

TUV SUD America Inc.
401 Edgewater Place Suite #500
Wakefield, MA 01880

Date of Grant: 07/01/2021
Application Dated: 07/01/2021

Racom
Mirova cp. 1283
Nove Mesto na Morave, 592 31
Czech Republic

Attention: Jiri Hruska , Programme Manager

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: SQT-RIPEX2-1A
Name of Grantee: Racom
Equipment Class: Licensed Non-Broadcast Station Transmitter
Notes: Radio modem and router

Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
EF ES	90	150.0 - 170.0	10.0	66.0 Hz	4K80G1D
EF ES	90	150.0 - 170.0	10.0	66.0 Hz	9K71G1D
EF ES	90	150.0 - 170.0	10.0	66.0 Hz	19K1G1D
EF ES	90	150.0 - 170.0	10.0	66.0 Hz	3K08G1D
EF ES	90	150.0 - 170.0	10.0	66.0 Hz	7K73G1D
EF ES	90	150.0 - 170.0	10.0	66.0 Hz	15K6G1D

Power listed is rated. The device is designed for professional installation, users and installers must be provided with appropriate antenna installation instructions and transmitter operating conditions, including antenna co-location requirements of § 1.1307(b)(3), for satisfying RF exposure compliance. The antennas used for this transmitter shall be installed to provide a separation distance from all persons during normal operation as documented in this filing. RF exposure compliance may need to be addressed at the time of licensing.

EF: This device may contain functions that are not operational in U.S Territories except as noted in the filing. This grant has extended frequencies as noted in the filing and Section 2.927(b) applies to this authorization.

ES: This equipment is capable of supporting a minimum data rate of 4800 bits per second per 6.25 kHz of channel bandwidth.

Fig. 10.7: Grant for RipEX2-1A

TCB

GRANT OF EQUIPMENT AUTHORIZATION

TCB

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

TUV SUD America Inc.
10 Centennial Drive
Peabody, MA 01960

Date of Grant: 01/23/2020

Application Dated: 01/22/2020

Racom
Mirova cp. 1283
Nove Mesto na Morave, 592 31
Czech Republic

Attention: Jiri Hruska , Programme Manager

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: SQT-RIPEX2-4A
Name of Grantee: Racom
Equipment Class: Licensed Non-Broadcast Station Transmitter
Notes: Radio modem and router

Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	19K8G1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	15K5F1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	10K0G1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	7K50F1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	5K0G1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	3K60F1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	19K8G1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	15K5F1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	10K0G1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	7K50F1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	5K0G1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	3K60F1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	19K8G1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	15K5F1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	10K0G1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	7K50F1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	5K0G1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	3K60F1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	19K8G1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	15K5F1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	10K0G1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	7K50F1D

Fig. 10.8: TCB Grant for RipEX2-4A

EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	5K0G1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	3K60F1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	19K8G1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	15K5F1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	10K0G1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	7K50F1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	5K0G1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	3K60F1D

Output power listed is rated conducted power. The device is designed for professional installation, users and installers must be provided with appropriate antenna installation instructions and transmitter operating conditions, including antenna co-location requirements of § 1.1307(b)(3), for satisfying RF exposure compliance. The antennas used for this transmitter shall be installed to provide a separation distance from all persons during normal operation as documented in this filing. RF exposure compliance may need to be addressed at the time of licensing.

EF: This device may contain functions that are not operational in U.S Territories except as noted in the filing. This grant has extended frequencies as noted in the filing and Section 2.927(b) applies to this authorization.

ES: This equipment is capable of supporting a minimum data rate of 4800 bits per second per 6.25 kHz of channel bandwidth.

Fig. 10.9: TCB authorization



TÜV SÜD America

FCB Technical Acceptance Certificate

CB Number: US0156

ISSUED TO	➢	**Racom** **Mirova cp. 1283** **Nove Mesto na Morave, Czech Republic**
CERTIFICATION No.	➢	**24993-RIPEX21A**
DESCRIPTION	➢	**Wireless modem router**
TYPE OF EQUIPMENT	➢	**Land-Mobile Transmitter and Receiver (27.41–960 MHz)**
HVIN(s)	➢	**RipEX2-1**
PMN(s)	➢	**RipEX2-1**
FVIN(s)	➢	**n/a**
TYPE OF LISTING:	➢	**New Single Certification**
ANTENNA INFORMATION	➢	**10 dBi**
RF EVALUATION TYPE	➢	**RF Evaluation**
MANUFACTURING No.	➢	**24993**
REPRESENTATIVE No.	➢	**10842A**
TEST LAB No.	➢	**3036B**
TESTING LABORATORY	➢	**Professional Testing (EMI), Inc.** **1601 North A.W. Grimes Blvd., Suite B** **Round Rock, Texas 78665**

Authorised by: Issue Date: 1 July 2021

Title of Signatory: Senior Technical Certifier Number: CB-21-106 Issue: 1

On Behalf of TÜV SÜD America

I hereby attest that the subject equipment was tested and found in compliance with the above-noted specification.

Certification of equipment means only that the equipment has met the requirements of the above-noted specification. Licence applications, where applicable to use certified equipment, are acted on accordingly by the ISED issuing office and will depend on the existing radio environment, service and location of operation. This certificate is issued on condition that the holder complies and will continue to comply with the requirements and procedures issued by ISED. The equipment for which this certificate is issued shall not be manufactured, imported, distributed, leased, offered for sale or sold unless the equipment complies with the applicable technical specifications and procedures issued by ISED.;

J'atteste, par la présente, que le matériel a fait l'objet d'essai et a été jugé conforme à la spécification ci-dessus.

La certification du matériel signifie seulement que le matériel a satisfait aux exigences de la norme indiquée ci-dessus. Les demandes de licences nécessaires pour l'utilisation du matériel certifié sont traitées en conséquence par le bureau de délivrance d'ISDE et dépendent des conditions radio ambiantes, du service et de l'emplacement d'exploitation. Le présent certificat est délivré à la condition que le titulaire satisfasse et continue de satisfaire aux exigences et aux procédures d'ISDE. Le matériel à l'égard duquel le présent certificat est délivré ne doit pas être fabriqué, importé, distribué, loué, mis en vente ou vendu à moins d'être conforme aux procédures et aux spécifications techniques applicables publiées par ISDE.

Certified Equipment shall not be distributed, leased, sold or offered for sale in Canada before the details of the certification have been added to the REL. This certificate has been issued in accordance with the Testing and Certification Regulations of TÜV SÜD America. For further details related to this certification please contact Certification@tuvam.com

UCB_F_10.09 Rev 1 TÜV SÜD America, Inc. 10 Centennial Drive, Peabody, MA 01960, USA Page 1 of 2

Fig. 10.10: FCB certificate for RipEX2-1A



TÜV SÜD America

FCB Technical Acceptance Certificate

CB Number: US0156

ISSUED TO	➢ **RACOM s.r.o.** **RACOM, Mirova 1283** **Nove Mesto na Morave 592 31 Czech Republic**
CERTIFICATION No.	➢ **24993-RIPEX24A**
DESCRIPTION	➢ **Wireless modem router**
TYPE OF EQUIPMENT	➢ **Land-Mobile Transmitter and Receiver (27.41–960 MHz)**
HVIN(s)	➢ **RipEX2-4**
PMN(s)	➢ **RipEX2-4**
FVIN(s)	➢ **N/A**
TYPE OF LISTING:	➢ **New Single Certification**
ANTENNA INFORMATION	➢ **External Antenna, 12.5 dBi Max**
RF EVALUATION TYPE	➢ **RF Evaluation**
MANUFACTURING No.	➢ **24993**
REPRESENTATIVE No.	➢ **10842A**
TEST LAB No.	➢ **3036B**
TESTING LABORATORY	➢ **Professional Testing (EMI) Inc.** **11400 Burnet Road, Austin, Texas, 78758, United States** **Tel: 512-244-3371; Fax: 512-244-1846** **Contact: Larry Finn; E-mail: lfinn@ptitest.com**

Authorised by:

Title of Signatory: Wireless Certification Manager

On Behalf of TÜV SÜD America

Issue Date: 12th March 2020

Number: CB-19-0187 Issue: 1

I hereby attest that the subject equipment was tested and found in compliance with the above-noted specification.

Certification of equipment means only that the equipment has met the requirements of the above-noted specification. Licence applications, where applicable to use certified equipment, are acted on accordingly by the ISED issuing office and will depend on the existing radio environment, service and location of operation. This certificate is issued on condition that the holder complies and will continue to comply with the requirements and procedures issued by ISED. The equipment for which this certificate is issued shall not be manufactured, imported, distributed, leased, offered for sale or sold unless the equipment complies with the applicable technical specifications and procedures issued by ISED.;

J'atteste, par la présente, que le matériel a fait l'objet d'essai et a été jugé conforme à la spécification ci-dessus.

La certification du matériel signifie seulement que le matériel a satisfait aux exigences de la norme indiquée ci-dessus. Les demandes de licences nécessaires pour l'utilisation du matériel certifié sont traitées en conséquence par le bureau de délivrance d'ISDE et dépendent des conditions radio ambiantes, du service et de l'emplacement d'exploitation. Le présent certificat est délivré à la condition que le titulaire satisfasse et continue de satisfaire aux exigences et aux procédures d'ISDE. Le matériel à l'égard duquel le présent certificat est délivré ne doit pas être fabriqué, importé, distribué, loué, mis en vente ou vendu à moins d'être conforme aux procédures et aux spécifications techniques applicables publiées par ISDE.

Certified Equipment shall not be distributed, leased, sold or offered for sale in Canada before the details of the certification have been added to the REL. This certificate has been issued in accordance with the Testing and Certification Regulations of TÜV SÜD America. For further details related to this certification please contact Certification@tuvam.com

Fig. 10.11: FCB certificate for RipEX2-4A 1/2

America

Radio Details

Number: CB-19-0187 Issue 1

Frequency Min (MHz)	Frequency Max (MHz)	RF Power (W) Min	RF Power (W) Max	Emission Designator	Specification Issue
406.1	430.0	11.8	11.8	19K8G1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	15K5F1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	10K0G1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	7K50F1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	5K00G1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	3K60F1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	19K8G1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	15K5F1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	10K0G1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	7K50F1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	5K00G1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	3K60F1D	RSS-119 Issue 12

Page 2 of 2

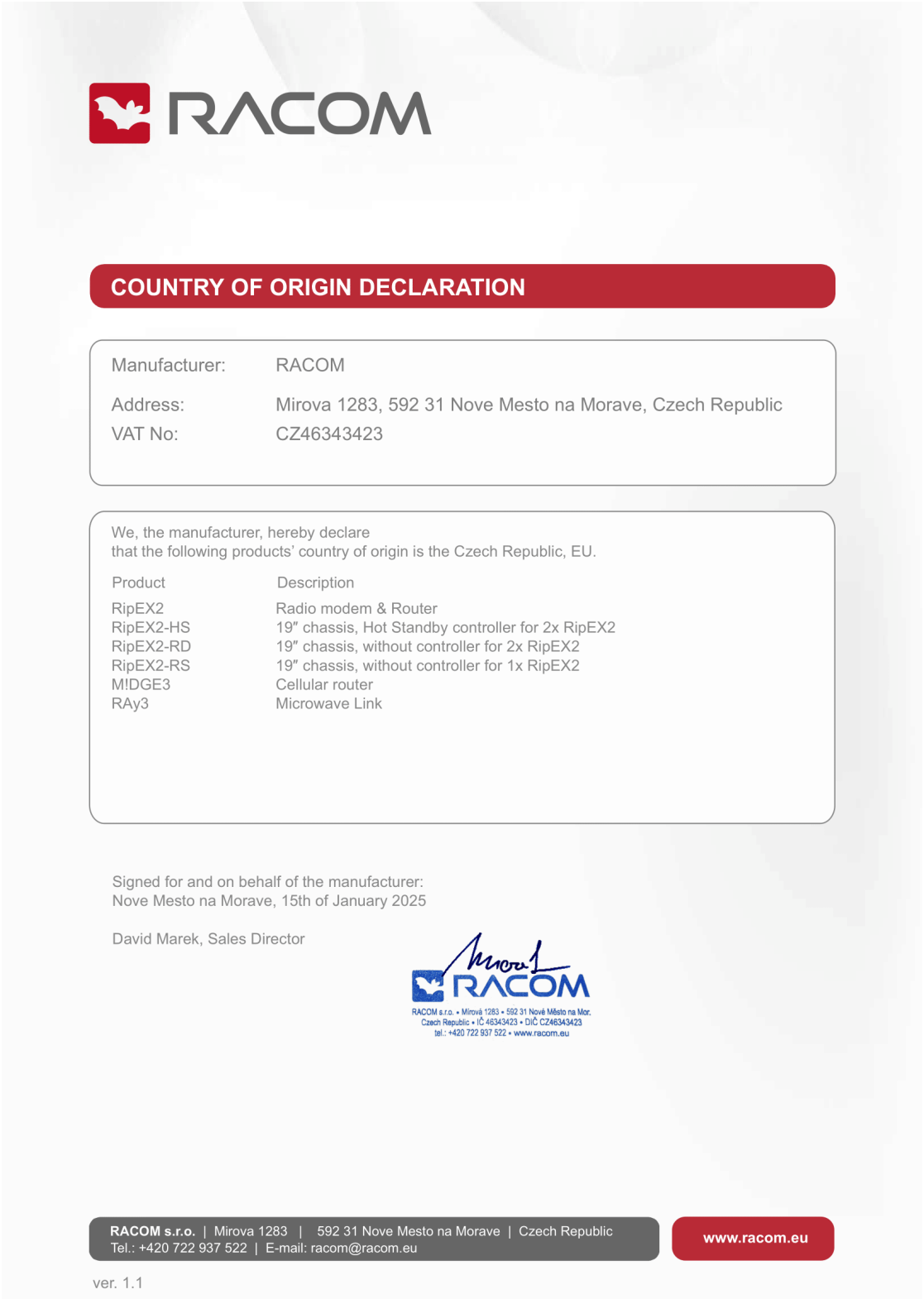
Fig. 10.12: FCB certificate 2/2

10.10. Compliance ANATEL Brasil

RipEX2-4A : This equipment is approved by ANATEL under number 16763-20-08917.



10.11. Country of origin



RACOM

COUNTRY OF ORIGIN DECLARATION

Manufacturer: RACOM

Address: Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

VAT No: CZ46343423

We, the manufacturer, hereby declare
that the following products' country of origin is the Czech Republic, EU.

Product	Description
RipEX2	Radio modem & Router
RipEX2-HS	19″ chassis, Hot Standby controller for 2x RipEX2
RipEX2-RD	19″ chassis, without controller for 2x RipEX2
RipEX2-RS	19″ chassis, without controller for 1x RipEX2
M!DGE3	Cellular router
RAy3	Microwave Link

Signed for and on behalf of the manufacturer:
Nove Mesto na Morave, 15th of January 2025

David Marek, Sales Director

RACOM

RACOM s.r.o. • Mirová 1283 • 592 31 Nové Město na Mor.
Czech Republic • IČ 46343423 • DIČ CZ46343423
tel.: +420 722 937 522 • www.racom.eu

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. 1.1

10.12. 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.

10.12.1. EU Compliance

10.12.1.1. RoHS, WEEE and WFD



RACOM
www.racom.eu

EU DECLARATION OF CONFORMITY

Equipment	**RipEX, RipEX2** **RAy2, RAy3** **M!DGE2, M!DGE3** **RipEX-HS, RipEX2-HS**
Manufacturer	**RACOM s.r.o.** **Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic**

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The equipment described above is in conformity with the Directive 2011/65/EU of the European Parliament and of the Council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS), as amended by Directive (EU) 2015/863, Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) and Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH).

REACH: Equipment mentioned above do not contain any substances from the "Candidate List of Substances of Very High Concern" with more than 0.1% of the global weight of the delivered item (without packaging of the item)

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, 3rd May 2024
Marek Bobula, Technical director

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. 1.4

Fig. 10.13: 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.

10.12.1.2. EU restrictions or requirements notice

Radio equipment used within the EU countries listed below:

- there are restrictions on putting into service or
- any requirements for authorisation of use.



BE	BG	CZ	DK	DE	EE	IE
EL	ES	FR	HR	IT	CY	LV
LT	LU	HU	MT	NL	AT	PL
PT	RO	SI	SK	FI	SE	UK

Fig. 10.14: EU restrictions or requirements

The RipEX2 radio modem predominantly operates within frequency bands that require a site license be issued by the radio regulatory authority with jurisdiction over the territory in which the equipment is being operated.

10.13. RipEX2 Availability and service life time

Annual availability is >= 99.99 % (for MTTR = 8 hours and P-t-P scenario)

The Availability depends on specific network design and Service availability. Availability can be increased by decreasing MTTR. Availability calculation needs to be done for each network element separately.

RipEX2 redundant solution within Field Replaceable Units fully achieving the level availability and reliability for the Core elements.

Note

Core networks elements(repeaters/bases) are typically designed for high availability i.e. needs to be 99.999% available with any single component (radio node) fails.

Service life of system >= 15 years

10.14. RipEX2 maintenance

Action	Period	Note
Visual check – Antenna: Draining hole on dipole must be downward pointing There should be no damaged elements on the antenna Angle of elevation of antenna Azimuth (angle of horizontal deviation) in accordance with design	Quarterly	
Visual check – Coaxial Cable: Mechanical damage Solar degradation Entire cable correctly mounted to surface Connectors tightened to function optimally Self-vulcanizing tape used for all connections requiring insulation PSV & RF measurements	Annually	
Visual check – Cabinet: Mechanical damage Damage resulting in lower categorization for cabinet coverage Bushings for running cables	Annually	
Visual check – Electricity Supply: Insulation damage Connection to terminals	Annually	
Visual check – Accumulator: Capacity in accordance with customer requirements Condition of the accumulator	Annually	
Functionality check – power source: Overcharging Accumulator damage	Annually	
Full utilization of provided protective coverings	Annually	
Remove any items which are not part of the installation	Annually	
Fix and secure makeshift installations correctly	Annually	
Check grounding connections	As required	
Check lightning arrester : connectors must be tightened	As required	
Check data connectors connected including securing screws	Annually	
Evaluate the RSS and MSE values as a preventive measure against the failure of the connection. RSS and MSE values be similar to those at time of commissioning.	Monthly	*Section 8.5.5, “Radio signal statistics”* *Section 8.7.2, “RSS ping”* *Section 8.5.9.3, “Cellular signal statistics”*

Action	Period	Note
Check activity logs to detect abnormalities in data transmissions	Monthly	*Section 8.5.3, "Radio protocol statistics"* *Section 8.5.4, "Radio protocol non-addressable statistics"* *Section 8.5.9.2, "Cellular state statistics"*
Check if internal temperature alarm has been triggered	Monthly	*Section 8.4, "Events"* *Section 8.2.1, "Measurements"*
Check that firmware is latest stable version – upgrading FW recommended when new features required	As required	*Firmware RipEX2*[2]

If you are unsure on any of the above, please contact RACOM technical support.

[2] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr2

Appendix A. Security Hardening Procedure

RipEX2/M!DGE3 are wireless cellular IP-enabled telecommunication devices providing a 24/7 reliable service for wireless data transfer in mission-critical applications like Industrial control systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems.

This appendix contains several steps that can be considered when deploying wireless telecommunications infrastructures.

If you discover any vulnerability, please report them to us by emailing vulnerability@racom.eu or via technical support.

A.1. Password and accounting

Use strong password for an **"Admin" Role** (full access)
- SETTINGS > Security > Local authentication > User accounts

Configure a **strong password** for all users. Consider changing the "Password complexity rules" feature
- SETTINGS > Security > Local authentication > Settings
- Using complex passwords is your first line of defense in protecting your device. Consider periodic updates
- The recommended length is at least 8-10 characters including A-z, 0-9 and special characters (@?* etc.)

Role-based access control (RBAC) enables you to assign privileges and access rights to administrative/read-only users through role assignment. You create user accounts (**local authentication** or remote **RADIUS**) and assign them roles via which they can access RipEX2/M!DGE3 GUI or API.
- There are four different levels of user access privileges – they are bound with four different user access roles:
  Guest
  Technician
  Security technician
  Administrator
- *Note*: You may export Local authentication users and import them to other units in your network. You do not need to create them separately in each device
  The file consists of hashed/salted passwords, i.e. not readable and non backwards deductible

Web inactivity timeout
- 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
- ADVANCED > Generic > UserAccess > Web inactivity timeout
- *Note:* A mechanism against brute-force attacks is implemented. When the 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.

A.2. Physical access

Restrict physical access to the device to only authorized personnel.

Disable physical ports which are not used
Ethernet ports

- SETTINGS > Interfaces > Ethernet > Ports
- Disable (ETH 1 to ETH 4 are by defaults enabled, ETH5 disabled)

Serial ports
- SETTINGS > Interfaces > COM

USB port
- for USB/ETH and USB/WiFi management access (by default enabled)
- SETTINGS > Device > Unit > Service USB

Cellular ports (if any)
- SETTINGS > Interfaces > Cellular > MAIN/EXT (by default enabled)

Wi-Fi (if any)
- SETTINGS > Interfaces > Wi-Fi (by default enabled)

Tamper detection
RipEX2 and M!DGE3 units are equipped by case opening detection. The behaviour in case of this event shall be set in menu SETTINGS > Device > Events > Tamper.

A.3. Encrypt data on Radio network

Encrypting your wireless radio data prevents anyone who might be able to access your network from viewing it. Radio traffic can be encrypted via AES-256-CCM (passphrase or key), or utilizing IPsec/OpenVPN secure VPN options (but these are not bandwidth-optimized options for a Radio channel).

Radio AES256
For the encryption is possible to set primary and secondary Passphrase or Key. This option allows to change credentials in the whole network without service outage.
The radio traffic encryption has an additional option AES-256-CCM + KEX, which enables periodical key replacement.
- SETTINGS > Interfaces > Radio > Encryption

VPN
- SETTINGS > VPN > IPsec
- SETTINGS > VPN > OpenVPN

A.4. Encrypt data on cellular network

Cellular networks are in control of operators and public APNs are connected to the public Internet. Any data sent or received by RipEX2 (EXT) or M!DGE3 (MAIN, EXT) can be captured by experienced hackers. If such data are not encrypted, sensitive data can be read by these hackers and misused.

It is highly recommended to **encrypt all sensitive data** via supported VPN options - **IPsec or OpenVPN**.

Note: Private APNs resemble private Radio networks. Such APNs are restricted from the Internet by the operator's firewalls and should be more secure. Nevertheless, it is still recommended to encrypt your sensitive data.

Note: Routing LAN2LAN (end2end) data through the operator’s APN/network is blocked by their firewalls and tunnelling or port-forwarding are the only ways to pass end2end data successfully.

A.5. Disable Remote access or configure it securely

Remote access is used to configure and manage remote units via bandwidth-friendly volumes of transmitted data. You must login to the local unit via username and password. There is no need to provide any other credentials to access other units remotely via Remote access. The security is based

on QSSH protocol (TCP port 8889) and a private key. Enable only the interfaces you will use for Remote access (by default Remote access is enabled for Radio interface, for all other interfaces is disabled):

- ADVANCED > Interfaces > Ethernet > Network interface - Default value is Off
- ADVANCED > Interfaces > Radio > Radio interface - Default value is On
- ADVANCED > Interfaces > Cellular > Cellular MAIN / EXT - Default value is Off
- ADVANCED > Interfaces > Wi-Fi EXT - Default value is Off

Or switch it off fully:

- SETTINGS > Security > Management access > Remote access

Hints for set in a secure way for enabled interfaces:

User generated Remote access key



Warning
The private key is the same for ALL manufactured units.

It is highly recommended to generate such a key in one unit and distribute it to all others within your network. No other unit with default key (or other user key) can access your units via Remote access.

- SETTINGS > Security > Credentials
  - to generate/download/upload the key
- SETTINGS > Security > Management access > Remote access
  - to set “user” key for Remote access
  - to define the user key ID

A.6. Exchange of certificates

It is recommended to change certificates for certificates trusted by the RipEX2 user.

The default certificates are part of installation of all units, so the replacement for your own certificates will increase the security of all processes and services (e.g. web access, radio encryption), which use certificates (see SETTINGS > Security > Credentials).

It is also possible to generate certificates with parameters required by the user application (see parameters in SETTINGS > Security > Credentials > Settings).

A.7. Services

Enable only **services** utilized on the device and disable all other services

Disable unused **SSH**

- ADVANCED > Security > Management access > Administration website > Enable SSH → Off

Disable SNMPv2c, if SNMP is required, **use SNMPv3**

- SETTINGS > Services > SNMP
- or use “SNMPv3”
  - security level: AuthPriv
  - Use secure Authentication and Encryption algorithms
  - Set strong passphrases

Change default **HTTPs** port

- SETTINGS (or ADVANCED) > Security > Management access > Administration website > HTTPS port

Disable **HTTP** access

- SETTINGS (or ADVANCED) > Security > Management access > Administration website > Enable HTTP → Off

Disable **SMS** or adjust allowed phone numbers

- SETTINGS > Services > SMS
  - Set strong SMS passphrase

Wi-Fi

- Only available if USB/Wi-Fi adapter for management access is used (plugged)
- Enable WPA2-PSK with strong password to ensure Wi-Fi security
  - SETTINGS > Security > Management access > Service USB > Wi-Fi > Security, Passphrase
- If not used, the feature can be disabled completely within the same menu

Disable **Netconf** interface

- Disable Netconf interface if it is not used or when Netconf interface is used change the Netconf default TCP port 830.
- ADVANCED > Security > Management access > NETCONF access

A.8. Firewall

Protect the unit via **Firewall** settings

- SETTINGS > Firewall > L2 / L3 / NAT
- Especially important if RipEX2/M!DGE3 has a public IP address!

Limit access to RipEX2/M!DGE3 GUI

- Only allow **authorized IPv4 addresses** to access your network. Each piece of hardware connected to a network has an assigned IPv4 address. You can restrict access to your network by filtering these IPv4 addresses within the L3 firewall.
- Local access can be restricted by filtering MAC addresses via L2 firewall (blacklist, whitelist).
- SETTINGS > Firewall > L2 / L3

A.9. HTTPS certificate

Since FW 2.1.0.0 and its feature Credentials, you can generate or upload your own certificates and keys, including **HTTPs**.

- SETTINGS > Security > Credentials
- SETTINGS > Security > Local authentication > Settings

A.10. Backup files

Configuration files are stored as **unencrypted JSON files** or encrypted zip files. It is possible to set that only encrypted files will be allowed and the rules for the password can be set as well.

- SETTINGS > Security > Policy

Complete backup should consist of:

- Configuration (see *7.6.2 Configuration*)
- User accounts (see *7.5.2 Local authentication*)
- Credentials (see *7.5.3 Credentials*)

Is is highly recommended to make backups often. Especially when:

- Post-Modification: Back up any changed sections (e.g., Configuration) immediately.
- Post-Update: Back up the system after every firmware update.

Note

Each user can only download a configuration file which includes configuration parameters available for a particular user level role.

A.11. Firmware

Keep the **firmware up-to-date**.

The latest FW can be downloaded from the RACOM website:

RipEX2 FW: *https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr2*

M!DGE3 FW: *https://www.racom.eu/eng/products/cellular-router-midge.html#dnl_fwr3*

Note

Standard FW versions are available quarterly, release notes with changes are available on the same web page.

Utilize **direct Upload and Activation** for locally connected RipEX2/M!DGE3 devices.

- SETTINGS > Device > Firmware > Local

Utilize **USB flash drive** - for FW upgrade via USB disk - this service is on by default, it can be disabled.

- SETTINGS > Device > Firmware > USB

Utilize **Firmware distribution** for RipEX2 networks in a bandwidth optimized way.

- FW distribution uses the authentication key during the process - the key is the same in all manufactured units - you can generate and use your own.
- SETTINGS > Services > Firmware distribution
- SETTINGS > Device > Firmware > Distributed

- ADVANCED > Device > Firmware distr. - receiver

A.12. Secure disposal guidelines

A.12.1. Physical Removal and Asset Prep

Uninstall the device from the deployment site. Remove all internal asset tags, location labels, or identification markings, and hand the unit over to an authorized personnel for data removal.

A.12.2. Configuration Purge

An authorized user with Admin privileges can manually clear device configuration. Navigate through the system menu as follows:

System Configuration:
SETTINGS > Device > Configuration
Select **Factory Reset** (reverts all general configuration settings).

User Accounts & Credentials:
Both User accounts and Credentials get removed with factory reset.

A.12.3. Comprehensive Data Deletion (Total Purge)

While the device does not store direct user files, it logs operational data and system statistics. To completely erase both the configuration segments (Configuration, Accounts, Credentials) and all accumulated operational data, execute the **Total Purge** function.

A.12.4. Hardware Destruction (Non-Operational Units)

The steps above assume the device is functional. If the unit cannot boot due to a unit failure and data removal is still strictly required, the chassis must be opened to mechanically remove or destroy the memory chip. Contact **Technical Support** for instructions before attempting physical disassembly.

A.13. Known vulnerabilities and their mitigations

A.13.1. Blast-RADIUS

This is a vulnerability that affects the RADIUS protocol.

The Blast-RADIUS attack allows a man-in-the-middle attacker between the RADIUS client and server to forge a valid protocol accept message in response to a failed authentication request.

For full security, we recommend to use VPN (IPsec/OpenVPN) connection to your RADIUS server.

Appendix B. Proprietary UDP/TCP ports

The following UDP and TCP ports are reserved for use in the unit's management system: 8800 - 9823. This entire range can be shifted to a different base value using the Advanced parameter DevicePortBase.

The following table lists some basic ports that may be important when configuring the unit.

Tab. B.1: RipEX2 proprietary UDP/TCP ports

UDP/TCP port number	Name
8881	COM1
8882	COM2
8883	COM3
8889	Remote access
8892	TS1
8893	TS2
8894	TS3
8895	TS4
8896	TS5
8906	RSS ping

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 0.9 2018-11-11
First issue

Revision 1.0 2019-07-30
Chapter Technical parameters updated.

Revision 1.1 2019-09-10
Minor improvements

Revision 1.2 2019-10-04
Added chapter 6 (*Web interface*) and 7 (*Settings*).

Revision 1.3 2019-11-14
Chapter 7 (*Settings*) improved.

Revision 1.4 2019-11-20
Bridge mode and Transparent radio protocol added.

Revision 1.5 2020-01-24
Minor modification of chapters 5-7, TBC grant added

Revision 1.6 2020-02-28
Screenshots updated according to version 1.3.6.0
Chapter Technical parameters updated.

Revision 1.7 2020-06-25
Added new features of 1.4.3.0 fw

Revision 1.8 2020-08-28
Added new features of 1.4.5.0 fw

Revision 1.9 2020-10-23
Minor modification of chapter 7

Revision 1.10 2021-02-11
Chapter 3 and 9 rework

Revision 1.11 2021-04-19
FW 2.0.0.0 features

Revision 1.12 2021-05-19
FW 2.0.3.0 features added

Revision 1.13 2021-07-27
Minor updates of chapters 5 and 7

Revision 1.14 2021-08-30
COMLI protocol added, chapter 8 update

Revision 1.15 2021-10-07
Update of chapters 5,7 and 8

Revision 1.16 2021-11-02
Update of chapters 7 and 8

Revision 1.17 2021-11-26
Babel protocol added

Revision 1.18 2021-12-23
Minor update of chapter 2 and 7

Revision 1.19 2022-03-07
Screenshots update. Chapter 7 structure slightly changed
Explosive atmosphere information added
Section Diagnostics > Information added

Revision 1.20 2022-05-05
Chapter 7.1.1 Ethernet improved.
Minor modifications of chapter Security

Revision 1.21 2022-06-03
Chapter Celullar added.
Chapter SMS added.

Revision 1.22 2022-08-06
RipEX2e HW product variant incorporated

Revision 1.23 2022-08-26
Section Diagnostic package added
Section Tamper reset added
Section IPsec improved

Revision 1.24 2022-12-19
Section Sleep mode added

Revision 1.25 2023-02-24
Section Firmware distribution added

Revision 1.26 2023-05-11
Minor modifications of chapter 7

Revision 1.27 2023-07-28
Section *Credentials* added
Section *Link management* added

Revision 1.28 2023-10-23
Section OpenVPN added
Appendix Security Hardening Procedure added

Revision 1.29 2023-12-15
New features for FW 2.1.2.0 version added

Revision 1.30 2024-03-05
New features for FW 2.1.6.0 version added

Revision 1.31 2024-06-05
New features for FW 2.1.7.0 version added

Revision 1.32 2024-08-29
New features for FW 2.2.0.0 version added

Revision 1.33 2024-10-07
Extension of the PPP protocol to include Tetra

Revision 1.34 2024-11-28
New features for FW 2.2.1.0 version added

Revision 1.35 2025-02-25
Section *Wi-Fi* added
Section *Logs* added
Gratuitous ARP Reply function added

Revision 1.36 2025-05-29
IPsec transport mode added
L3 firewall improvements added
End of Russian language support

Revision 1.37 2025-10-07
System fonts now used to speed up loading of GUI
Radio ACM added

Revision 1.38 2026-03-05
New LTE modules ME310G1 - Order code ‘R' and 'S’ added
Enhanced menu navigation - screenshots updated
Unit configuration backup - encrypted option documented
Boot time updated (30 → 40 s)
RipEX2 and Midge3 essential version details updated

Revision 1.39 2026-05-12
Section *OpenVPN* updated
Firmware Module Visibility
Advanced Menu Enhancements
Correction and addition of documentation for the second COM on the main board and the COM port extension module
Ordering codes correction