RACOM
RADIO DATA NETWORKS

User manual

RipEX2
Radio modem & Router

Quick start

Hardware

Configuration

Parameters

fw 1.3.2.0
01/13/2020
version 1.4

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

Copyright

Disclaimer

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

Trademark

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

Important Notice

- Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the 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.

Quick start

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.

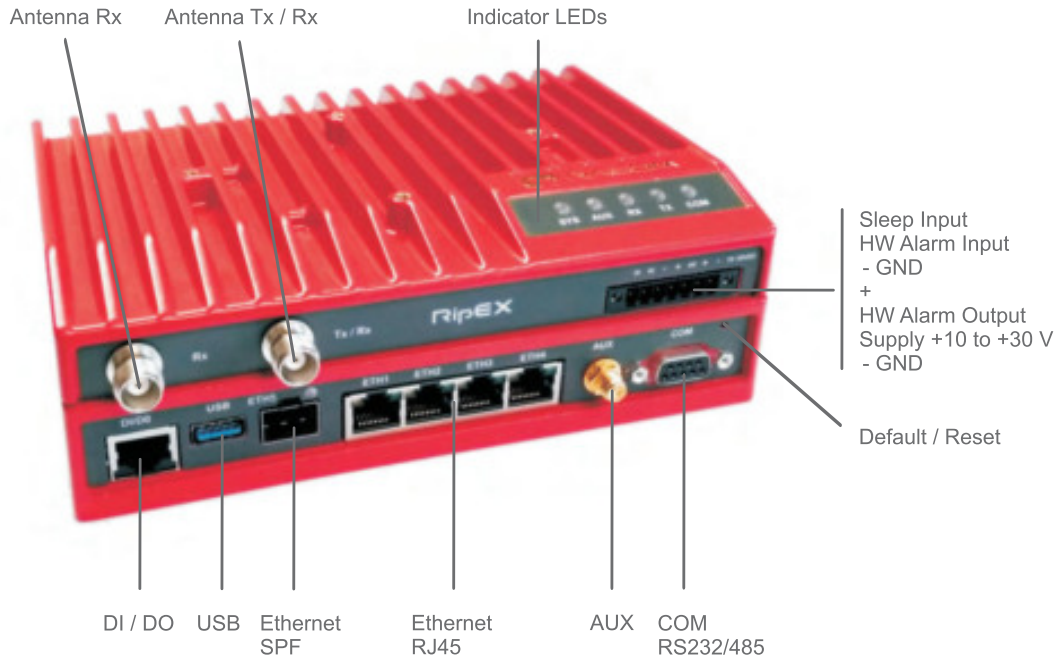


Fig. 1: RipEX2 radio router

Default password for "admin" account is "admin". Change the password before signing to a network.

Ethernet

RipEX2 default IP is 192.168.169.169/24, so set a static IP 192.168.169.x/24 on your PC, power on the RipEX2 and wait approximately 30 seconds for the RipEX2 OS to boot. Connect your PC to RipEX2 ETH interface, start your browser and type https://192.168.169.169 in the address line.

USB/ETH adapter

When accessing over the optional “XA” USB/ETH adapter, your PC will get its IP settings from the built-in DHCP server and you have to type https://10.9.8.7 in your browser. You do not need to worry about other RipEX2 units, you will be connected to the local unit in all cases.

Wifi adapter

When accessing over the optional “W2” Wifi adapter, connect your PC (tablet, smart phone) to the RipEX2 Wifi AP first. Its default SSID is “RipEX2 + Unit name + S/N”. By default the WPA2 PSK secured connection with password "123456789" is used.

Your PC will get its IP settings from the built-in DHCP server and you have to type http://10.9.8.7 in your browser. Remaining steps are the same and you do not need to worry about other RipEX2 units, since you will be connected to the local unit in all cases.

SCADA radio network step-by-step

Building a reliable radio network for a SCADA system may not be that simple, even when you use such a versatile and easy-to-operate device as the RipEX2 radio modem. The following step-by-step checklist can help you to keep this process fast and efficient.

1. Design your network to ensure RF signal levels meet system requirements.
2. Calculate and estimate the network throughput and response times when loaded by your application.
3. Perform a bench-test with 3-5 sets of RipEX2 units and SCADA equipment (*Chapter 3, Step-by-step guide*).
4. Design the addressing and routing scheme of the network (*RipEX App notes*[1] and *RipEX App notes-Address planning*[2])
5. Preconfigure all RipEX2 units.
6. Install individual sites
    1. Mount RipEX2 into cabinet (*Section 4.1, “Mounting”*).
    2. Install antenna (*Section 4.2, “Antenna installation”*).
    3. Install feed line (*Section 4.3, “Antenna feed line”*).
    4. Ensure proper grounding (*Section 4.4, “Grounding”*).
    5. Run cables and plug-in all connectors except from the SCADA equipment (*Section 1.2, “Connectors”*)
    6. Apply power supply to RipEX2.
    7. Test radio link quality (e.g. using Monitoring tool).
    8. Connect the SCADA equipment.
7. Test your application.

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

List of documentation

User manuals:

- **RipEX2 - User manual**

  User manual RipEX2 - this document

- ***RipEX2 Hot Standby***[1] **- User manual**

  User manual

Datasheets:

- ***RipEX2 - Datasheet***[2]

Application notes:

- ***RipEX - Application notes***[3]
  - Bridge mode
  - Flexible protocol
  - Base driven protocol
  - Network planing
  - Migration solution
  - and many others

Contents of the box

Standard RipEX2 package in paper box contents:

- RipEX2 – 1 pc
- Removable sticker plate – 1 pc
- Power and Control plug connector (counterpart) – 1 pc
- DIN set (a pair of DIN rail clips + screws) – 1 pc
- SFP port dust cap

[1] https://www.racom.eu/eng/products/m/ripex-hs/index.html
[2] https://www.racom.eu/download/hw/ripex/free/eng/ripex-dsA4-en.pdf
[3] https://www.racom.eu/eng/products/m/ripex/app/index.html

1. 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 4.1, “Mounting”*.

1.1. Dimensions

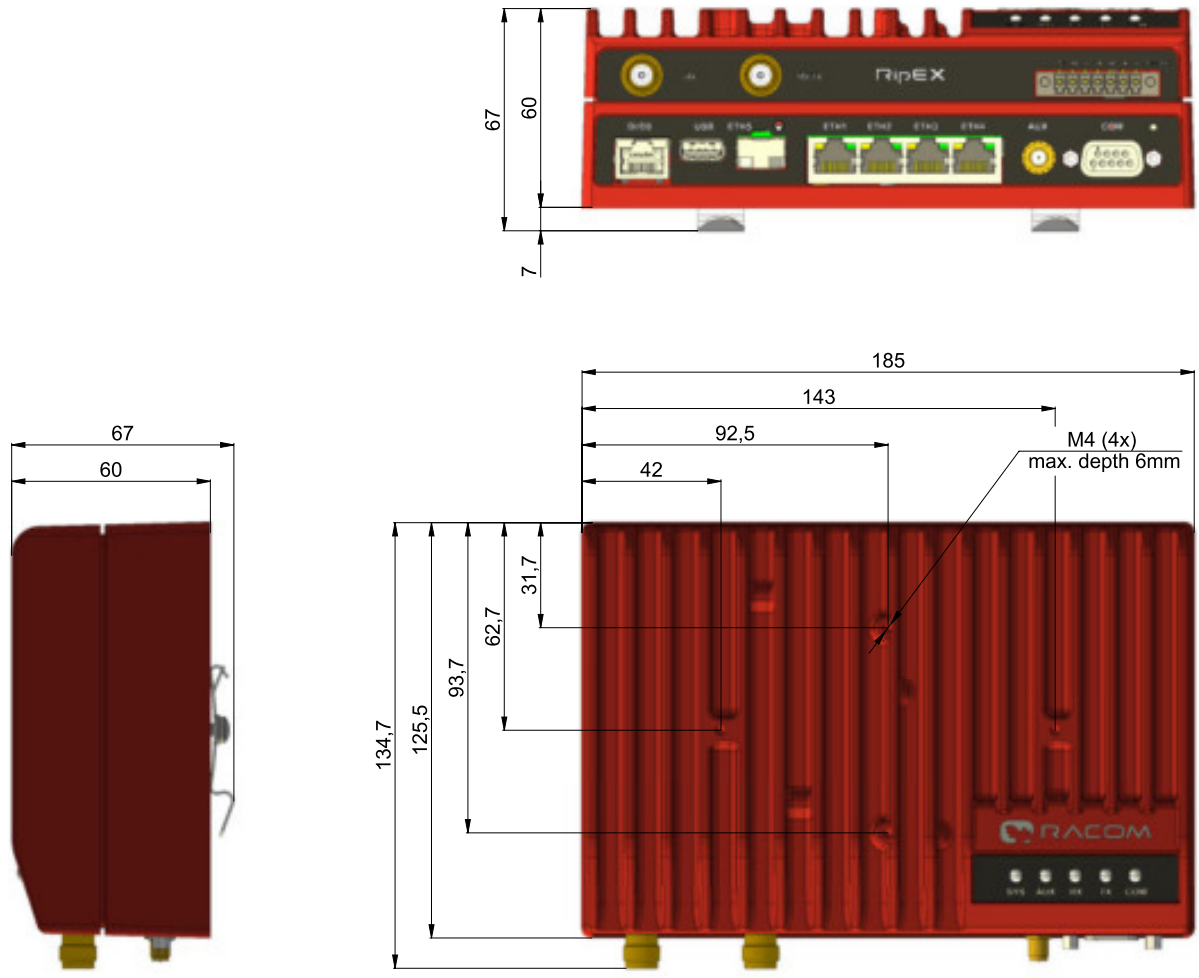


Fig. 1.1: RipEX2 dimensions

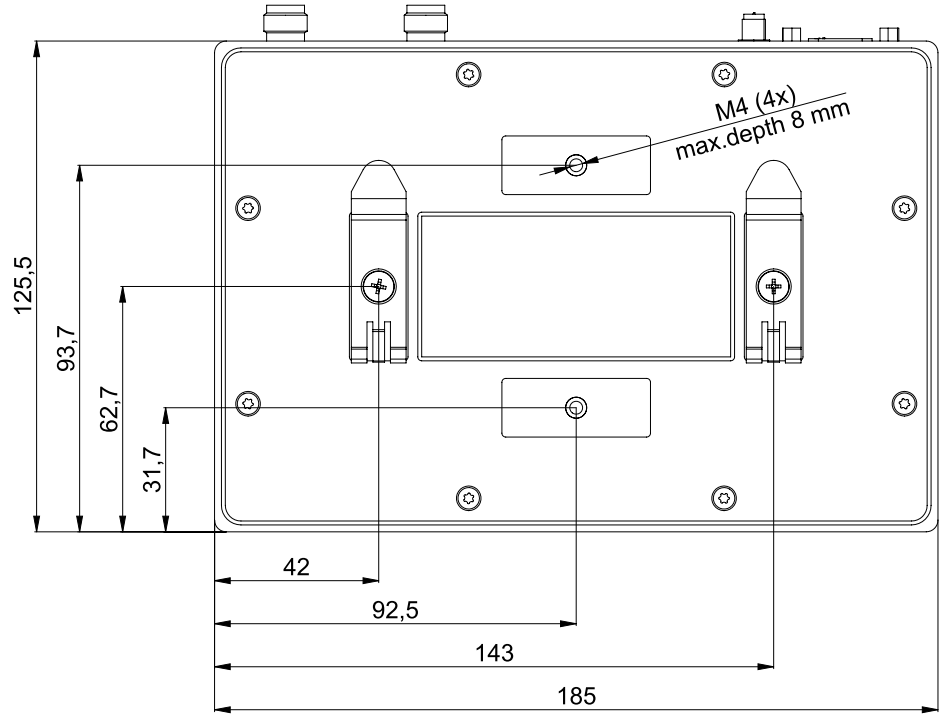


Fig. 1.2: RipEX2 dimensions – bottom

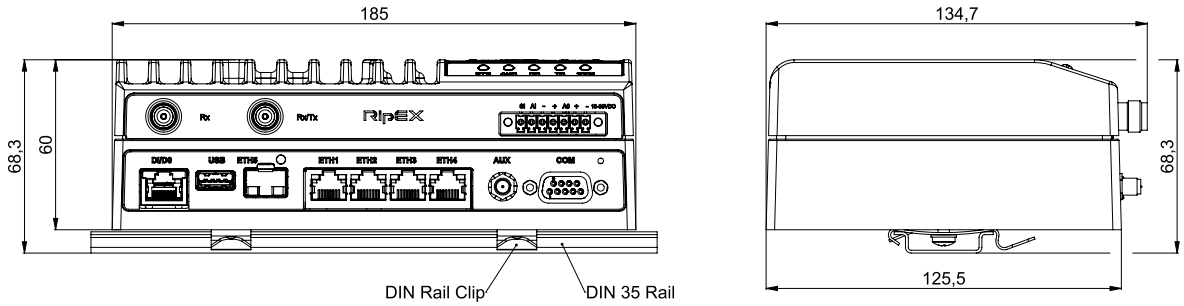


Fig. 1.3: RipEX2 with DIN rail

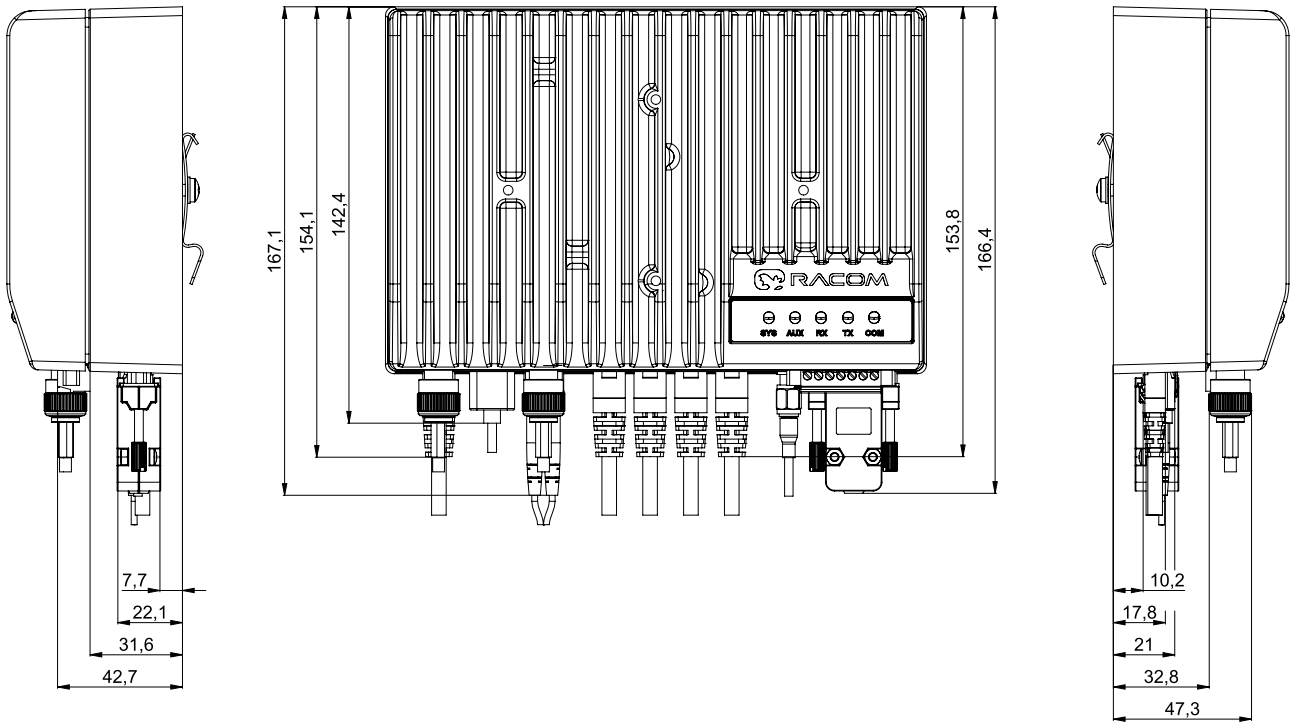


Fig. 1.4: RipEX2 dimensions with connectors

For more information see *Section 4.1.1, “DIN rail mounting”* and *Section 4.1.2, “Flat mounting”*.

1.2. Connectors

All connectors are located on the front panel. The upper side features an LED panel. The RESET button is located in an opening in the bottom side.

Fig. 1.5: Connectors

1.2.1. 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).

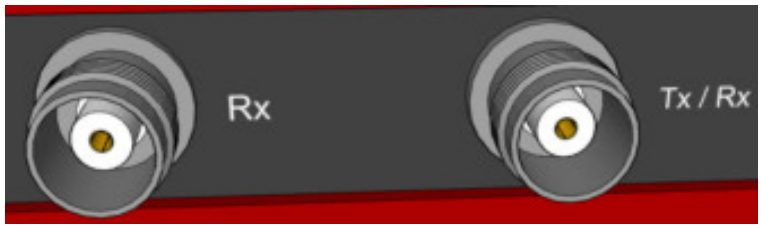


Fig. 1.6: Antenna connectors

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

Warning

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

1.2.2. 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. 1.1: 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.

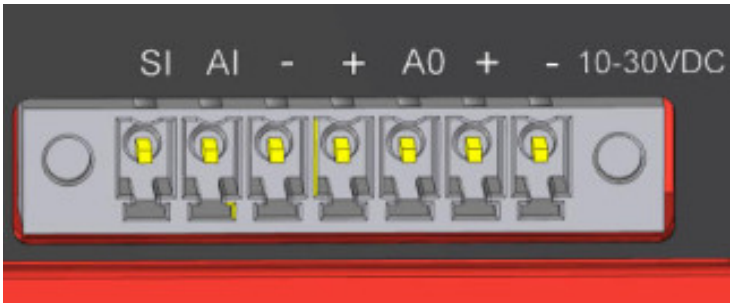


Fig. 1.7: Supply connector

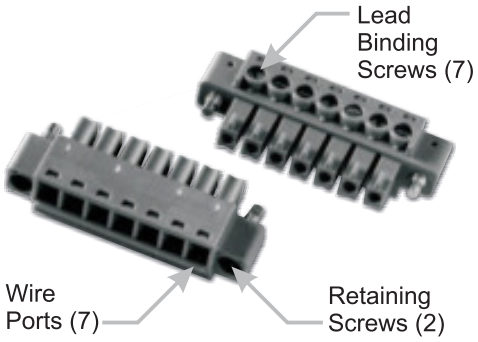
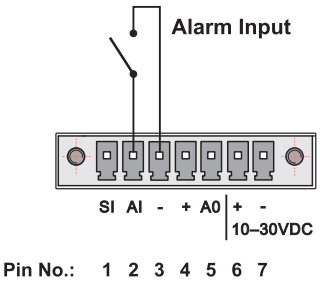


Fig. 1.8: Power and Control - cable plug

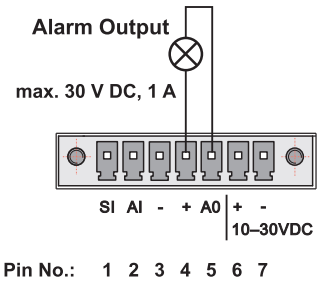
HW ALARM INPUT

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



HW ALARM OUTPUT

HW ALARM OUTPUT is a digital output.



POWER

The POWER pins labelled + and - serve to connect a power supply 10–30 VDC. The requirements for a power supply are defined in *Section 4.6, "Power supply"* and *Chapter 9, Technical parameters*.

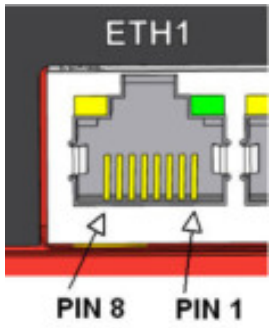
1.2.3. ETH1 - ETH4

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. 1.2: 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



1.2.4. 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.

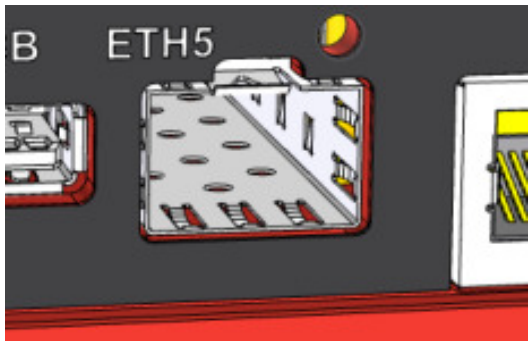


Fig. 1.9: SFP slot

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.

1.2.5. COM

RipEX2 provides serial interface COM terminated by DSUB9F connectors. It can be configured as RS232 or 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. 1.3: COM pin description

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	—	—	—	

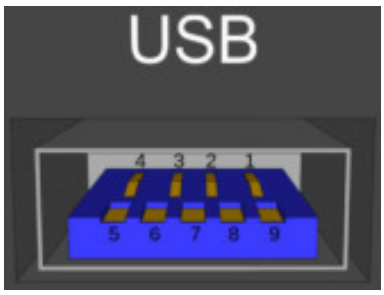
RipEX2 keeps pin 6 DSR at the level of 1 by RS232 standard permanently.

1.2.6. USB

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

Tab. 1.4: USB A Pinout Cable Assembly

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



The USB interface is designed for the connection to an external ETH/USB adapter or a Wifi adapter. They are optional accessories to RipEX2, for more details see *Section 3.3, "Connecting RipEX2 to a programming PC"*. The adapters are used for service access to web configuration interface of RipEX2 unit.

The USB interface can also be used for an external flash disc connection, which has been specifically designed to simplify complex maintenance tasks, so that these tasks can be performed by unqualified personnel in the field by simple plugging-in an USB stick and waiting until a LED flashes.

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.

External USB flash disc

An external USB flash disc can be used for firmware upgrade, SW keys upload, configuration backup and restore, ssl certificate and ssh keys upload and tech-support package download. Any common USB stick with several megabytes of free space can be used for these tasks.

1.2.7. AUX

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

Standard basic model – the AUX 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. 1.10: AUX connector SMA

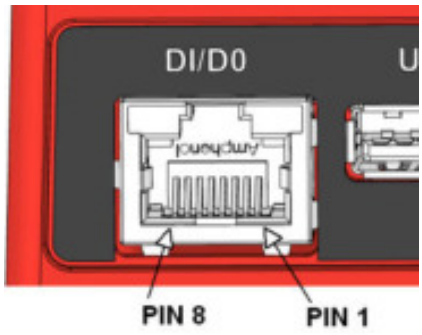
RipEX2 can be equipped with an internal GPS. The GPS module is used for time synchronization of the NTP server inside RipEX2. In this case the AUX connector serves for connecting the GPS antenna:

- active antenna
- 3.3 VDC supply

1.2.8. DI/DO

Tab. 1.5: Digital Inputs and Outputs

Pin	Signal
1	Differential digital input - Positive - (P)
2	Differential digital input - Negative - (N)
3	GND
4	Digital Output 1
5	Digital Output 2
6	GND
7	Digital Input 1
8	Digital Input 2



- 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

1.2.9. HW button

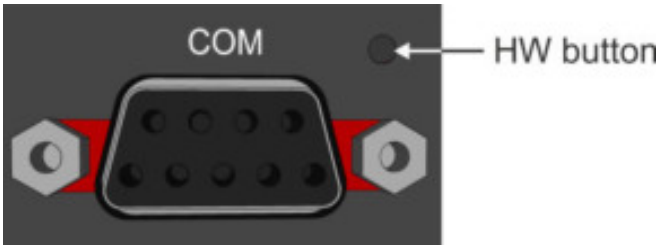


Fig. 1.11: HW button

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

1.3. Indication LEDs

Fig. 1.12: Indication LEDs

Tab. 1.6: Key to LEDs

LED	Colour	Style	Function
SYS	Green	Permanently lit	System OK
		Flashing - period 500 ms	Reset button pushed
		One fast (50 ms) flash - pause (500 ms)	Reset button to reset
		Three fast (50 ms) flashes - pause (500 ms)	Reset button factory reset
		Flashing - period 1 sec	Save mode
		Flashing - period 3 sec	Sleep mode
	Red	Permanently lit	Alarm
		Flashing regularly - period 500 ms	Serious system error
	Orange	Permanently lit	Unit is starting
		Three fast (50 ms) flashes - pause (500 ms)	USB attached
		Flashing - period 100 ms	Skip go to sleep mode, boot normally
		Flashing regularly - period 500 ms	Firmware writing in progress - DO NOT POWER OFF !
AUX	Green	Permanently lit	Activity
	Red	Permanently lit	Alarm
Rx	Green	Permanently lit	Receiver is synchronized to a packet

LED	Colour	Style	Function
	Yellow	Permanently lit, or flashing in 1 sec intervals	Rx mode of operation - high resistance (strong interfering signals - above -45 dBm - are present within the frequency band), adaptive mode of receiver operation
Tx	Red	Permanently lit	Transmitting to radio channel
	Green	no function	no function
COM	Green	Permanently lit	Data receiving
	Yellow	Permanently lit	Data transmitting

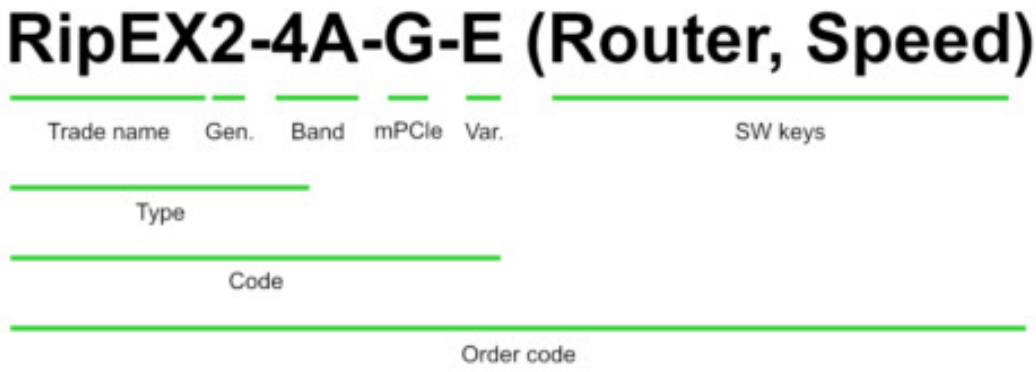
Alarm – is “On” when any controlled item in Alarm management, (see Adv. Conf., Alarm management for more) is in alarm status (out of thresholds) and “SNMP Notification", "HW Alarm Output" or "Detail graphs start” for any line in the Alarm configuration table are checked.

Adaptive mode of receiver operation Cognitive function of receiving mode selection is implemented in RipEX2. 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 (and lowers its sensitivity by 3 dB). When interference holds, RipEX2 stays in high resistance 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.

1.4. Ordering codes

RipEX2 radio modem has been designed to have minimum possible number of hardware variants. Different HW models are determined by frequency, internal GPS and separate connectors for RX and TX antennas.

All ordering codes are available on RACOM website. See *Ordering information*[1].



- **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 doesn't have any number in this position.
  Possible values:
  none
  2
- **Band** - frequency band and sub-bandlinebreak
  Possible values:
  1A: 135-175 MHz
  3A: 275-330 MHz (coming soon)
  3B: 335-400 MHz
  4A: 400-470 MHz
- **mPCIe** - Expansion module (mPCIe module is inserted during production)
  Possible values:
  N – not used
  E, P, A - LTE bands (see *Table 9.1, "Technical parameters"* for detailes):
  G – GPS (GNSS) module, Part.No.: mPCIe-GPS
  C – Expansion 2× RS232, Part.No.: mPCIe-COMS

  Note

  Only one option for mPCIe slot is possible.

- **Var.** – designation of product variant, if it is used. Generally, more variants can be used within one unit, i.e. more letters can be on this position. These variants can't be ordered and included in the unit later on.

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

Possible values:
X*– Processor with HW encryption option
N – Processor without HW encryption option. Encryption features will never be possible, neither HW nor SW encryption
E – Processor without HW encryption option. SW encryption possible

* The processor included in the unit uses an encryption module listed as 5A002 a.1 in the COUNCIL REGULATION (EC) No 428/2009, 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 *Dual-use trade controls*[2].

- **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:
  Router – enables Router mode. If not activated, only Bridge mode is available, Part No. RipEX2-SW-ROUTER
  Speed – enables 256QAM modulation, Part No. RipEX2-SW-SPEED
  SFP – enables SFP interface, Part No. RipEX2-SW-SFP
  10W – enables RF output power up to 10 W for CPSK modulations, Part No. RipEX2-SW-10W
  Backup routes – enables Backup routes, Part No. RipEX2-SW-BACKUP ROUTES
  Duplex – enables Duplex mode, Part No. RipEX2-SW-DUPLEX
  Master – enables all functionalities of all possible SW feature keys, Part No. RipEX-SW-MASTER

- **Type** – specific product type for which type approvals like CE, FCC etc. are issued.
  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 *RACOM WebService*[3].

[2] http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm
[3] https://webservice-new.racom.eu/main/eshop.list?t=10

2. Accessories

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

1. **RipEX2 Hot Standby**

   RipEX2-HS is redundant Hot Standby chassis. There are two Hot Standby standard RipEX2 units inside. In case of a detection of failure, automatic switchover between RipEX2 units is performed. RipEX2-HS is suitable for Central sites, Repeaters or Important remote sites where no single point of failure is required.

Fig. 2.1: RipEX2-HS

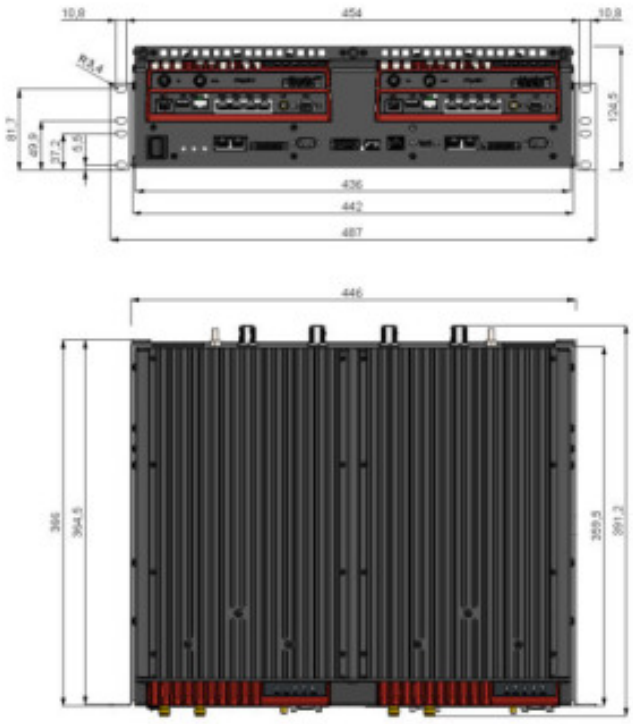


Fig. 2.2: RipEX2-HS dimensions

For more information see RipEX2-HS datasheet or User manual on *RACOM website*[2].

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories
[2] https://www.racom.eu/download/hw/ripex-hs/free/eng/RipEX-HS-A4-en.pdf

2. **RipEX2-RD**

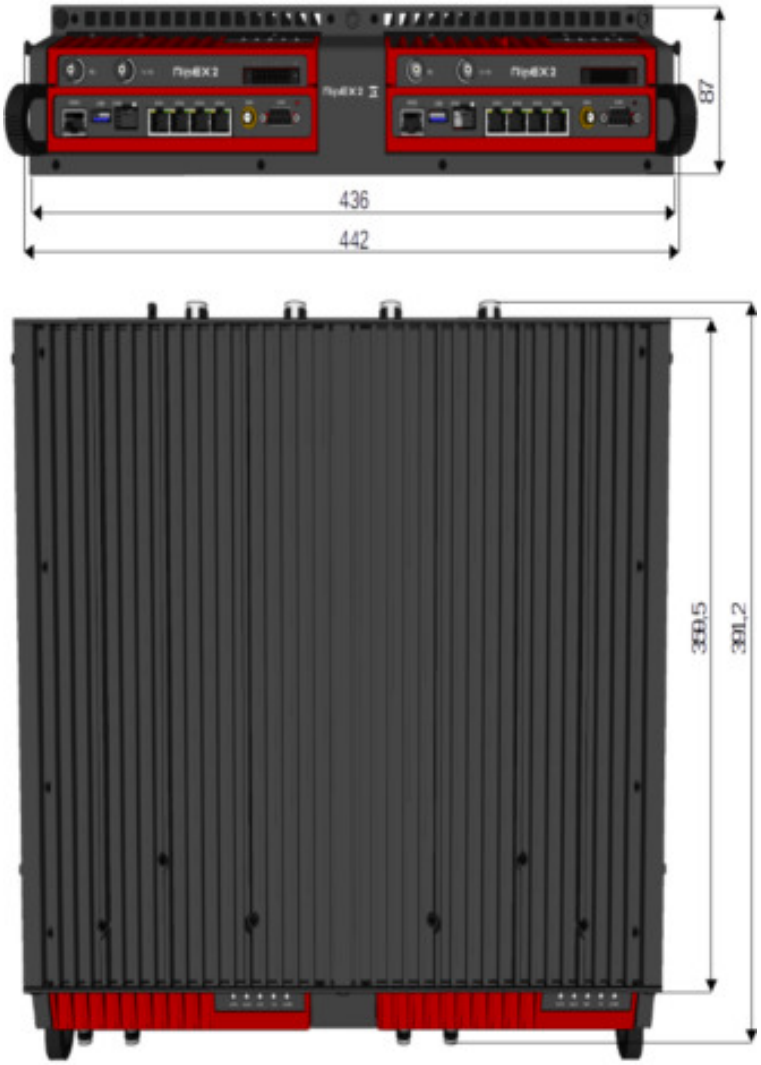


Fig. 2.3: RipEX2-RD

3. **RipEX2-RS**

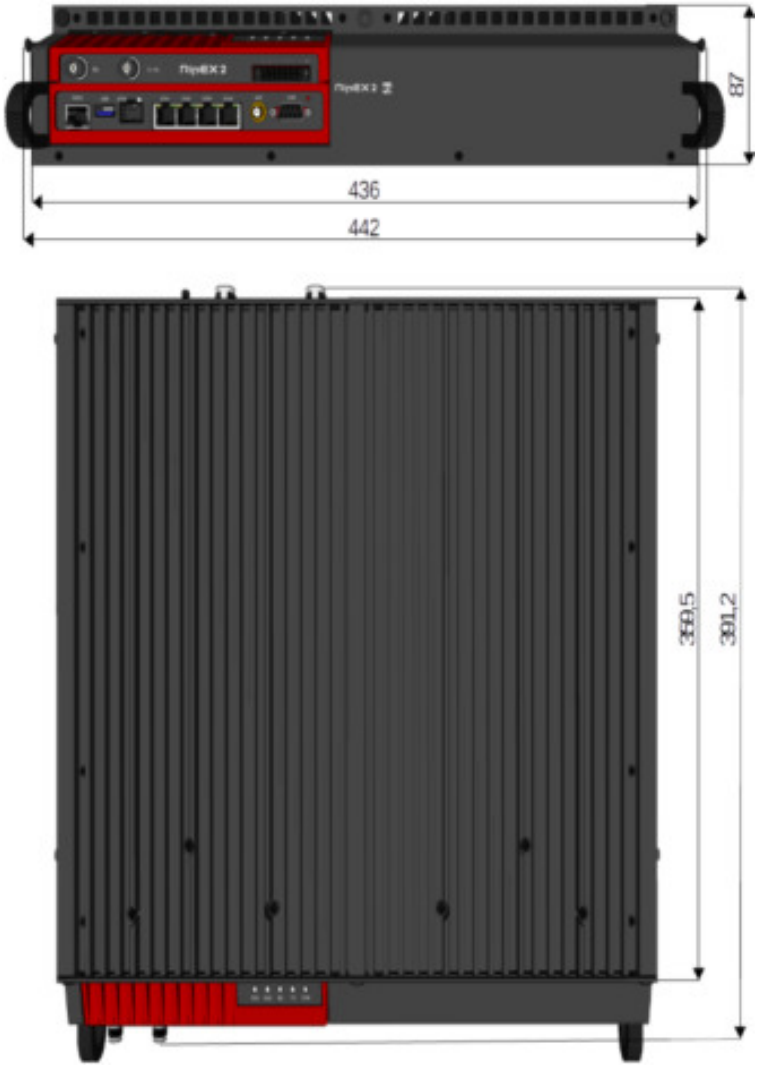


Fig. 2.4: RipEX2-RS

4. **ETH/USB adapter**

ETH/USB adapter for service access to the web interface via USB connector. Includes a built-in DHCP server which provides up to 5 leases. To access the RipEX always use the fixed IP 10.9.8.7. For details on use see *Section 3.3, "Connecting RipEX2 to a programming PC"*.

Fig. 2.5: ETH/USB adapter

5. **Wifi adapter**

Wifi adapter for service access to the web interface via USB connector. Includes a built-in DHCP server which provides up to 5 leases. To access the RipEX always use the fixed IP 10.9.8.7. For details on use see *Section 3.3, "Connecting RipEX2 to a programming PC"*.

Fig. 2.6: WiFi adapter

Note

Wifi adapter PartNo: 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.

6. **Demo case**

A rugged plastic case for carrying up to three RipEX2 units and one M!DGE2 4G SCADA router. It can be used to perform an on-site signal measurement, complete application bench-test or a functional demonstration of both radio modems and the 4G router.

Fig. 2.7: Demo case

Content:
- Brackets and cabling for installation of three RipEX2 units and one M!DGE2 (units are not part of the delivery)
- 1× power supply Mean Well GST160A24-R7B (100-240 V AC 50-60 Hz/24 V DC)
- 1× Power cable (European Schuko CEE 7/7 to IEC 320 C13)
- 1× Ethernet patch cable (3 m, UTP CAT 5E, 2× RJ-45)
- Quick start guide

RipEX2 accessories:
- 6× Dummy load antennas
- 1× L-bracket, 1× Flat-bracket samples
- 1× ETH/USB adapter
- 1× Wifi adapter

M!DGE2 accessories:
- Antenna ANT-LTE-W1 (0 dBi)

Mechanical properties of case
- Outside dimension: 455 × 365 × 185 mm
- Weight approx. 5.5 kg (excluding the RipEX2 and M!DGE2 units) / 10.6 kg (including 3× RipEX2 units and 1× M!DGE2 unit)

7. **L-bracket**

Installation L bracket for vertical mounting. For details on use see *Section 4.1, “Mounting”* and *Section 1.1, “Dimensions”*.

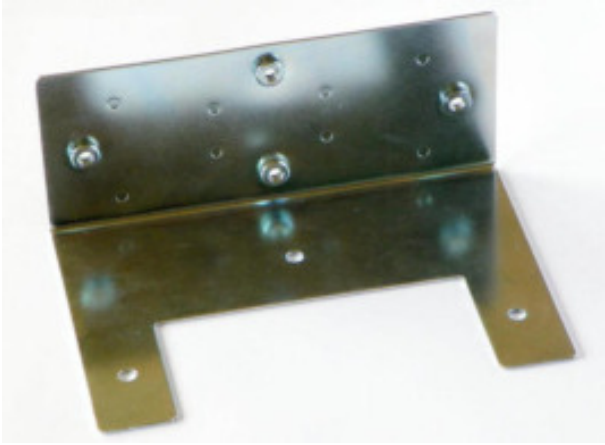


Fig. 2.8: L-bracket

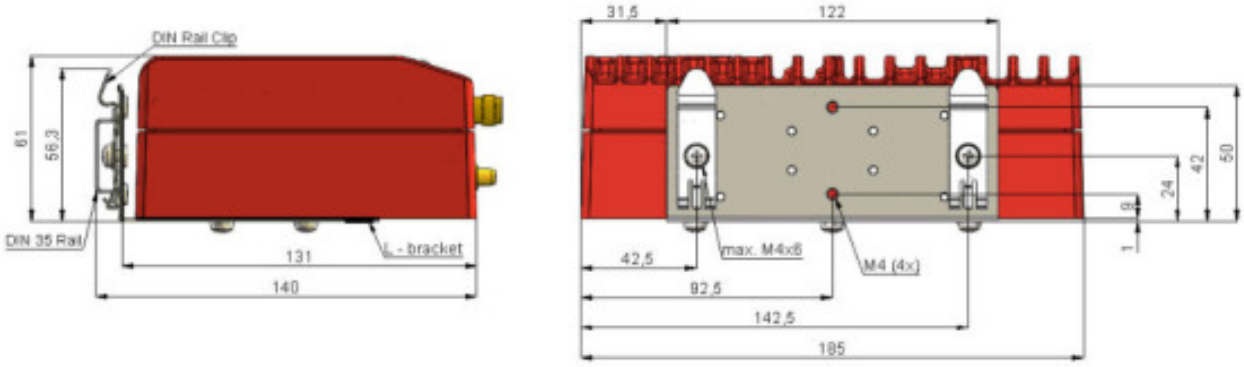


Fig. 2.9: RipEX2 with L-bracket

8. **Flat-bracket**

Installation bracket for flat mounting. For details on use see *Section 4.1, “Mounting”*.

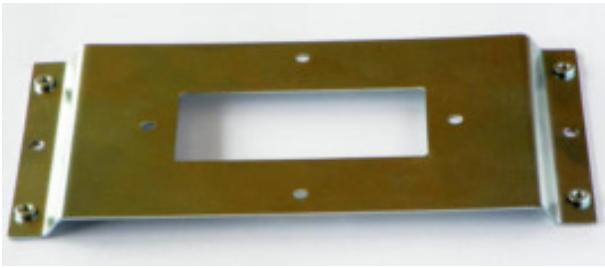


Fig. 2.10: Flat bracket

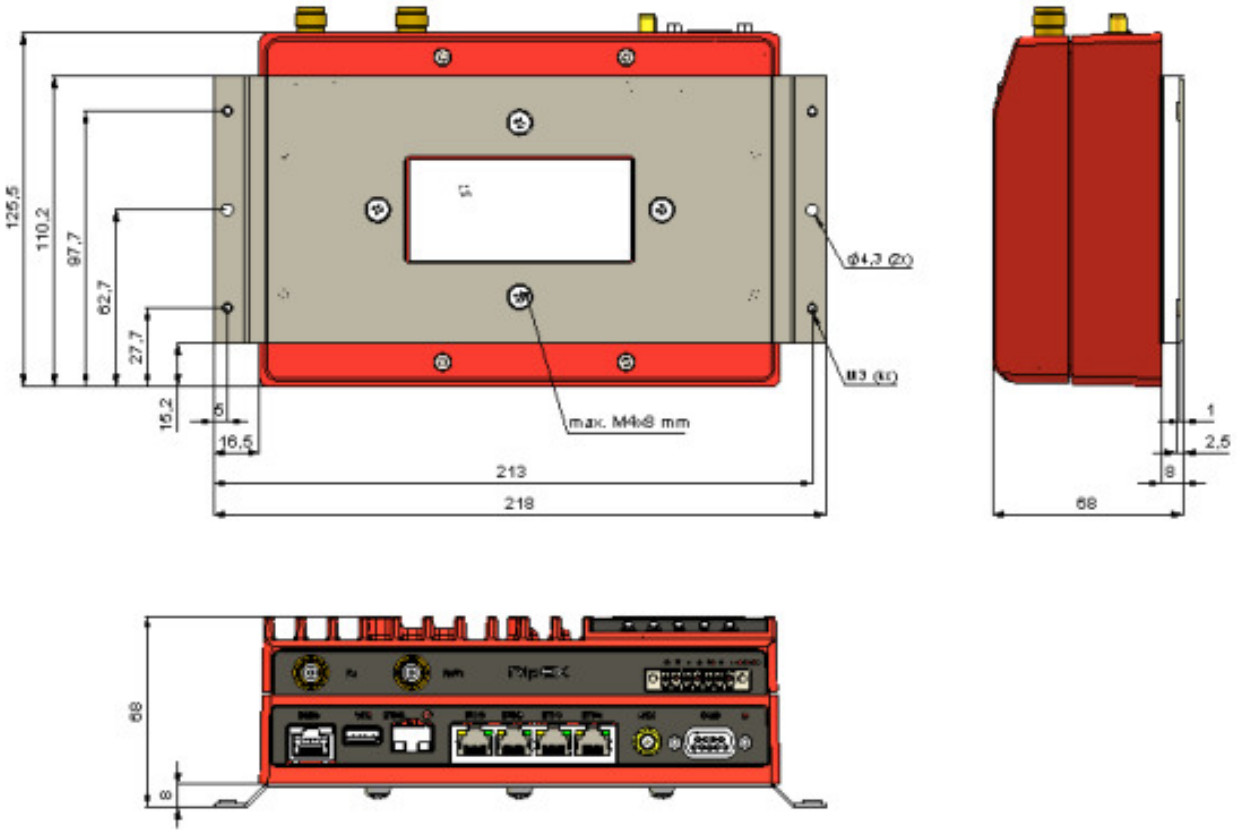


Fig. 2.11: RipEX2 with Flat-bracket

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.

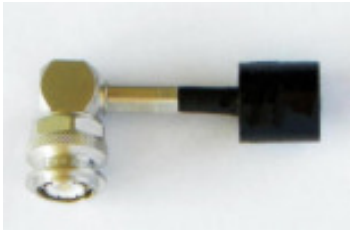


Fig. 2.12: Dummy load antenna

10. **Coaxial overvoltage protection**

Frequency range 100-512 MHz,
connectors N(female) / N(female).

Fig. 2.13: Overvoltage protection

11. **Feedline adapter cable**

Feedline cable is 50 cm long and is made from the RG58 coaxial cable. There are TNC Male (RipEX2 side) and N Male connectors on the ends. It is intended for use between RipEX2 and cabinet panel.

Fig. 2.14: Feedline adapter cable

12. **Others**

For other accessories (Power supplies, Antennas, Coaxial overvoltage protection etc.) kindly visit *RACOM website*[3].

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

3. Step-by-step guide

3.1. Connecting the hardware

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
- The 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.

Bench test connection possibilities:

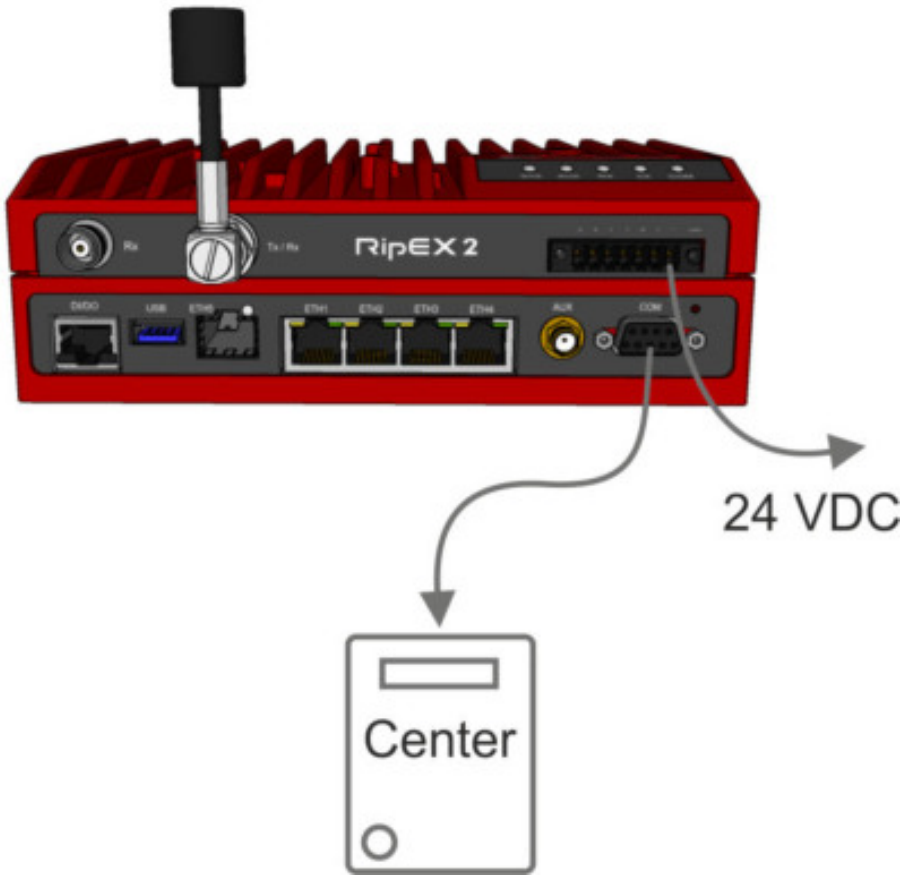


Fig. 3.1: RipEX2 connected to SCADA center

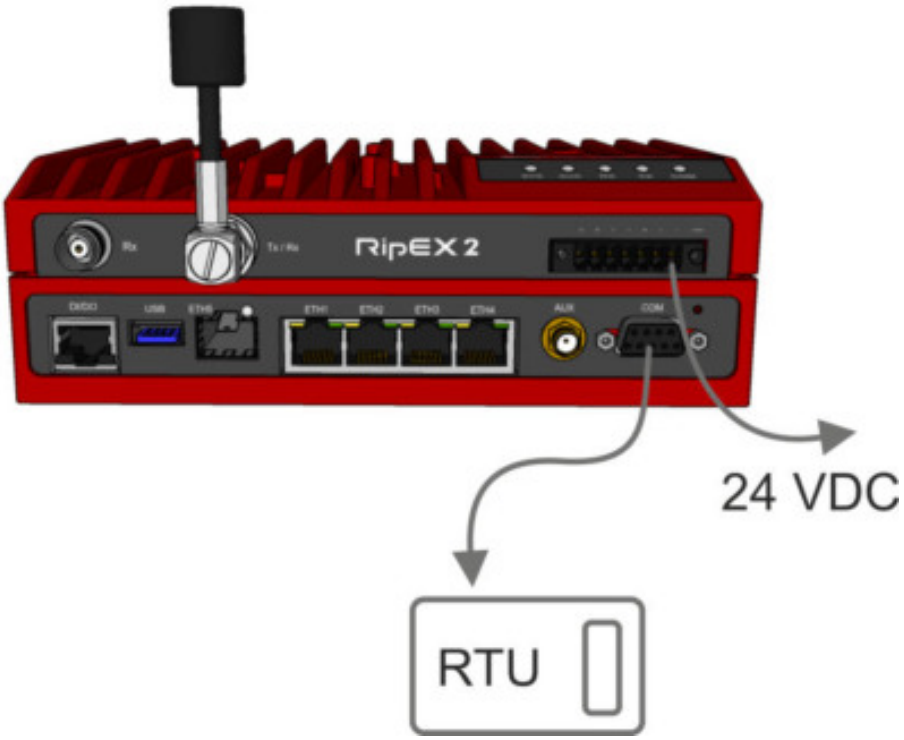


Fig. 3.2: RipEX2 connected to RTU

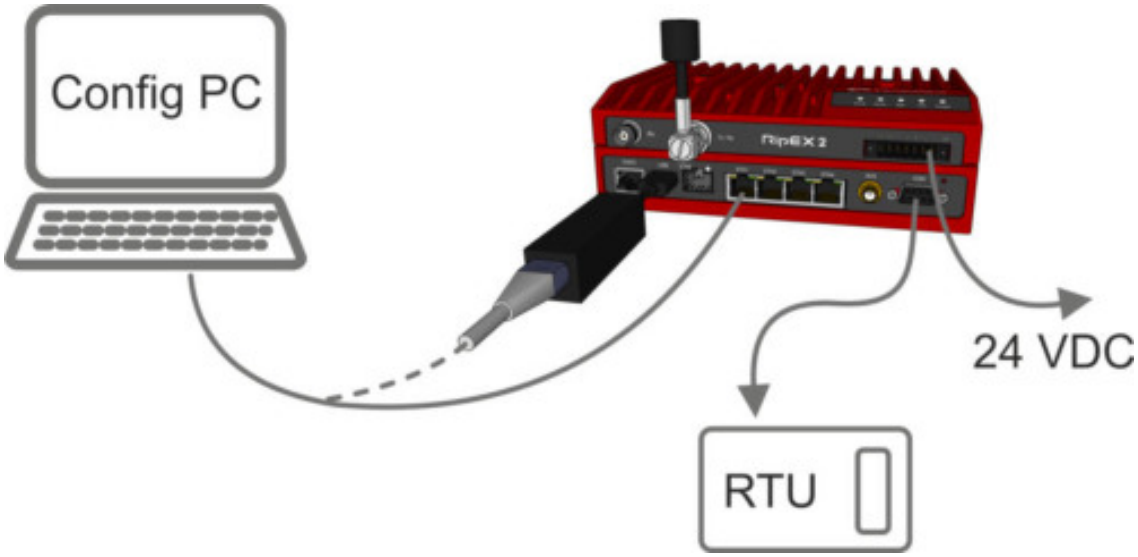


Fig. 3.3: Connecting management PC to RipEX2

3.2. Powering up your RipEX2

Switch on your power supply. LED SYS shines orange and after approximately 30 seconds your RipEX2 will have booted and will be ready, the SYS LED shines green. You'll find the description of the individual LED states in *Section 1.3, "Indication LEDs"*.

3.3. Connecting RipEX2 to a programming PC

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

- Using the external Wifi adapter
- Using the external ETH/USB adapter
- Directly over the Ethernet interface

Fig. 3.4: Connecting to a PC over WiFi

Fig. 3.5: Connecting to a PC over ETH/USB adapter

Fig. 3.6: Connecting to a PC over ETH

- **PC connected via Wifi adapter**

  External Wifi adapter PartNo OTH-USB/WIFI-W2 (an optional accessory of the RipEX2) needs to be used. Any other adapter will not work correctly when connected to RipEX2 unit. Connect your PC, tablet or smartphone to RipEX2 Wifi AP first. Its default SSID is “RipEX2 + Unit name + S/N”. The Wifi adapter contains a built-in DHCP server, so if you have a DHCP client in your PC (as most users do), you do not need to set anything up. The IP address of RipEX2 unit, for access over the ETH/USB adapter, is fixed: 10.9.8.7.
  Continue to *Login to RipEX*.

- **PC connected via ETH/USB adapter**

  We recommend using the "XA" - external ETH/USB adapter (an optional accessory of the RipEX2). 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 IP address of RipEX2 unit, for access over the ETH/USB adapter, is fixed: 10.9.8.7.
  Continue to *Login to RipEX*.

- **PC connected directly to ETH port**

  Set a static IP address in PC, example for Windows 10:

  Start > Settings > Network & Internet >Ethernet > Change adapter options > Ethernet (right click) > Properties > Protocol IP version 4 (TCP/IPv4) > Properties > Use the following IP address:
  IP address 192.168.169.250 - for RipEX in the default state (for all ETH interfaces)
  Subnet mask 255.255.255.0
  Default gateway leave empty.
  OK (Internet Protocol Properties window)
  OK (Local Area Properties window)
  Some Operating systems may require you to reboot your PC.

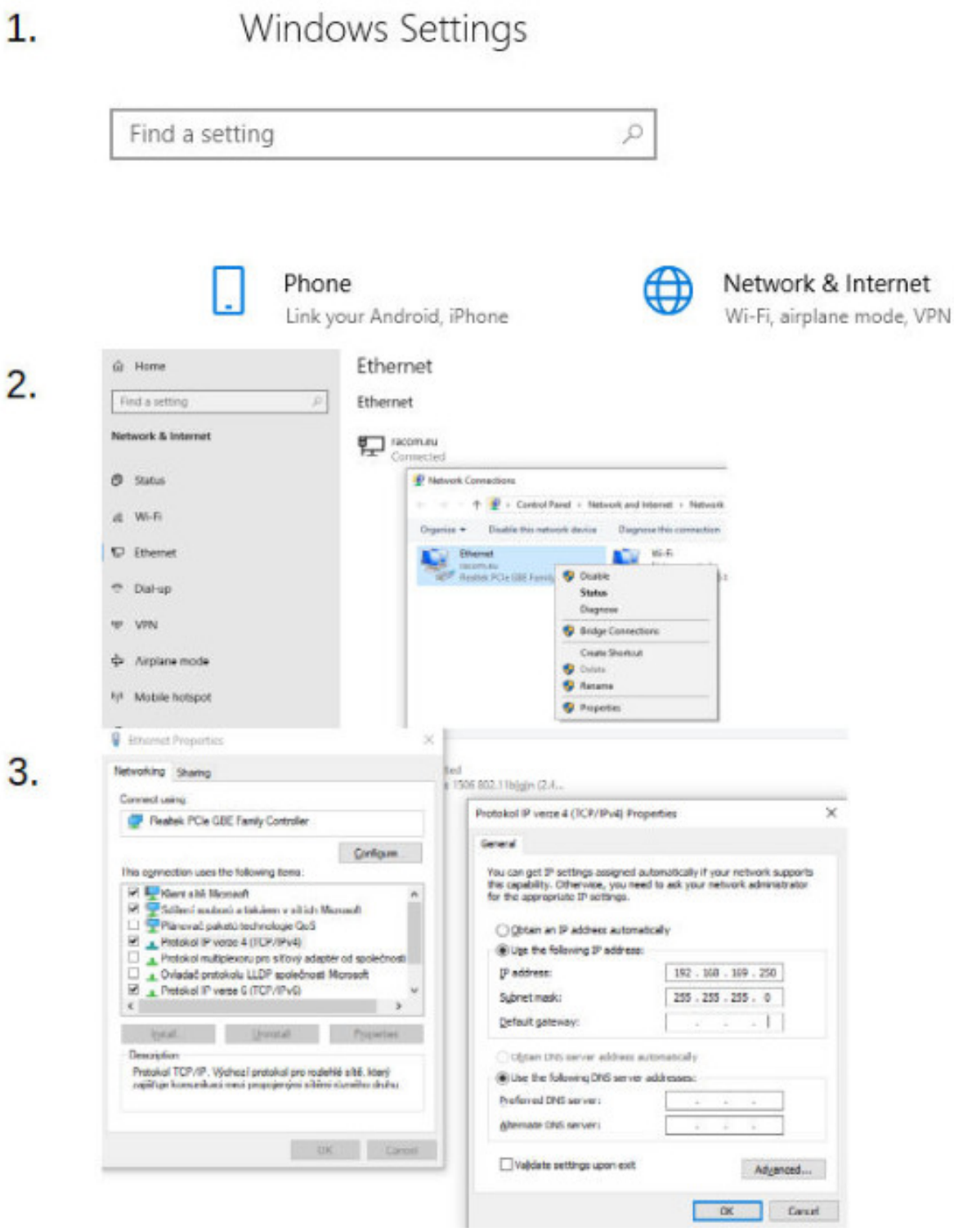


Fig. 3.7: PC address setting

Important

When you change the RipEX2 ETH address to a different IP address/mask, the IP address of your PC might be neccesary to be updated to match the same subnet (mask).

- **Login to RipEX2**

  Start a web browser on your PC and type the RipEX's default IP in the address line field:
  - **10.9.8.7** – when connected via external ETH/USB or Wifi adapter. IP address 10.9.8.7 is fixed and cannot be changed.
  - **192.168.169.169** – when connected directly to ETH. This is the default IP address which can be changed later on - during the unit configuration process.

Note

https - For security reasons the http protocol with ssl encryption can be used for the communication between the PC and RipEX. The https protocol requires a security certificate. You must install this certificate into your web browser. The first time you connect to the RipEX, 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.

The login screen appears.

The default entries for a new RipEX are:

User name: admin

Password: admin

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.)

- **IP address unknown**

  If you do not have the adapter or you have forgotten the password, you can reset the access parameters to defaults, see *Section 1.2.9, “HW button”*.

4. Installation

Step-by-step checklist

1. Mount RipEX2 into cabinet (*Section 4.1, “Mounting”*).
2. Install antenna (*Section 4.2, “Antenna installation”*).
3. Install feed line (*Section 4.3, “Antenna feed line”*).
4. Ensure proper grounding (*Section 4.4, “Grounding”*).
5. Run cables and plug-in all connectors except from the SCADA equipment (*Section 1.2, “Connectors”*).
6. Apply power supply to RipEX2.
7. Connect configuration PC (*Section 3.3, “Connecting RipEX2 to a programming PC”*).
8. Configure RipEX2.
9. Test radio link quality (e.g. using Monitoring tool).
10. Connect the SCADA equipment.
11. Test your application.

4.1. Mounting

4.1.1. 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

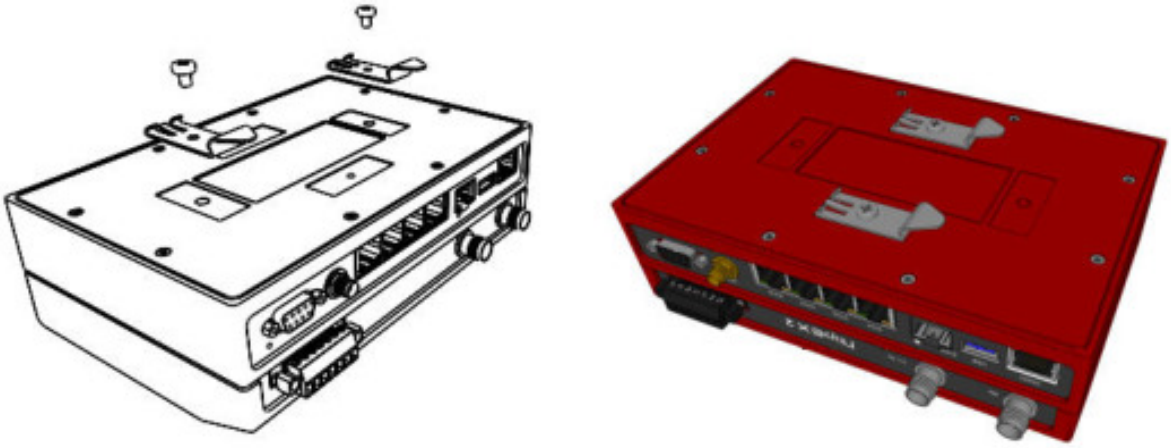


Fig. 4.2: Flat widthwise mounting to DIN rail

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

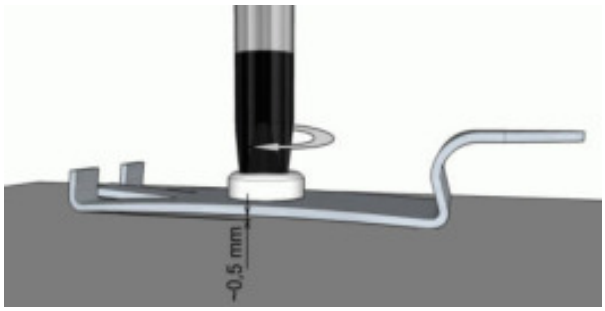


Fig. 4.3: Clip mounting

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

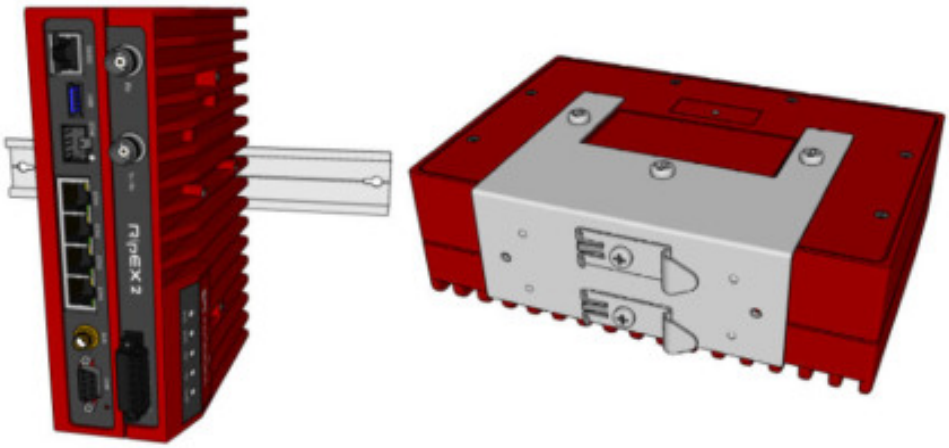


Fig. 4.4: Vertical widthwise mounting to DIN rail

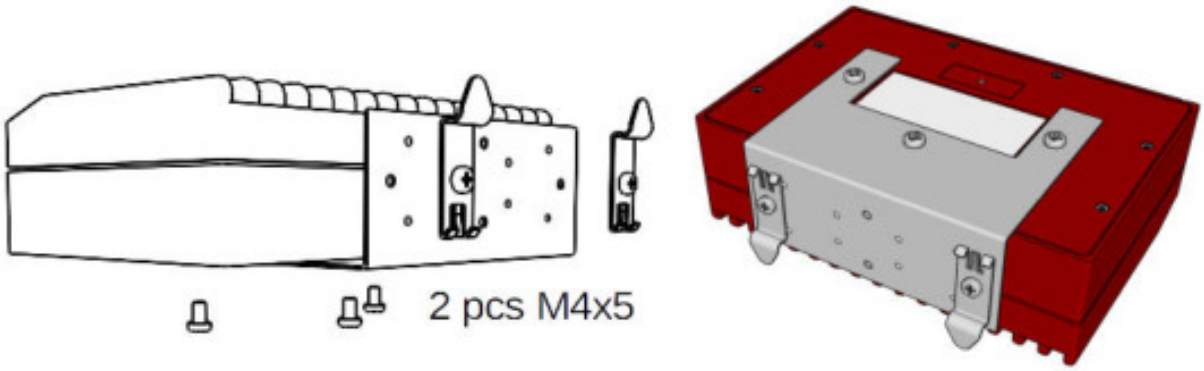


Fig. 4.5: Vertical lengthwise mounting to DIN rail

For more information see *L-bracket*.

4.1.2. Flat mounting

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

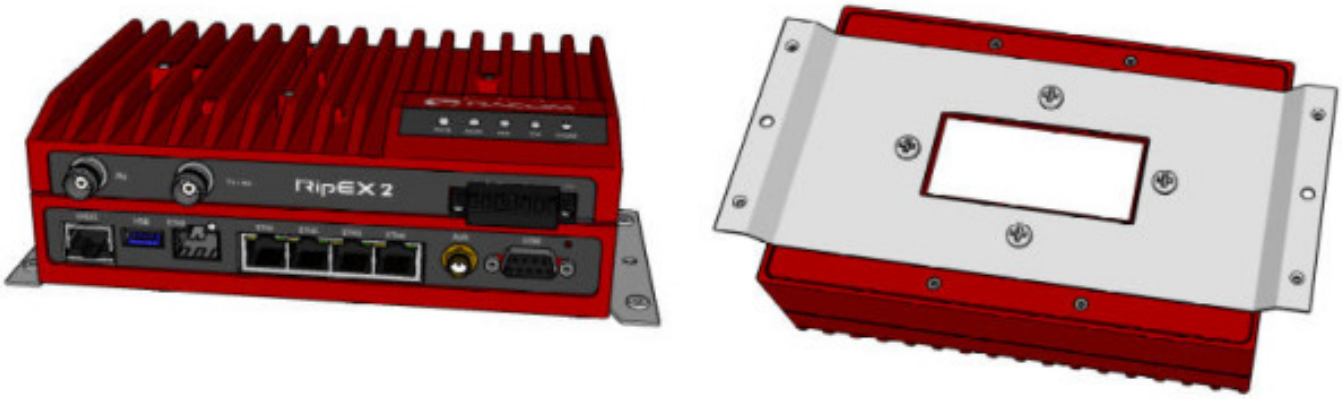


Fig. 4.6: Flat mounting using Flat bracket

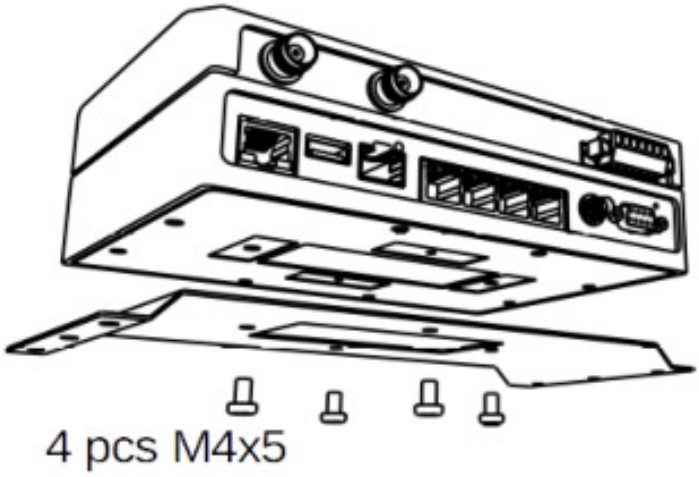


Fig. 4.7: Flat mounting using Flat bracket

For more information see *Flat-bracket*.

4.1.3. IP52 mounting

To meet IP52 protection requirements RipEX2 unit must be physically installed with the connectors facing downward.

Install the SFP port dust cap if the SFP port is not used.

4.2. 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.

4.3. 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"*. This arrangement is recommended especially when the feed line would be very long otherwise (more than 15 meters) or the link is expected to operate with low fading margin.

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.

4.4. 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.

A lightning protector should be used where the antenna cable enters the building. Connect the protector to the building grounding, if possible. All grounds and cabling must comply with the applicable codes and regulations.

4.5. Connectors

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

You will find the pin-outs of connectors in *Section 1.2, "Connectors"*.

4.6. 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. 4.8: 10–30 VDC Supplying

5. RipEX2 in detail

5.1. Bridge mode

5.1.1. Detailed Description

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).

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 network of RipEX2 radio modems behaves as a standard Ethernet network 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 in the LAN (the LAN to which the respective ETH interface is connected).

One has to be very careful when RipEX2 in Bridge mode is connected to LAN, because all LAN traffic is then broadcasted to the Radio channel.

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

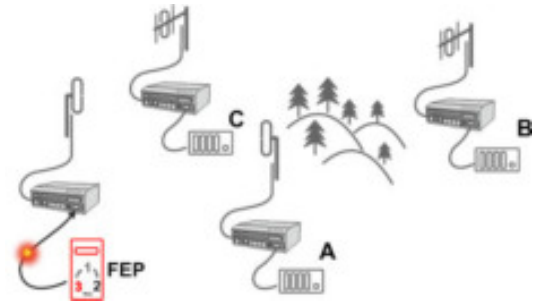
Behavior of Terminal Servers is similar to COM port. "Transparent" protocol needs to be selected when transparent data transfer to whole network (broadcasts) is needed. The other protocol types can be used for "Router mode" type of addressed communication.

5.1.2. Functionality example

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

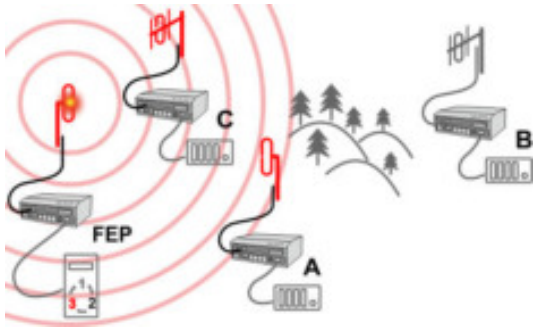
- FEP - Front End Processor, designates the communication interface equipment in the center
- RTU - Remote Telemetry Unit, the terminal SCADA equipment at remote sites

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 5.1.3, “Configuration examples”*.



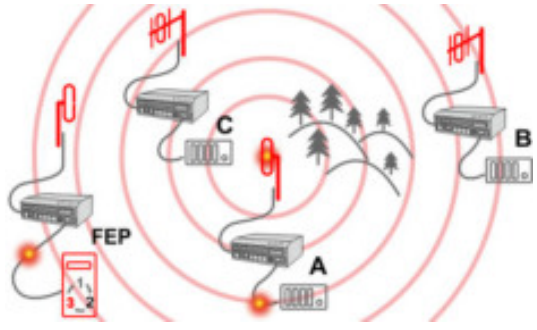
Step 1

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



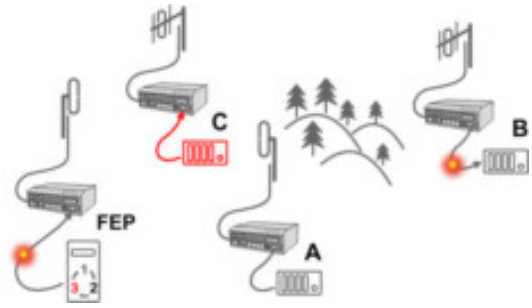
Step 2

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 .



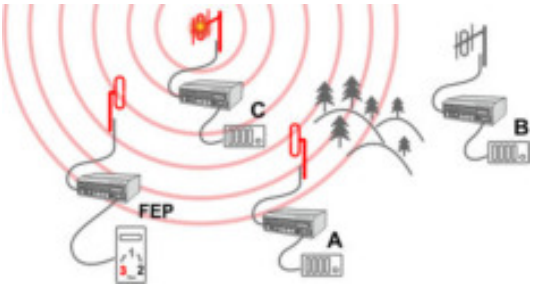
Step 3

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.



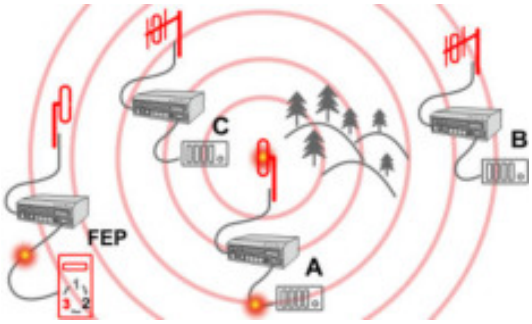
Step 4

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.



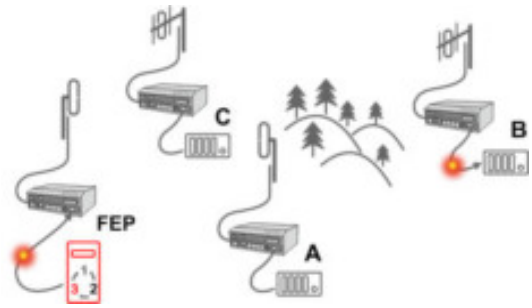
Step 5

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…

5.1.3. 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 ETH 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).

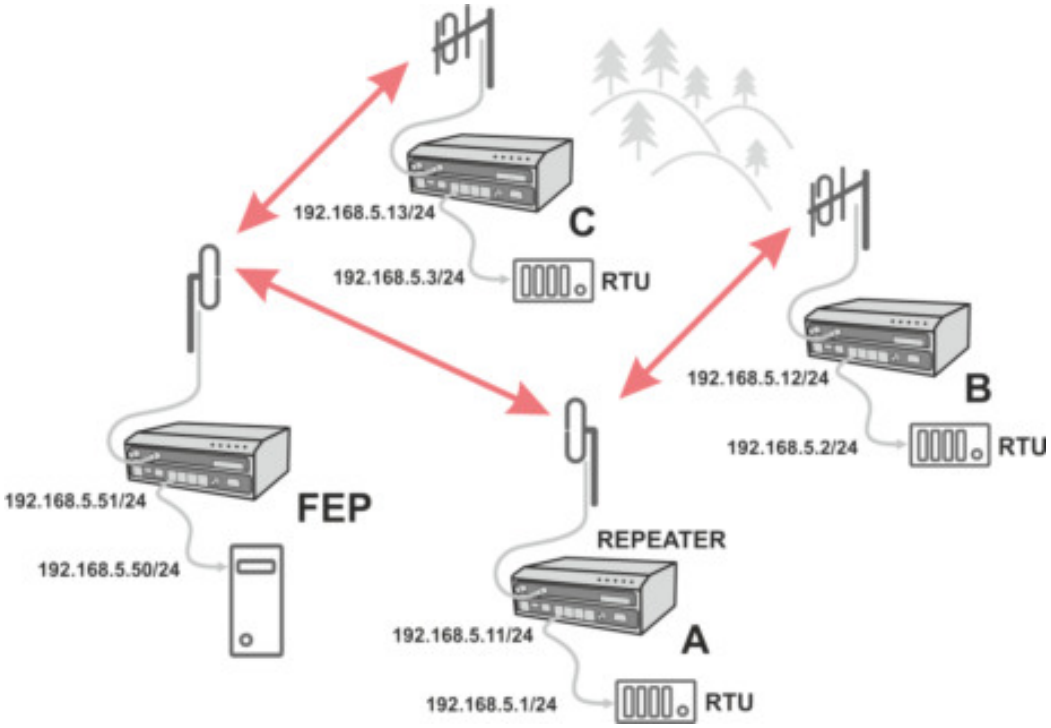


Fig. 5.1: Bridge mode example

Repeater

Because using the bridge mode makes the 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.

5.2. Router mode

5.2.1. Detailed Description

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.

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.

5.2.2. Router - Base driven, Detail description

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.

5.2.3. 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.

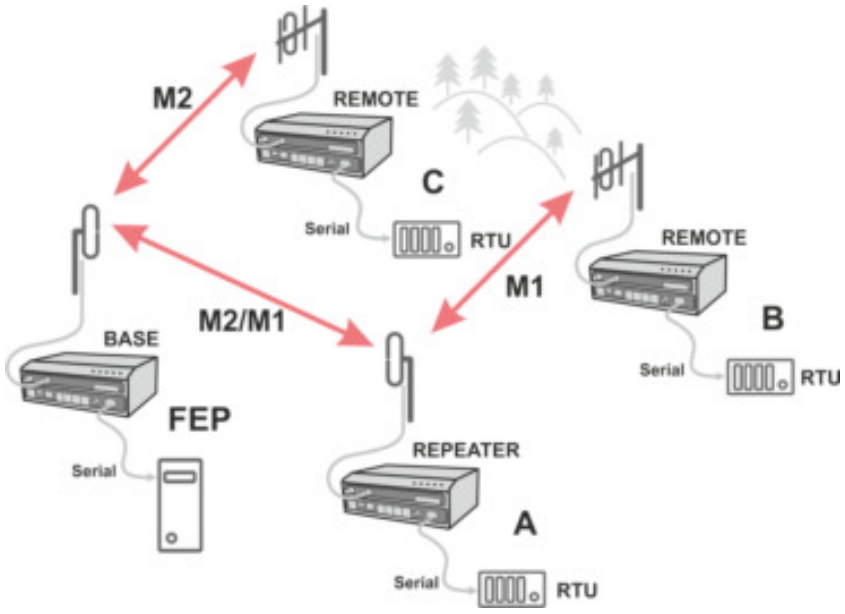


Fig. 5.2: Router - Base driven, Functionality example

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.

5.2.4. 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.

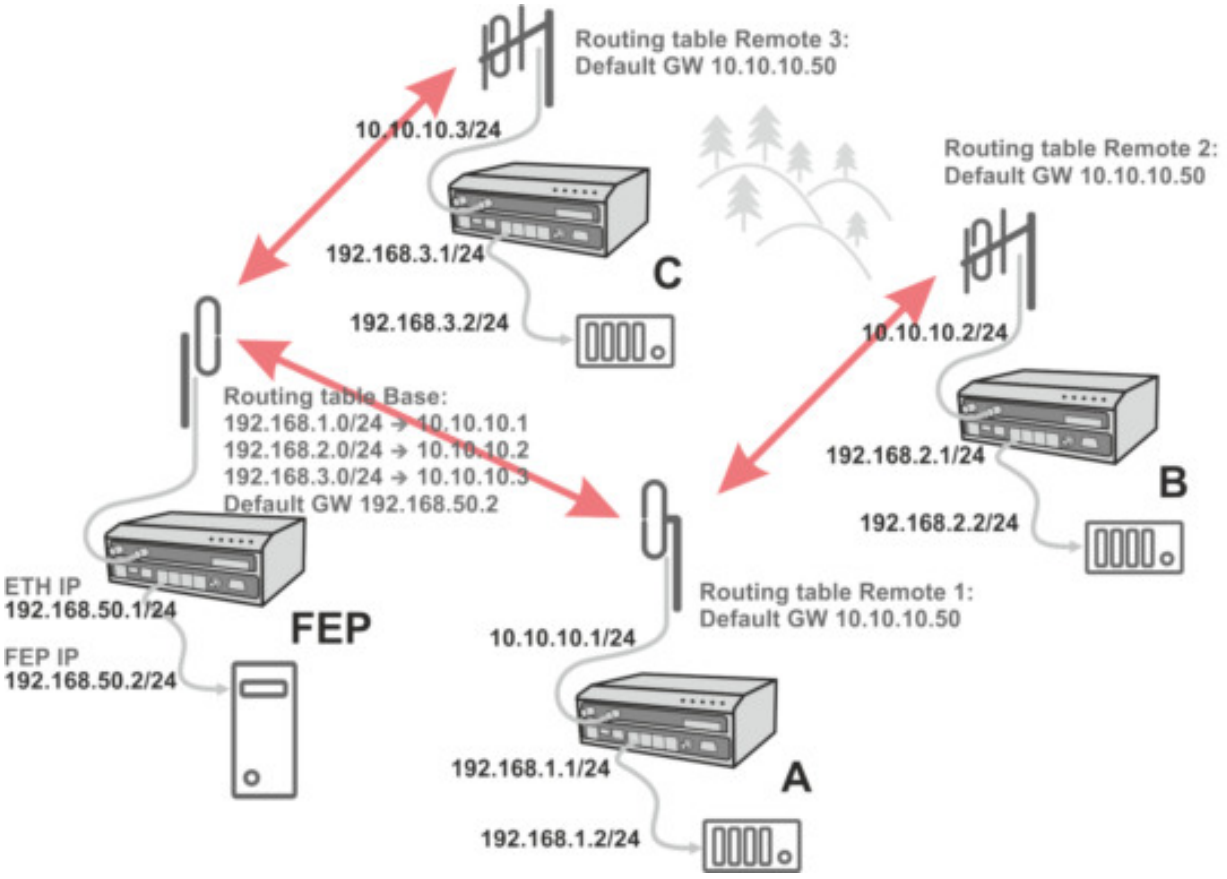


Fig. 5.3: Router - Base driven, Addressing

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.

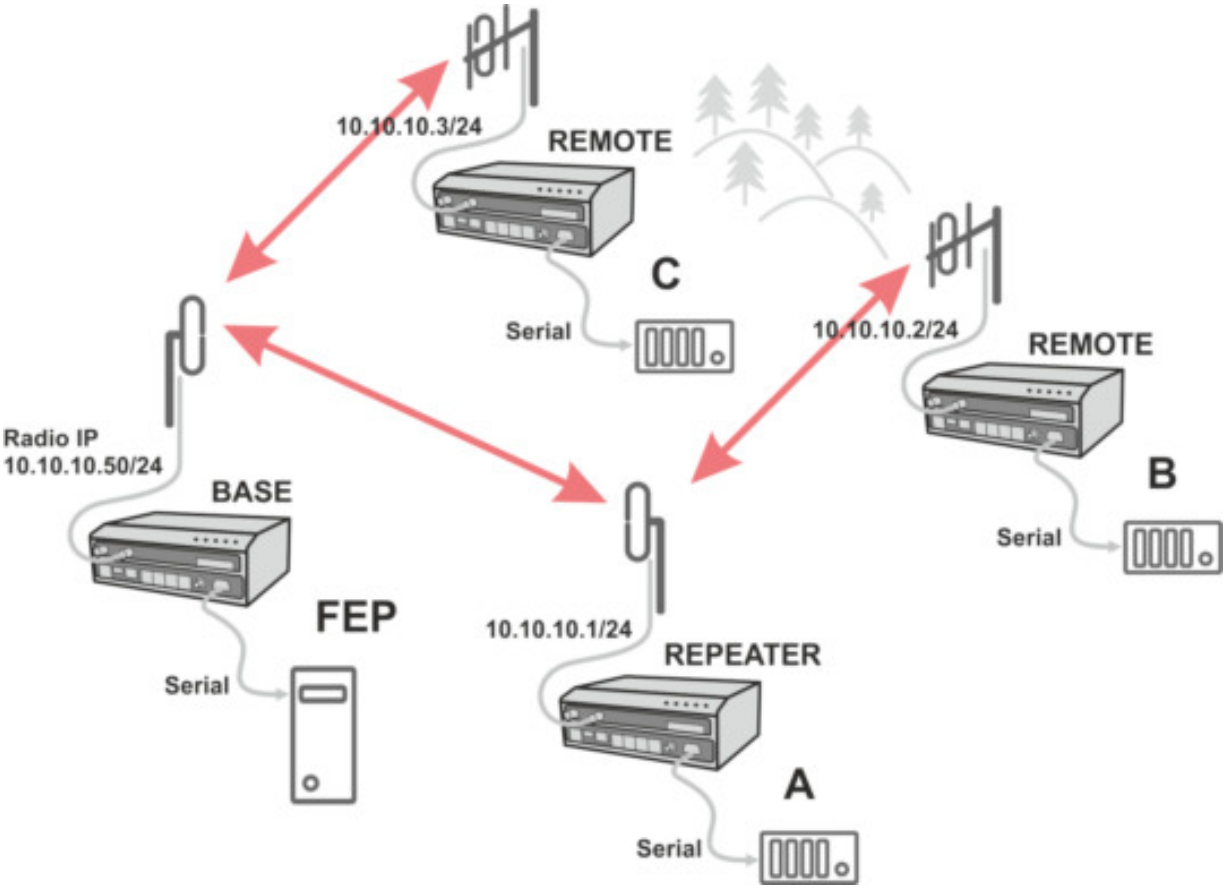


Fig. 5.4: Router - Base driven, Addressing - Serial

5.3. 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).

You can see an instructional video explaining the Terminal server functionality here: *https://www.racom.eu/ripex-terminal*

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.

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 connected 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 (IP of ETH interface in Local RipEX2) and the destination IP (either Radio or ETH interface in Remote RipEX2) exist needs to be configured properly.

When in Bridge mode, IP addresses of Ethernet interfaces are used for both the Local and Remote units. 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.

- **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 changing of the language of the whole web interface (English language is default).

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

- **Web page header**

The header of each web page contains:

  - Unit name and
  - IP address of the RipEX2 unit you are connected to
  - Identification of the web current page (2nd or 3rd level of the menu)
  - Remote access button
  - Changes to commit button
  - Refresh settings button
  - User menu button

6.1. Supported web browsers

Supported web browsers for desktop are current versions of:

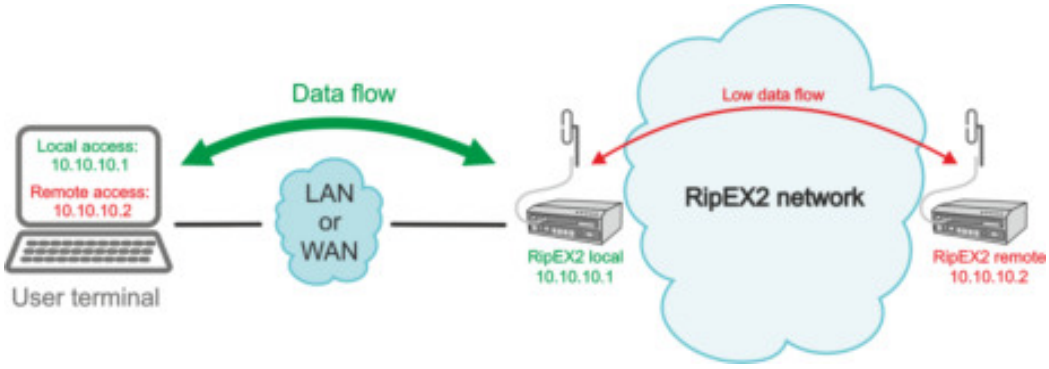
- Edge
- Chrome
- Firefox
- Safari
- Internet Explorer v.11

Supported Web browsers for mobile equipment are current versions of:

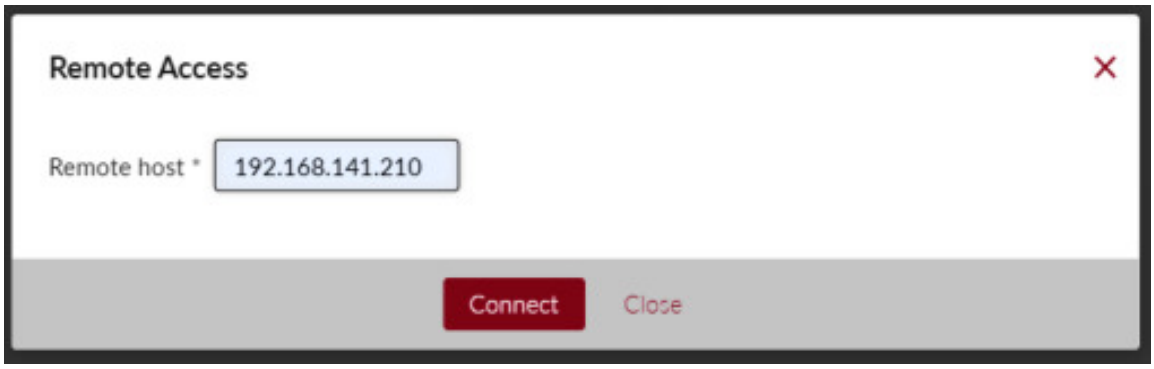
- Safari for iOS
- Chrome for android

6.2. Remote access

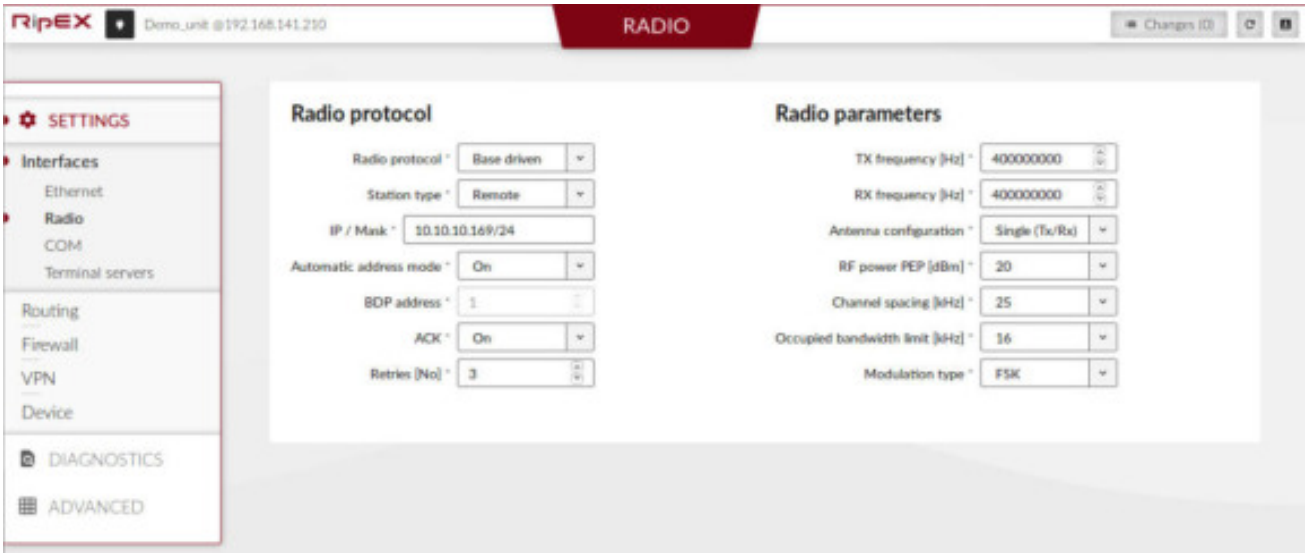
RipEX2 unit management is designed to work smoothly even when the unit under configuration is connected via relatively slow radio channel. In case of locally connected unit - direct configuration of the unit (accessing the unit IP address directly from the web browser) works fine. If the unit should be connected remotely via the radio 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 radio (which needs to be accessible from the locally connected unit via the RipEX2 network).



Remote access can be activated via click on the Remote access button.



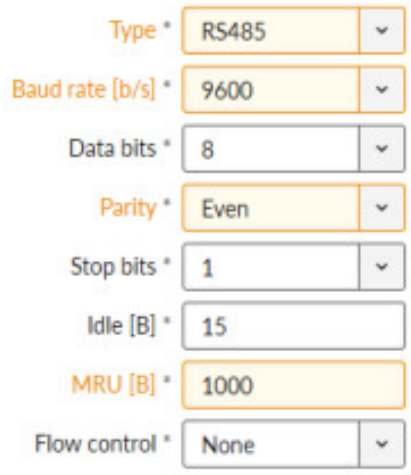
The connection to remote radio proceeds...



The IP address of the actually connected RipEX2 unit is displayed as 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.

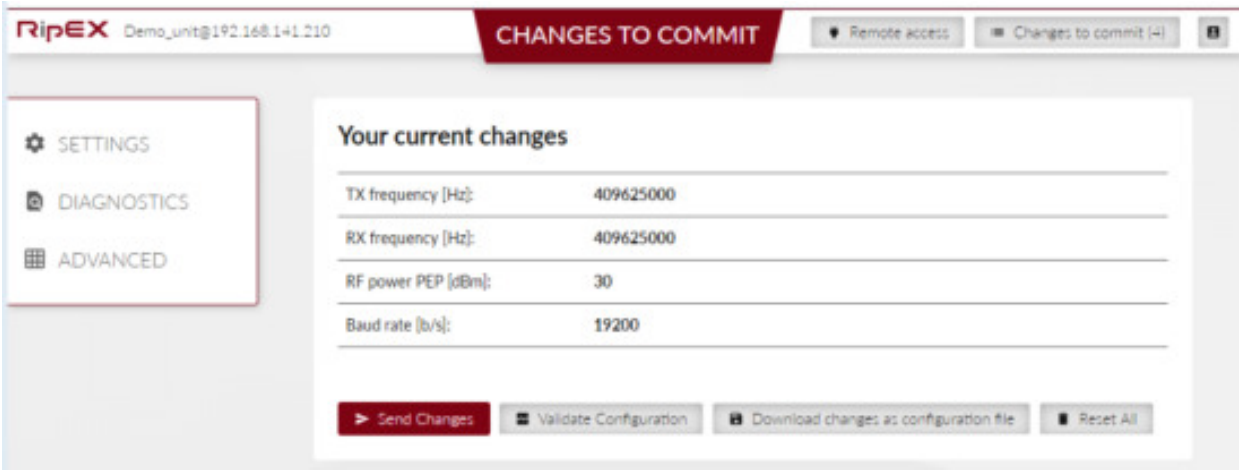
6.3. Changes to commit

All changes of configuration parameters are marked by different color.



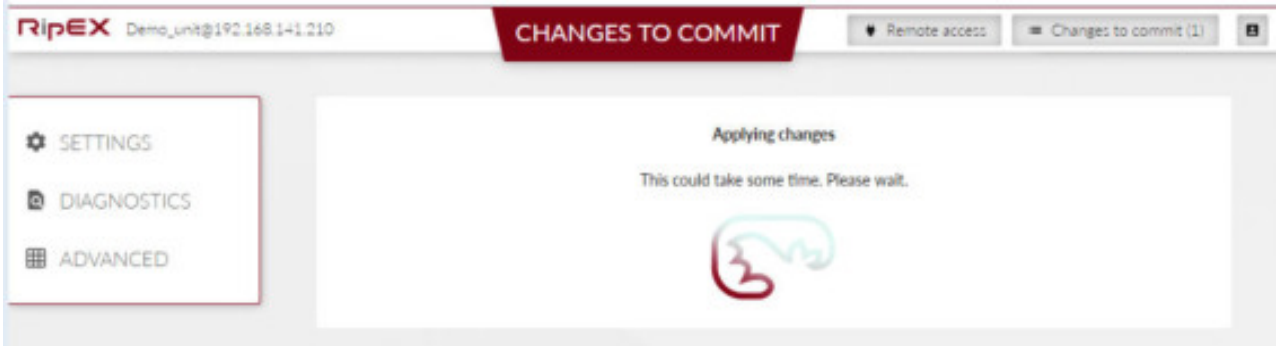
Multiple configuration changes in various menus can be prepared prior to final Commit.

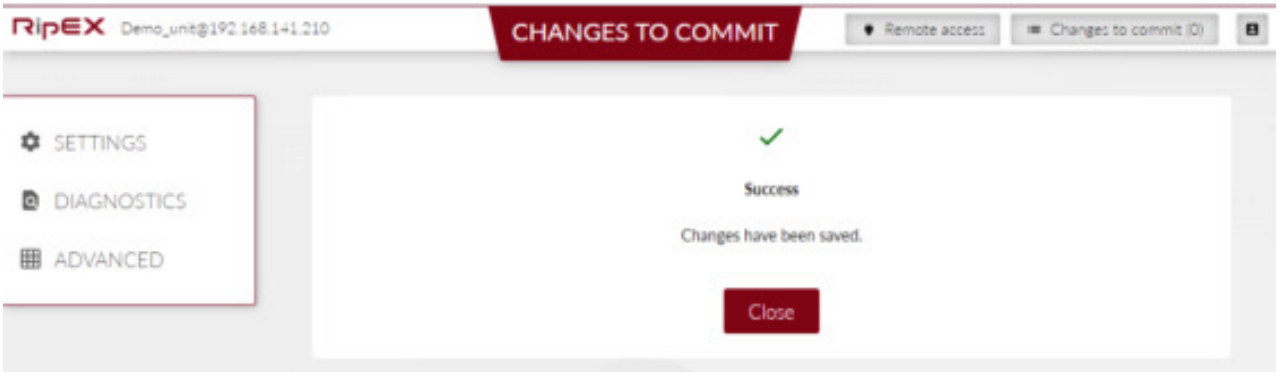
Changes to commit "basket" collects all the changes.



You can:

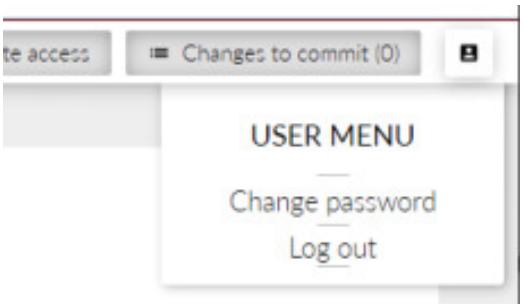
- Apply (Save to radio unit) all the changes using Send Changes or





- Discard all changes via Reset All

6.4. User menu



It is strongly recommended to change the default password.

7. Settings

Information provided in this chapter is identical with the content of Helps for individual menu.

7.1. Interfaces

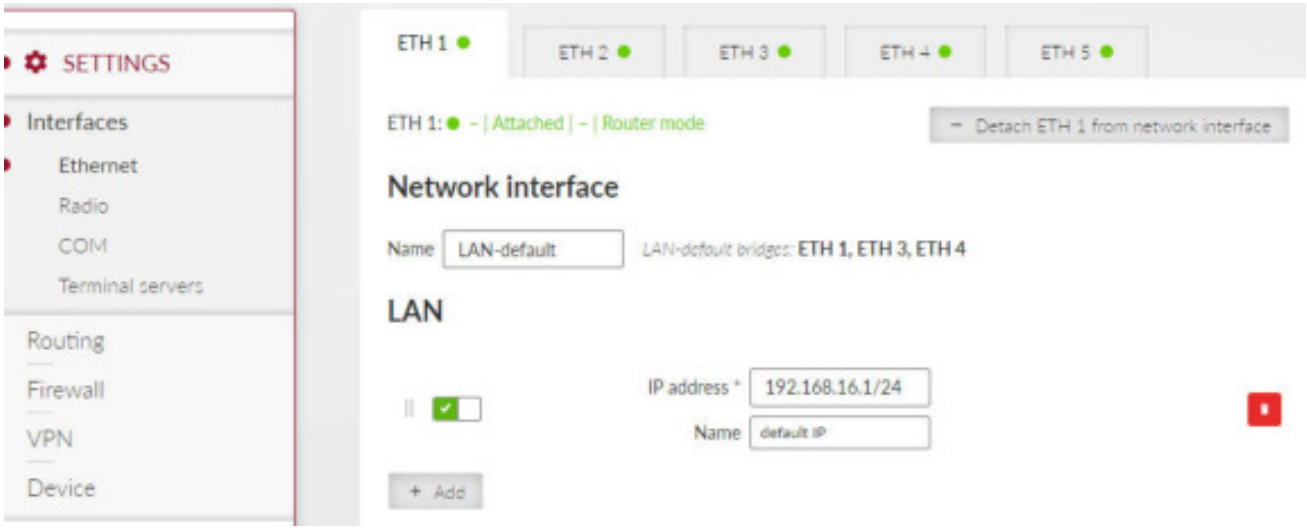
7.1.1. Ethernet

RipEX2 provides 5 physical Ethernet ports ETH1, ETH2, ETH3, ETH4 and ETH5. First 4 ETH ports are metallic, the 5th port is a 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.

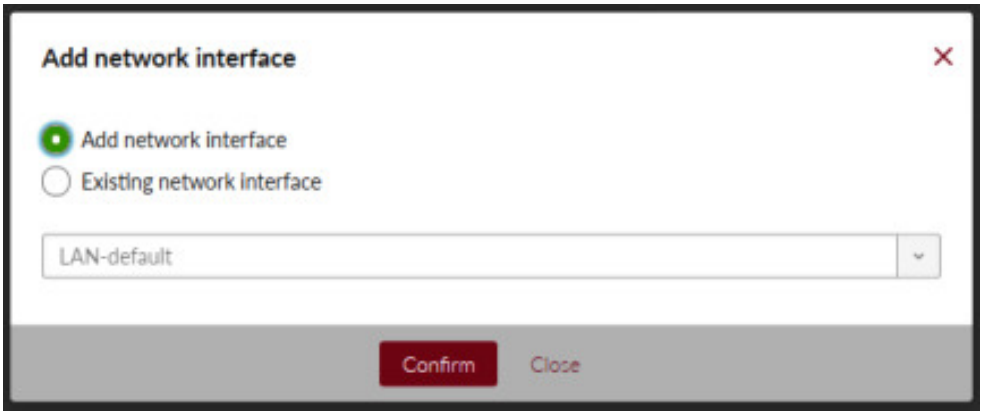
The Network interface (technically - an Ethernet bridge) is identified by a name. The name always begins with a "LAN-" prefix. Multiple Network interfaces can be defined. Multiple physical Ethernet interfaces can be bridged together by using single Network interface.

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 Radion 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.



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.



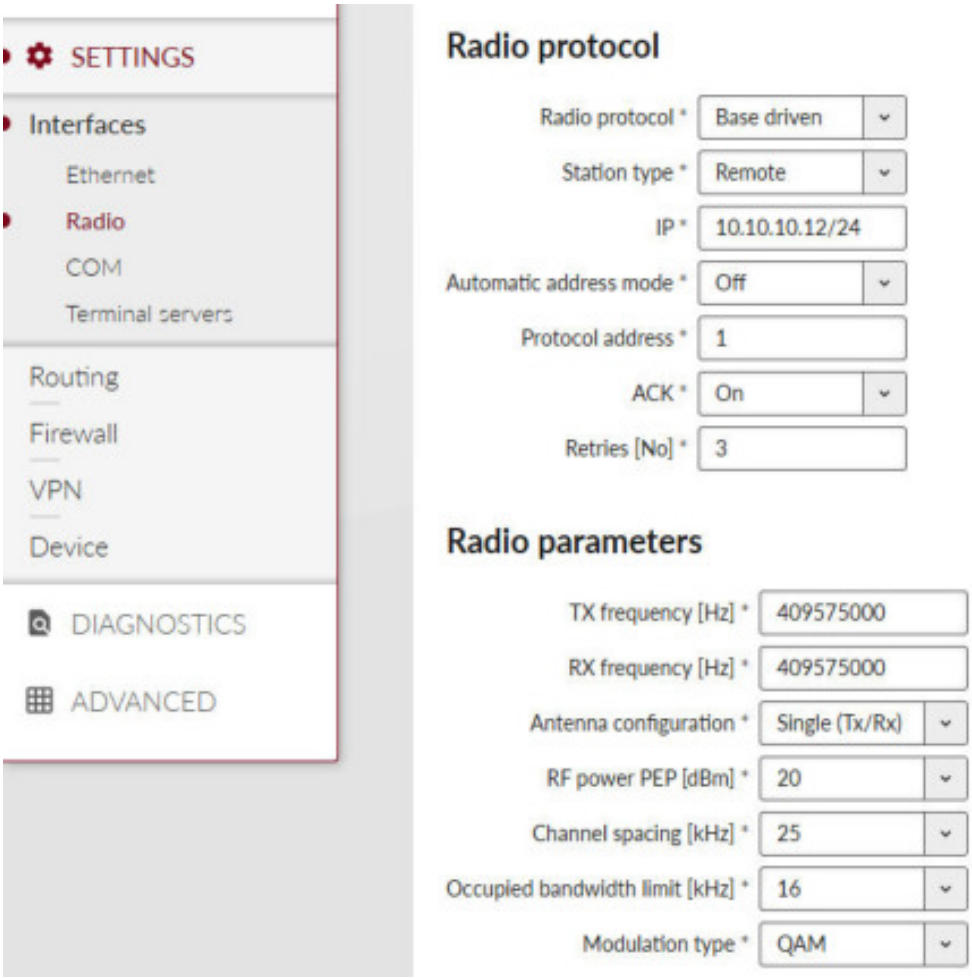
Single or multiple Ethernet subnets can be defined within one Network interface. Each subnet is identified by its IP address&mask. Use the optional field. Note to keep your network configuration in human readable manner.

Enable / Disable: enables / disables specific Ethernet subnet

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

Note Optional Ethernet subnet description

7.1.2. Radio



a) Radio protocol

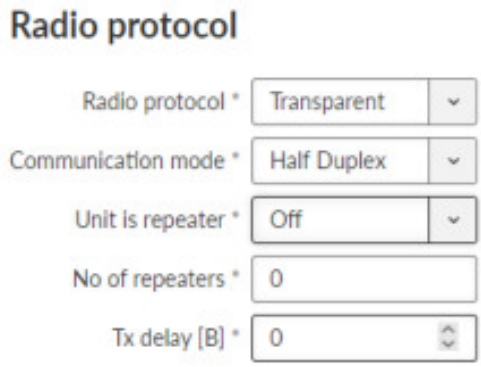
- **Radio protocol:** type of the radio protocol
  - **Transparent** (bridge mode) default
  - **Base driven** (router mode)
- **Transparent** (bridge mode)

  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 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.



- **Communication mode**

  List box {Half Duplex, Full Duplex}, default Half Duplex

  Full duplex operation is available only for Point-to-Point communication.

- **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**

  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]**

  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.

- **Base driven protocol**

Router mode with Base driven protocol 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.

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.

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.

- **Station type**

List box {Base, Remote}, default Base

- **Base**

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

- **Remotes**

  Radio protocol parameters for every Remote station must be configured in this table.

- **Protocol address**

Protocol address [0 to 255] is the unique address assigned to each Remote and is used only 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 (Protocol address mode in Remote unit is then set to Automatic address mode).

Note

If you configure any Remote station protocol addresses, which are not present in the running network, radio channel access will be granted to them regularly resulting in lower total network throughput: Every address listed in this table will be taken into consideration, when configuring radio channel access. It is possible to prepare configuration for an additional radio unit in the network if needed. The “Active” parameter (see below) within such a table record can be marked as not active. In this case, the record is never granted radio channel access.

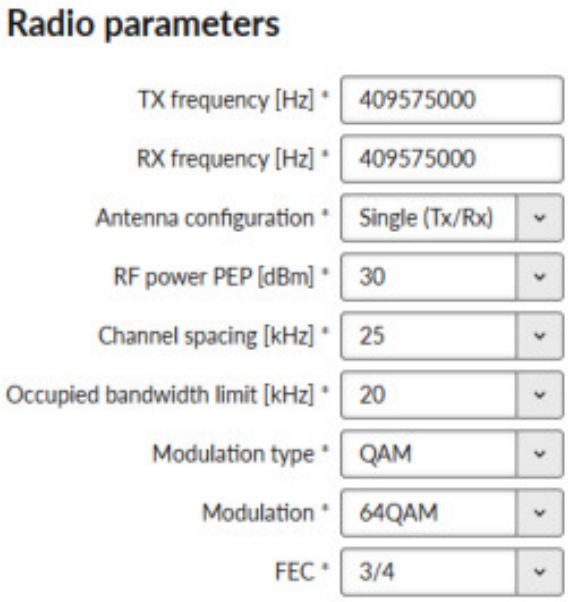
- **ACK**

  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.

- **Retries**

  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.

b) Radio 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

  RipEX2-3B: 335-400 MHz

  RipEX2-4A: 400-470 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

- **RF power PEP**

  Setting of RF power in dBm (PEP) for the maximum power for individual modulations and the relationship between PEP and RMS see *Tab. 9.10* of this manual.

- **Channel spacing [kHz]**

  List box {possible values}, default = 25 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 *chapter 7.1.2. Detailed Radio 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.

    Note

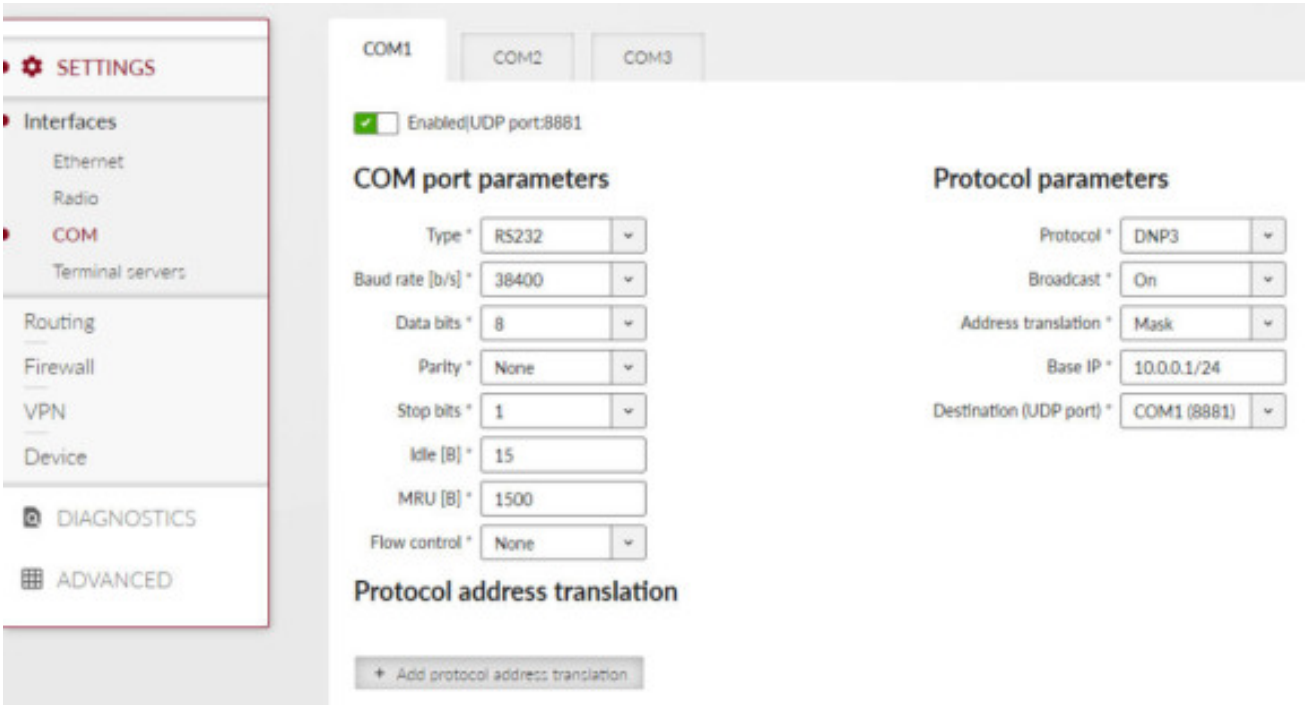
    QAM belongs to the phase shift keying family of linear modulations. Compared to FSK (non-linear modulations), QAM is characterized by wider bandwidth. The spectral efficiency is higher, power efficiency is lower and system gain is typically lower.

- **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 user data rate. The lower the FEC ratio, the better the capability of error correction and the lower the user data rate. The User data rate = Modulation rate × FEC ratio.

7.1.3. COM



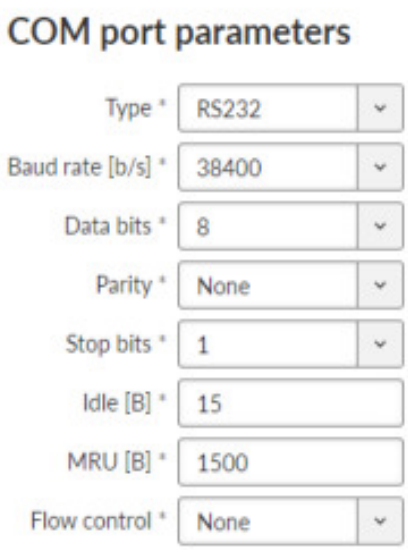
The menu is divided to two parts:

- **COM port parameters**

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

- **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.



- **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 300 to 1152000 b/s}, default = 19200.

  Select Baud rate from the list box: 300 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 {8, 7}, default = 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: {possible values}, default = 1

  Wikipedia: Stop bits send 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 [B]**

  Default = 5 [0 - 2000]

  This parameter defines the maximum gap (in bytes) 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]**

  Default = 1600 [1 - 1600]

  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.

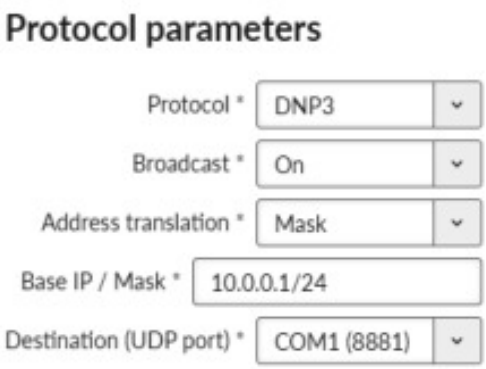
- **Flow control**

  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.



- **Protocol**

  List box: {None, Async Link, DNP3, DF1}, default = DNP3

  Common parameters:

  - **Broadcast**

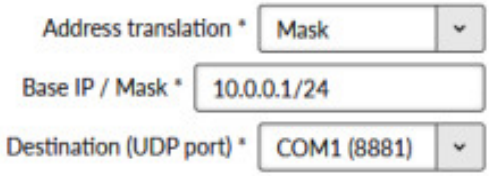
    List box: {On, Off}, default = on

    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.

- **Address translation**

  SCADA protocol address is translated to the IP address using either Mask or Table type of conversion.

- **Mask**



  - **Base IP / Mask**

    Default = IP address of ETH interface

    When the IP destination address of UDP datagram, in which serial SCADA message received from COM is encapsulated, is created, this Base IP is taken as the basis and only the part defined by Mask is replaced by 'Protocol address'.

    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.

  - **/Mask**

    Default = 24 (i.e. 255.255.255.0)

    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.

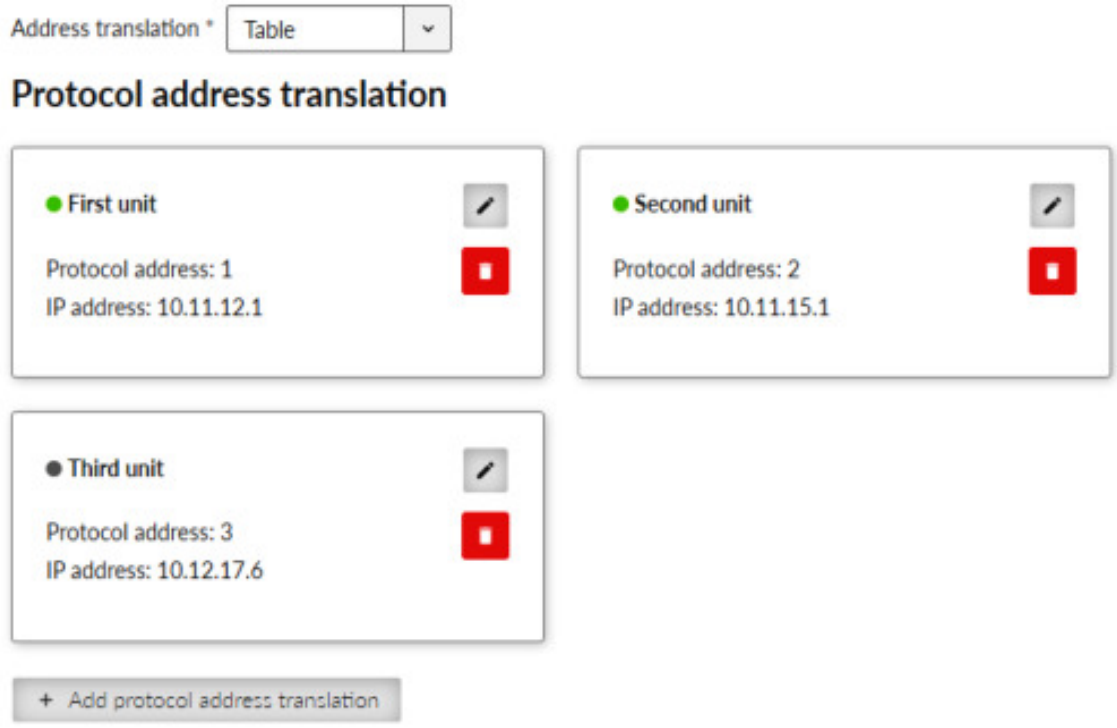
- **Destination (UPD port)**

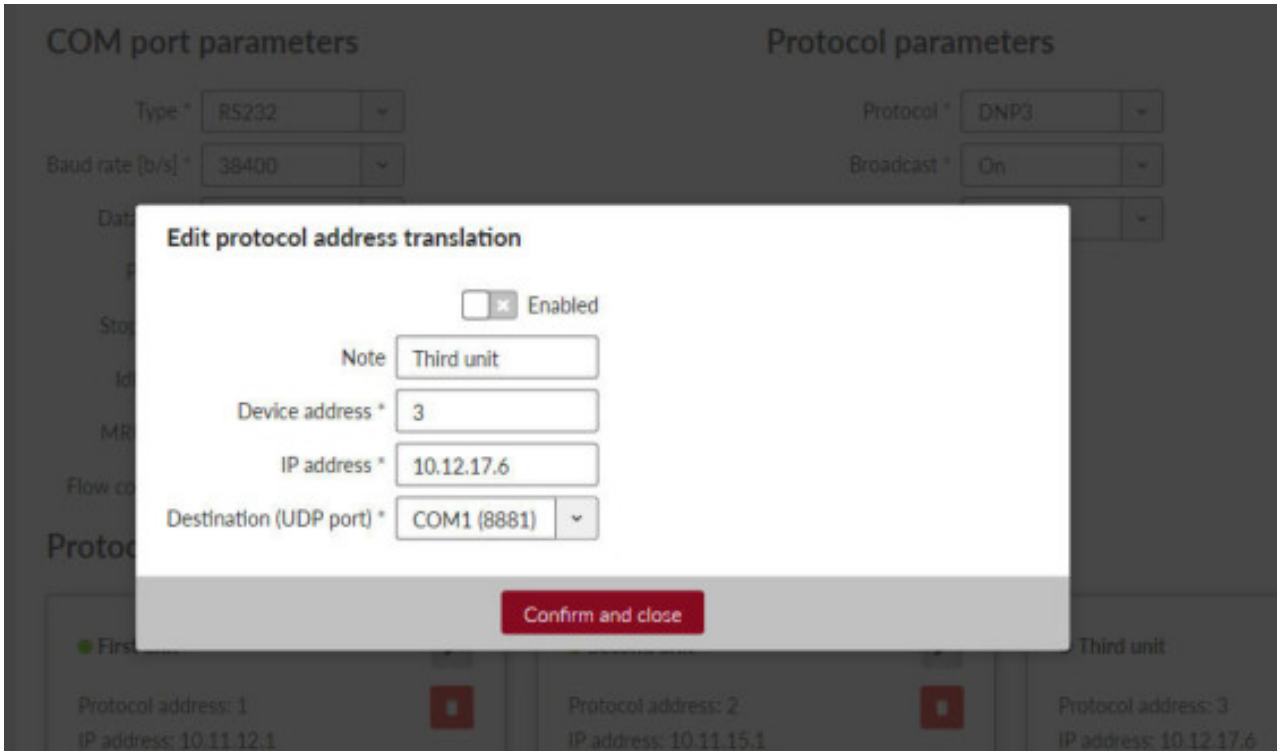
  List box: {COM, TS1-TS5, Manual}

  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 destination 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.

- **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.

- **Protocol address**

  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.

- **IP address**

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

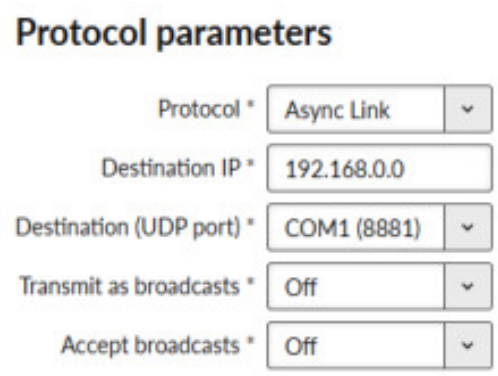
- **Destination (UDP port)**

  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.

Individual parameters

- **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 to Radio channel to set IP destination and UDP port. Received frames from Radio channel are sent to COM or Terminal server according to Destination (UDP port) parameter.



- **Destination IP**

  This is IP address of destination RipEX2, either ETH or Radio interface.

- **Destination (UDP port)**

  This is UDP port number, which is used as a destination UDP port in UDP datagram, in which packet received from COM (or TS) is encapsulated.

- **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 spontaneous communication from the remote units.

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

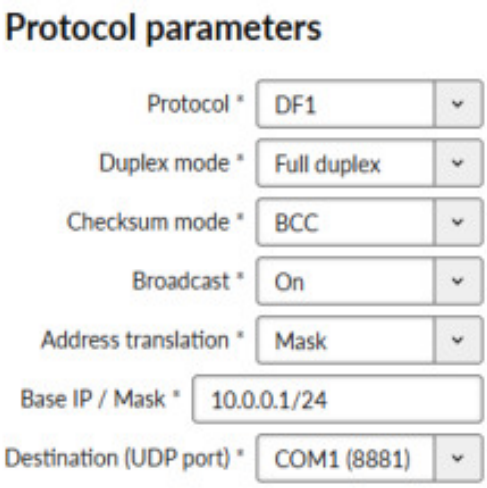
  Note

  Broadcast

  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.

- **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}

- **Connected service mode**

  List box {Master, Slave}, default=Slave

  SCADA application follows Master-Slave scheme, where the structure of the message is different for Master and Slave SCADA units. Because of that it is necessary to set which type of SCADA unit is connected to the RipEX2.

  Note

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

- **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

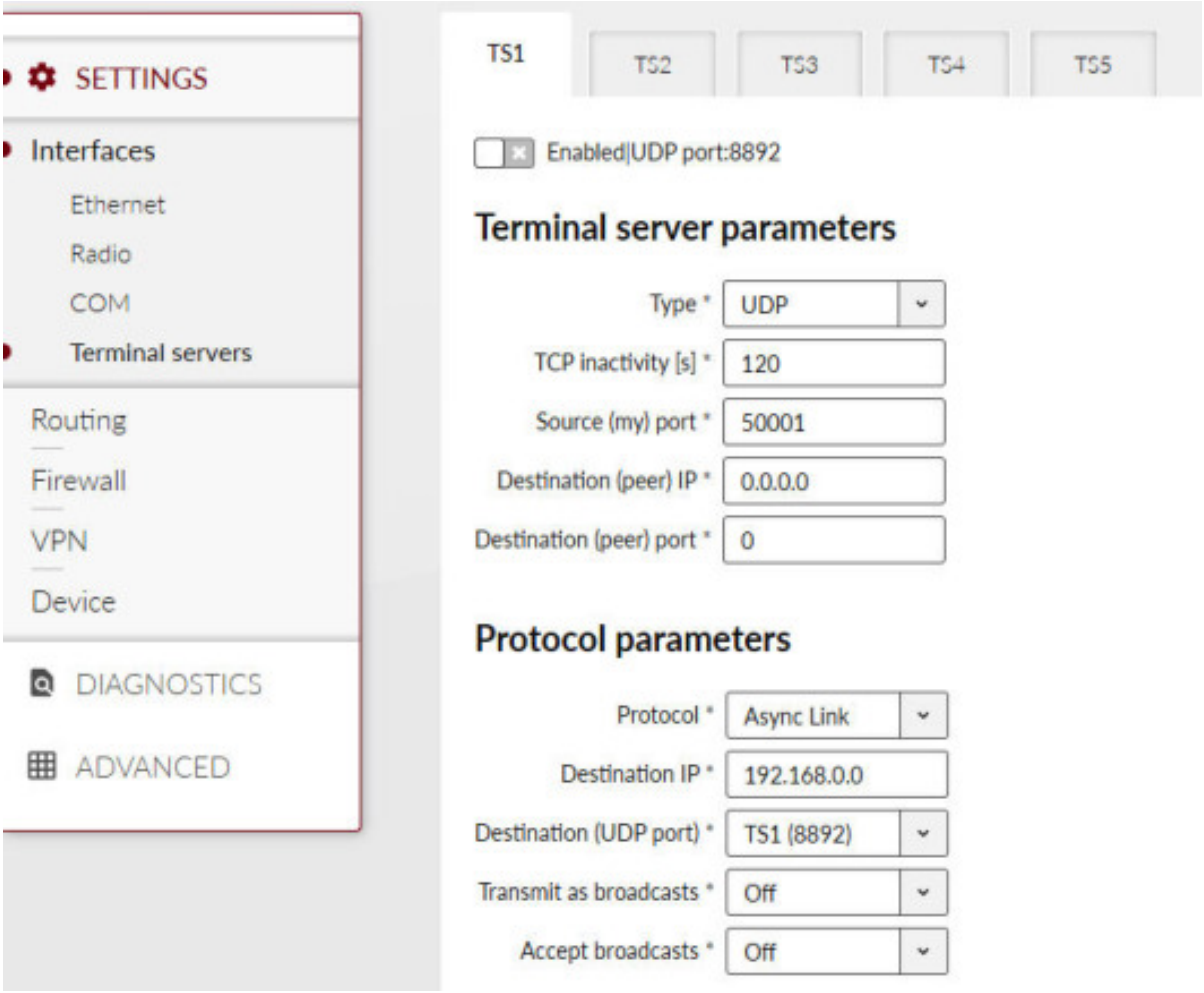
  Broadcast

  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.

7.1.4. 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.



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 chap. 7.2.1), **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.

Note

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

7.2. Routing

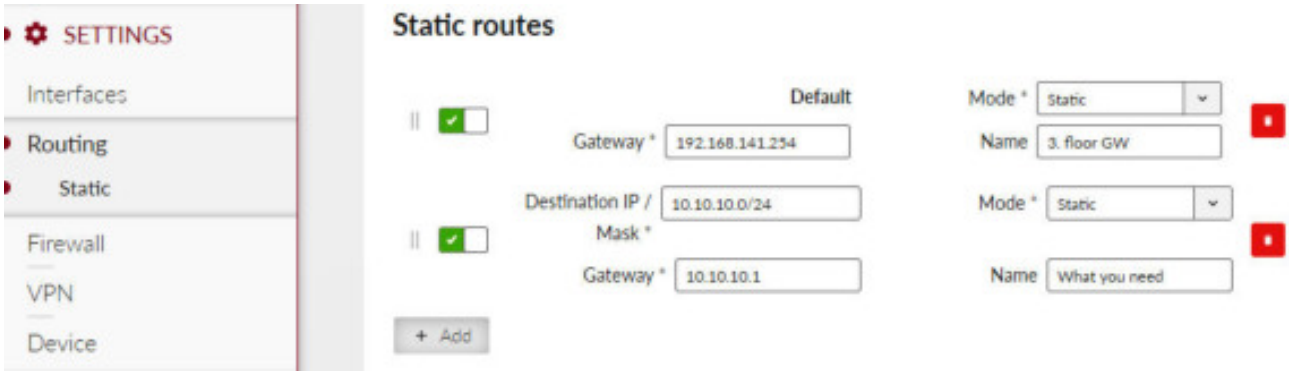
7.2.1. Static

Routing table is active only when Router mode (Settings/Device/Operating mode) is set. In such a case 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. Then 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.



- **Active** {On / Off}

  Switches the rule on / off

- **Destination IP / mask**

  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 and Mask) is written in CIDR format, e.g. 10.11.12.13/24.

Note

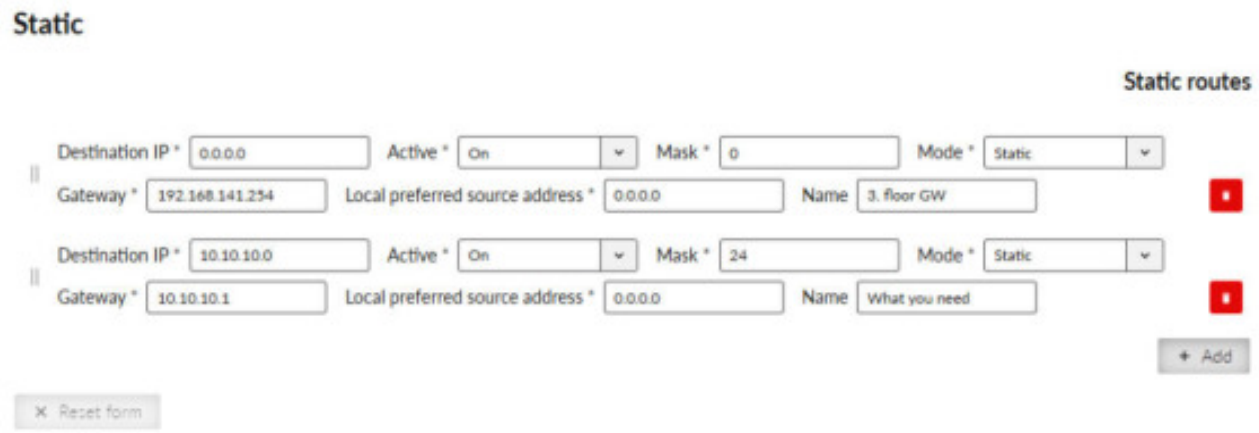
Networks defined by IP and Mask for Radio and other interfaces must not overlap.

- **Mode** {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).

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

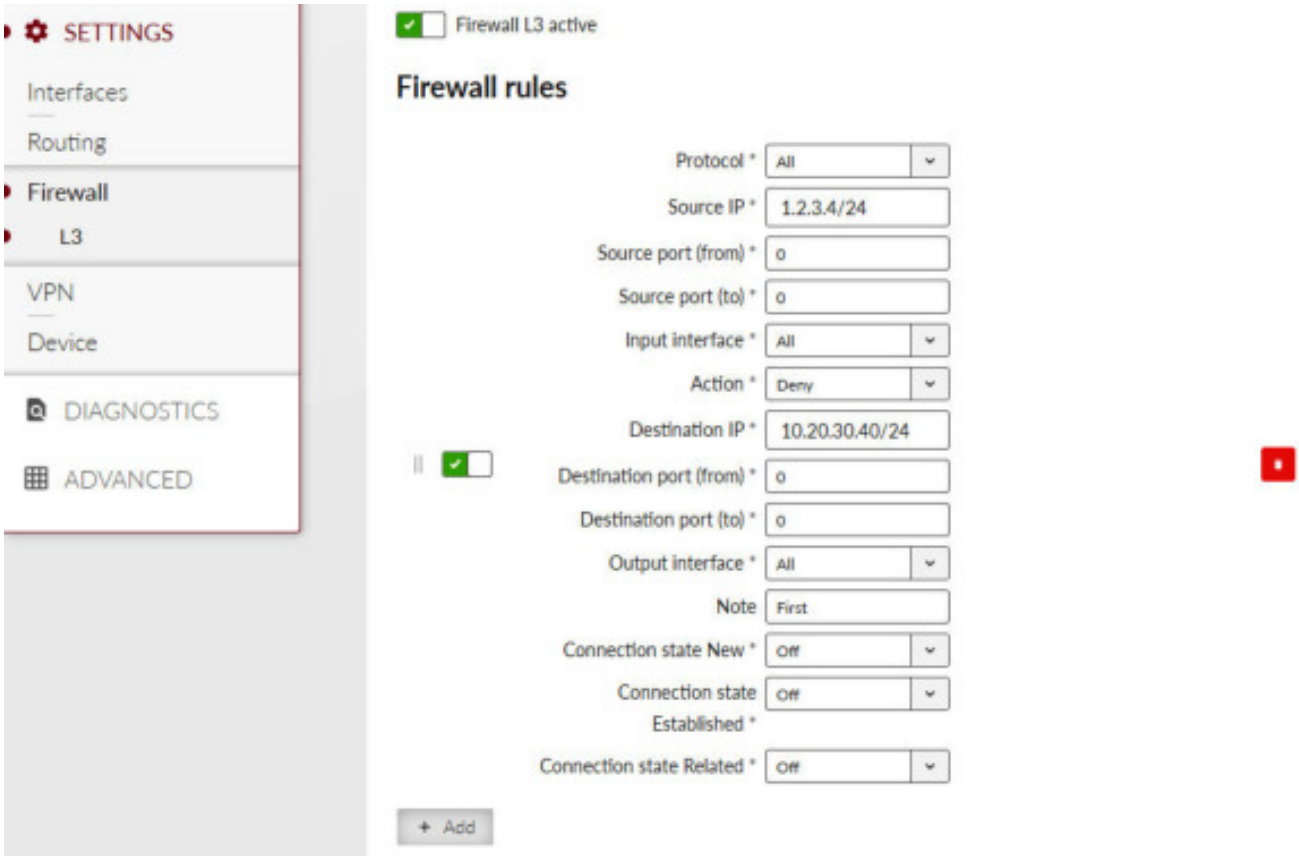
- Menu ADVANCED / Routing / Static allows to set additional parameter:



Local preferred source address: (Routing_LocalUseSrcAddr) 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.

7.3. Firewall

7.3.1. L3



Firewall L3 active switches L3 firewall Off, On; default is Off

Each individual firewall rule is described by the following items:

- **Protocol**

  List box {All, ICMP, UDP, TCP, GRE, ESP, Other}

- **Source IP/Mask** source IP address and mask.

  The rule with narrower mask has higher priority. The rule's order does not affect priority.

- **Source port (from)** and **(to)** interval of source ports
- **Input interface** list box {All, Radio, All ETH, ETH1..ETH5, Other}
- **Action** list box {Deny, Allow}, default Deny
- **Destination IP/Mask**
- **Destination port (from)** and **(to)** interval of destination ports
- **Output interface** list box {All, Radio, All ETH, Other}

- **Connection state New** list box {Off, On} active only for TCP protocol

  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} active only for TCP protocol

  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} active only for TCP protocol

  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

L2/L3 firewall settings do not impact the local ETH access, i.e. settings never deny access to a locally connected RipEX2 (web interface, ping, ...).

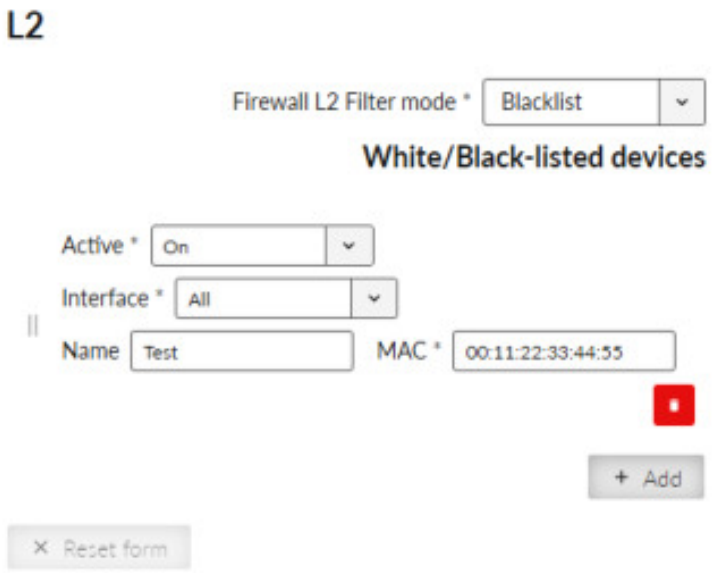
Note

Ports 443 and 8889 are used (by default, can be overridden) internally for service access. Exercise caution when making rules which may affect datagrams to/from these ports in L3 Firewall settings. Management connection to a remote RipEX2 may be lost, when another RipEX2 acts as a router along the management packets route and port 443 (or 8889) is disabled in firewall settings of that routing RipEX2 (RipEX2 uses iptables "forward").

Note

L3 Firewall settings do not impact packets received and redirected from/to Radio channel. The problem described in NOTE 2 will not happen, if the affected RipEX2 router is a radio repeater, i.e. when it uses solely the radio channel for input and output.

7.3.2. L2



- **Active** list box {Off, On}

  If "On" and when in the Router mode, Layer 2 Linux firewall is activated:

- **Filter mode** list box {Blacklist, Whitelist}, default Blacklist

  - **Blacklist**

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

  - **Whitelist**

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

- **Interface** list box {All, ETH1..ETH5}, default All

  MAC IPv4 MAC address

7.4. VPN

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

7.4.1. Basic Description

Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys for use during the session. IPsec uses cryptographic security services to protect communications over Internet Protocol

(IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec is an end-to-end security scheme operating within the Internet Layer of the Internet Protocol Suite. IPsec is recognized as a secure, standardized and well-proven solution by the professional public.

Although there are 2 modes of operation RipEX2 only offers Tunnel mode. In Tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet (ESP – Encapsulating Security Payloads) with a new IP header.

Symmetrical cryptography is used to encrypt the packets. The symmetric keys must be safely delivered to the peer. In order to maintain a secure connection, symmetric keys must be regularly exchanged. The protocol used for secure key exchange is IKE (Internet Key Exchange). Both IKE version 1 and the newer version 2 are available in 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.

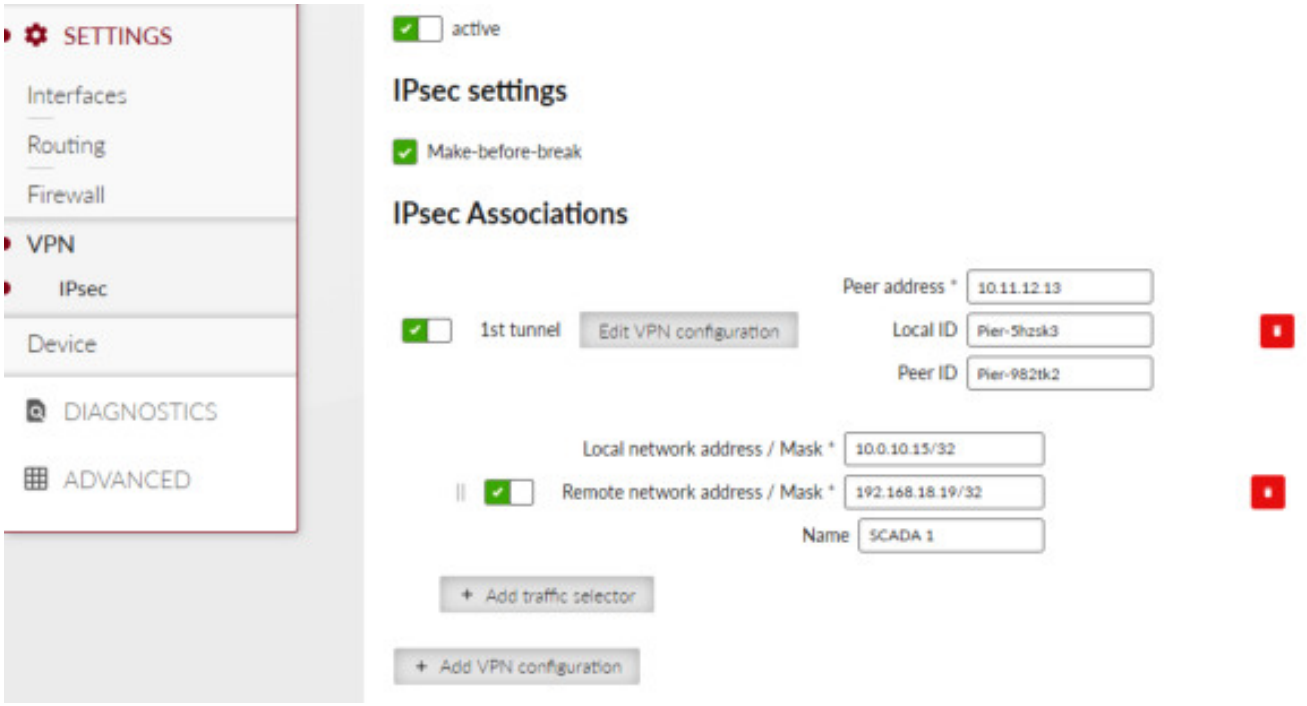
Link partner (peer) secure authentication is assured using Pre-Shared Key (PSK) authentication method: Both link partners share the same key (password).

As and when the CHILD SA expires, new keys are generated and exchanged using IKE SA.

As and when the IKE SA version IKEv1 expires - new authentication and key exchange occurs and a new IKE SA is created. Any CHILD SA belonging to this IKE SA is re-created as well.

As and when the IKE SA version IKEv2 expires one of two different scenarios might occur:

- If the re-authentication is required - the behavior is similar to IKEv1 (see above).
- It the re-authentication is not required - only new IKE SA keys are generated and exchanged.



- **Configuration**

  Active {On, Off}

  IPsec system turning On/Off

- **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).

- **Peer Address**

  Default = 0.0.0.0

  IKE peer IP address.

- **Local ID**

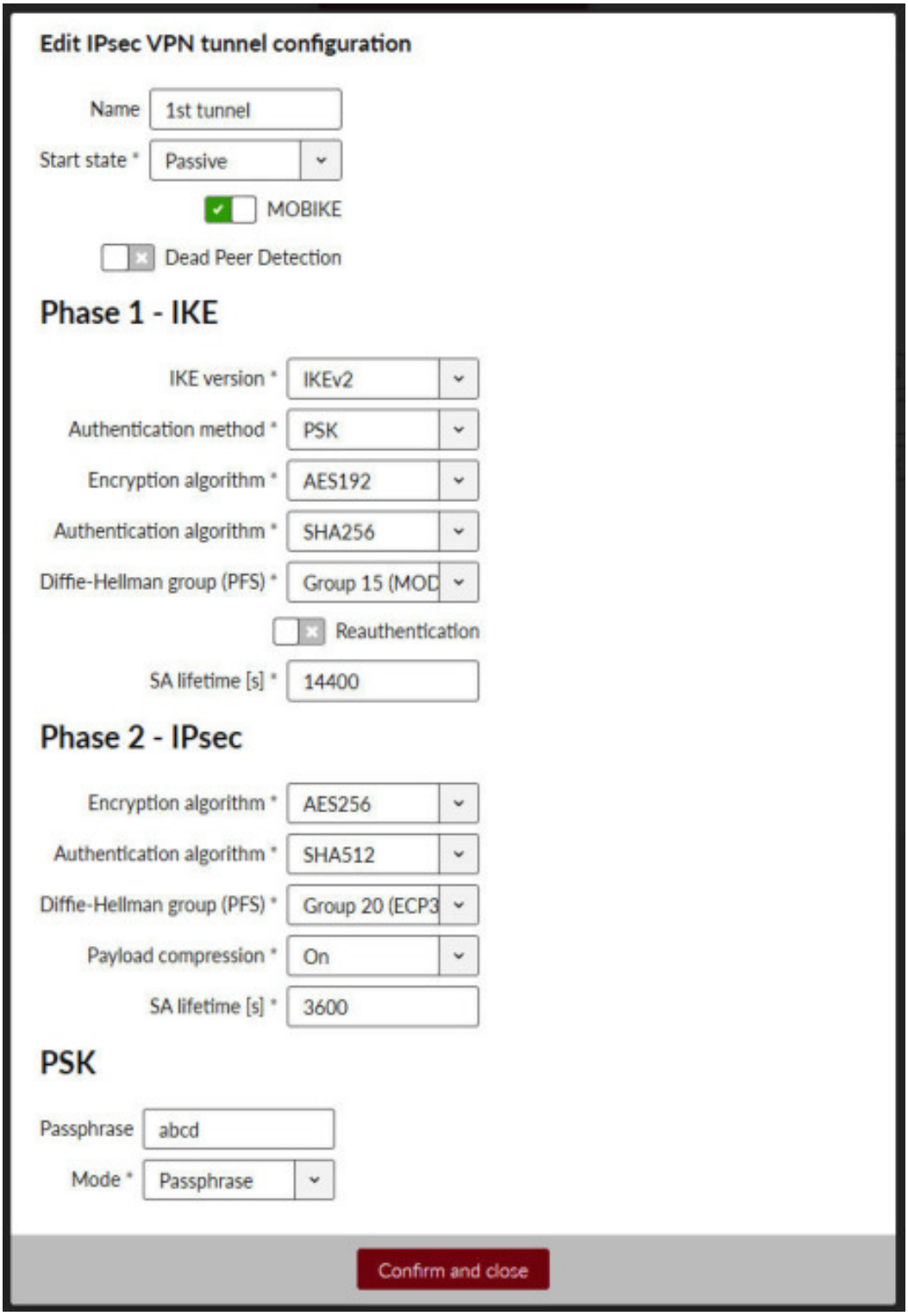
  IP address or FQDN (Fully Qualified Domain Name) is used as the Local side identification. It must be the same as "Peer ID" of the IKE peer.

- **Peer ID**

  IP address or FQDN (Fully Qualified Domain Name) is used as the IKE peer identification. It must be the same as "Local ID" of the IKE peer. The "Peer ID" must be unique in the whole table.

- **Add / Edit IPsec associations**

  Every item in the table represents one IKE SA. There can be a maximum of 8 active IKE SA (limited by system resources).



- **Start state**

  List box {Passive, On demand, Start}, default Passive

- **MOBIKE**

  List box {On, Off}, default On

Enables MOBIKE for IKEv2 supporting mobility or migration of the tunnels. Please note IKE is moved from port 500 to port 4500 when MOBIKE is enabled. The peer configuration must match.

- **Dead Peer Detection**

  List box {On, Off}, default = On

  Detection of lost connection with the peer. IKE test packets are sent periodically. When packets are not acknowledged after several attempts, the connection is closed (corresponding actions are initialized). In the case when Detection is not enabled, a connection loss is discovered when regular key exchange process is initiated.

- **Phase 1 IKE**

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

  - **IKE version**

    List box {IKEv1, IKEv2}, default = IKEv2

    IKE version selection. The IKE peer must use the same version.

  - **Authentication method**

    List box {PSK}

    Peer authentication method. Peer configuration must match.

    The "main mode" negotiation is the only option supported. The "aggressive mode" is not supported; it is recognized as unsafe when combined with PSK type of authentication

  - **Encryption algorithm**

    List box {3DES (legacy), AES128, AES192, AES256}, default = AES128

    IKE SA encryption algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

  - **Authentication 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.

    The same value as selected for the Integrity algorithm, is used for the PRF (Pseudo-Random Function).

  - **Diffie-Hellman group (PFS)**

    List box {None (legacy), Group 2 (MODP1024, legacy), Group 5 (MODP1536, legacy),

    Group 14 (MODP2048), Group 15 (MODP3072), Group 25 (ECP192), Group 26 (ECP224),

    Group 19 (ECP256), Group 20 (ECP384), Group 21 (ECP521), Group 27 (ECP224BP),

Group 28 (ECP256BP), Group 29 (ECP384BP), Group 30 (ECP512BP)}, 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 RipEX2 unit load is seriously affected when key exchange is in process. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

The higher the Diffie-Hellman group, the higher the security but also the higher the network and CPU load.

- **Reauthentication**

  List box {On, Off}, default = Off

  This parameter is valid if IKEv2 is used. It determines the next action after IKE SA has expired. When enabled: the new IKE SA is negotiated including new peer authentication. When disabled: only the new keys are exchanged.

- **SA lifetime [s]**

  Default = 14400 s (4 hours). Range [180 - 86400] s

  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%, to prevent collision when the key exchange is triggered from both sides simultaneously.

  Unfortunately, the more frequent the key exchange, the higher the network and CPU load.

- **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.

- **Authentication algorithm**

  List box {MD5 (legacy), SHA1 (legacy), SHA256, SHA384, SHA512}, default = SHA256

  IKE CHILD SA integrity algorithm. The "legacy" marked methods are recognized as unsafe. Peer configuration must match.

  The same value as selected for the Integrity algorithm, is used for the PRF (Pseudo-Random Function).

- **Diffie-Hellman group (PFS)**

  List box {None (legacy), Group 2 (MODP1024, legacy), Group 5 (MODP1536, legacy),

Group 14 (MODP2048), Group 15 (MODP3072), Group 25 (ECP192), Group 26 (ECP224),

Group 19 (ECP256), Group 20 (ECP384), Group 21 (ECP521), Group 27 (ECP224BP),

Group 28 (ECP256BP), Group 29 (ECP384BP), Group 30 (ECP512BP)}, 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 RipEX2 unit load is seriously affected when key exchange is in process. 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

- **SA lifetime [s]**

  Default = 3600 s (1 hour). Range [180 - 86400 s]

  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%, to prevent collision when the key exchange is triggered from both sides simultaneously.

  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.

- **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.

  - **Passphrase**

    The PSK key is entered as a password. Empty password is not allowed. It is possible to set 256 bits long Key instead of Passphrase in the ADVANCED / VPN / IPsec menu.

- **Traffic selector**

  "Traffic selector" defines which traffic is forwarded to the IPsec tunnel. The rule that defines this selection matches an incoming packet to "Local network ..." and "Remote network ..." address ranges.

- **Basic rules:**

  Each line contains the configuration settings of one CHILD SA and indicates its association to a specific IKE SA

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.

- **Local network address / Mask**

  Source IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

- **Remote network address / Mask**

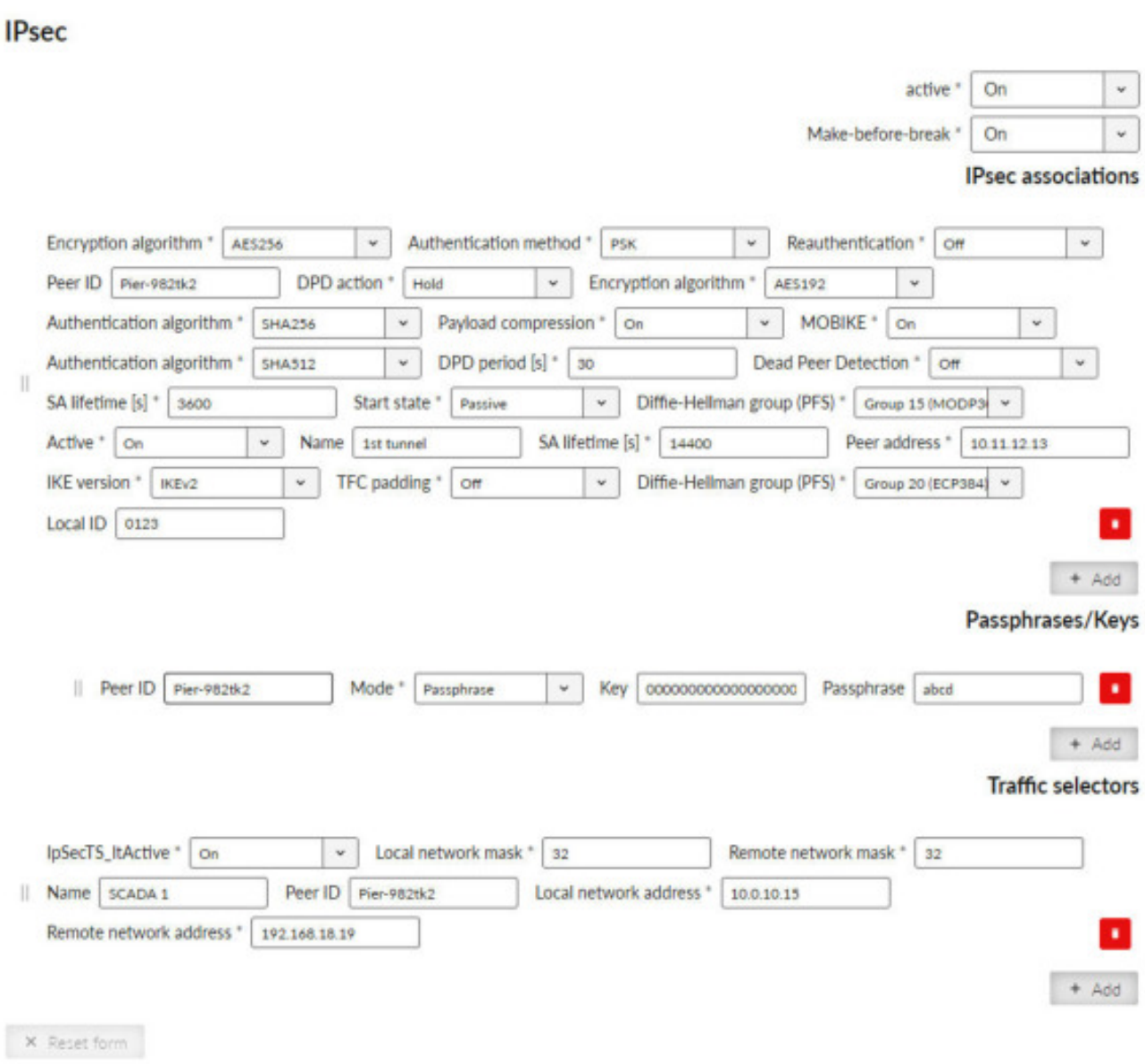
  Destination IP address and mask of the packets to be captured and forwarded to the encrypted tunnel.

- **Active** {On, Off }, default On

  Relevant CHILD SA can be enabled/disabled.

Advanced menu

Several additional parameters are available in menu: ADVANCED / VPN / IPsec



- **DPD check period [s]**

  Default = 30 s. Range [5 - 28800 s]

  Dead Peer Detection check period

- **Dead Peer Detection**

  List box {Clear, Hold, Restart}, default = Hold

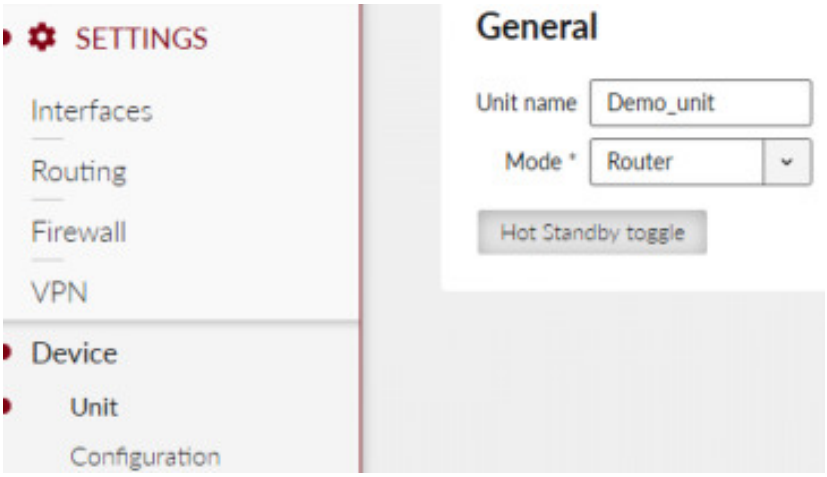
  One of three connection states automatically activated when connection loss is detected:

  - **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

7.5. Device

7.5.1. Unit

The general settings affecting the whole unit.



- **Unit name**

  This name is used as a real name of the Linux router, so the allowed characters are strictly limited to:

  _a..zA..Z0..9

- **Unit note**

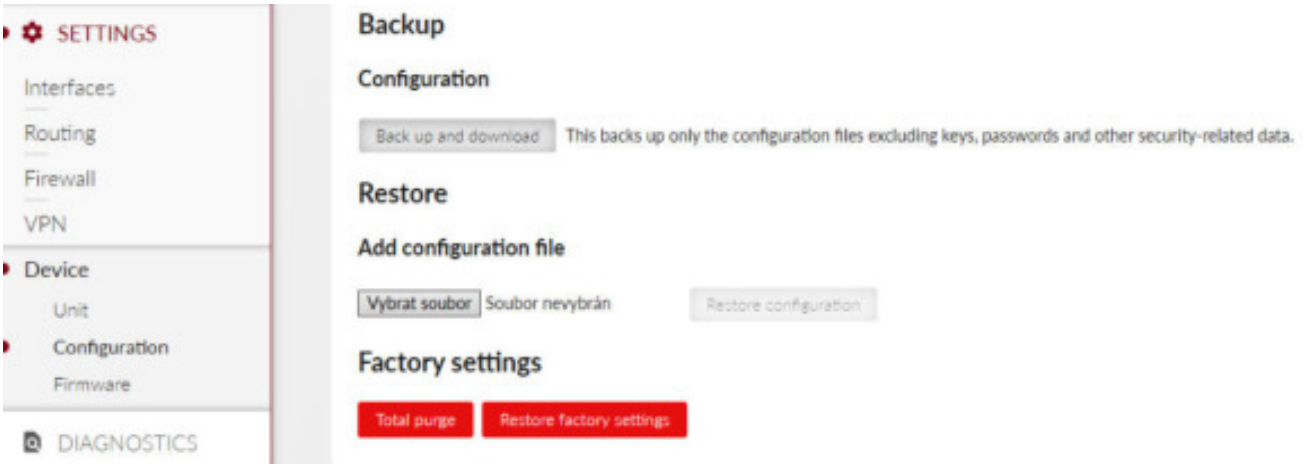
  Longer unit name without special characters restrictions.

- **Mode** list box (Bridge, Router)

  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.

7.5.2. Configuration

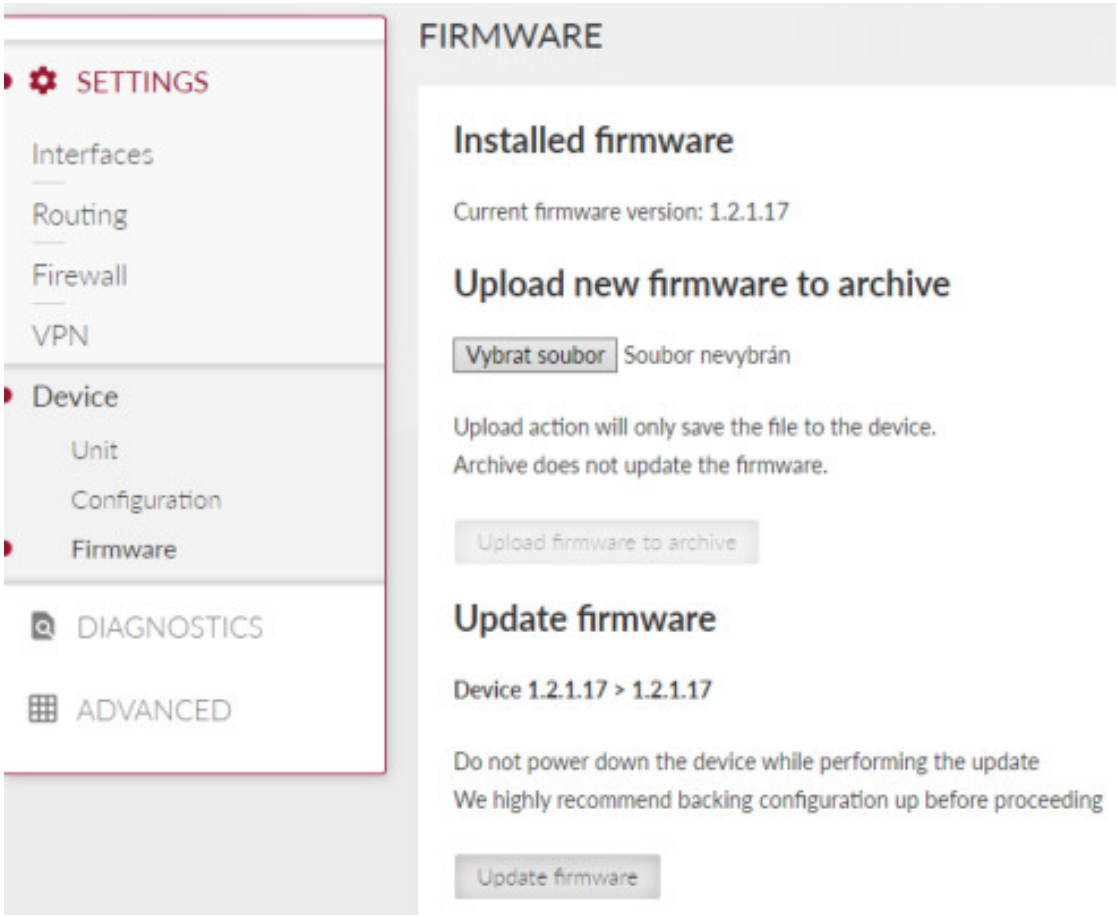
You can backup the actual unit configuration into a file or restore backed up configuration from the file.



7.5.3. Firmware

The firmware update has two phases:

- Upload new firmware into archive
- Update firmware from archive



Warning

Do not shut down the unit during the firmware update process.

8. Diagnostic

8.1. 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, ETHs, COMs, TSs), some internal interfaces between software modules can be monitored when such advanced diagnostics is needed.

Monitoring output can be viewed on-line or saved to a file in the RipEX2 (e.g. a remote RipEX2) and downloaded later on.

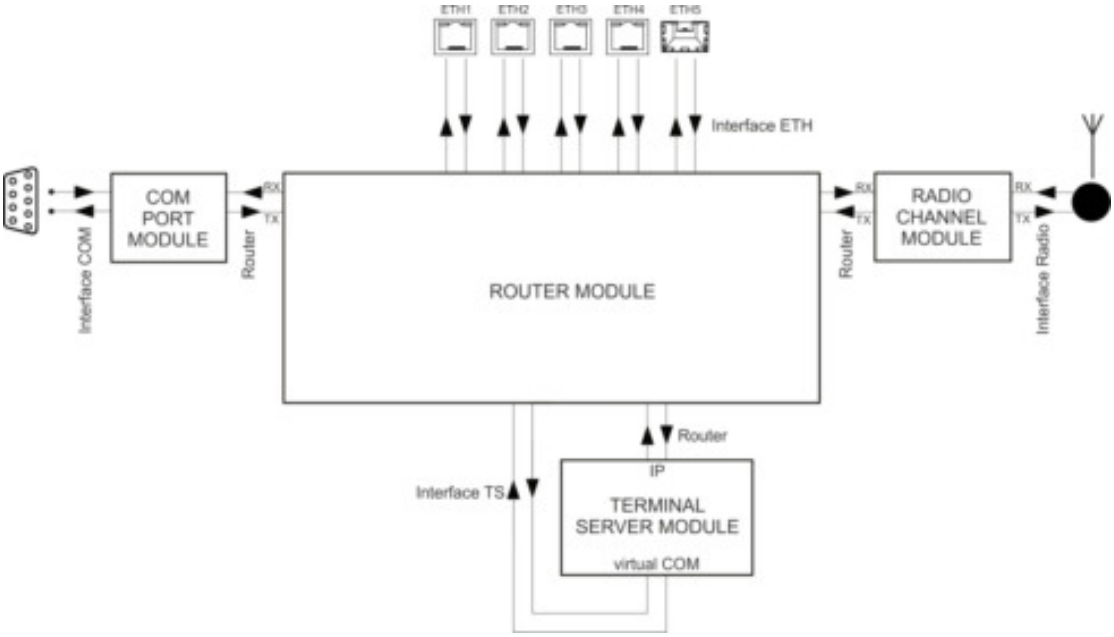
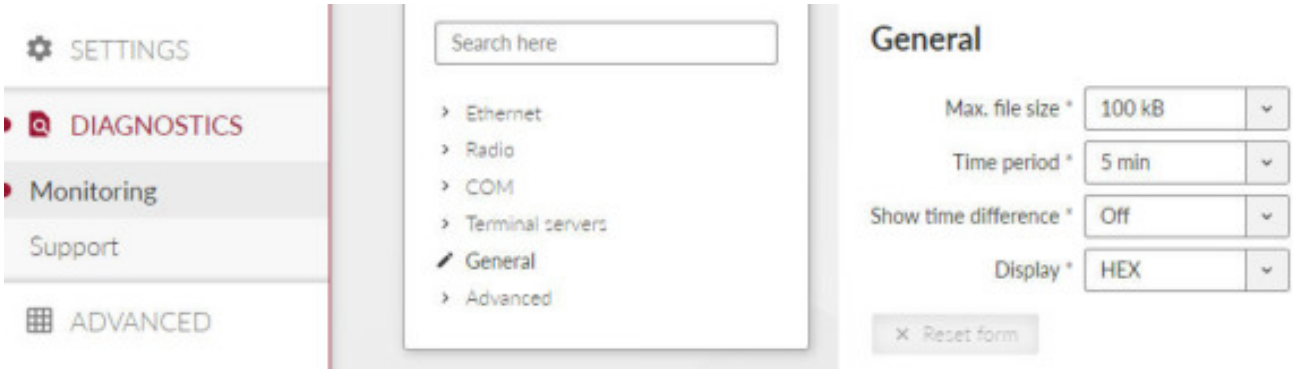


Fig. 8.1: Interfaces

8.1.1. Common parameters



- **Max. file size**

  List box {1 kB, 10 kB, 50 kB, 100 kB, 500 kB, 1 MB, max (~2 MB)}, default = 100 kB

When the selected "Time period" expires or the "Max. file size" has been reached, whichever event occurs first, the file is closed. The file can be downloaded later. Monitoring to the file will be implemented in future FW versions.

- **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

  Please, see **Max. file size** description above for more details.

- **Show time difference**

  List box {On, Off}, default = Off

  When On, the time difference between subsequent packets is displayed in the monitoring output.

- **Display**

  List box {HEX, HEX+ASCII, ASCII}, default = HEX

- **Show output** {On, Off}

  Enable/disable monitoring output on the local screen

- **Start monitoring** / **Stop monitoring** button

  Starts / Stops monitoring according to set parameters

- **Clear** button

  Clears local monitoring screen

8.1.2. Interfaces / Router

Common parameters for several interfaces:

- **Rx enabled, Tx enabled**

  List boxes {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 consult *Fig. 8.1, "Interfaces"* 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 = 100

  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**3798A285**93CD6B96

  Monitoring output: 3798A285

- **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) (to)**

  TCP/UDP source port to be enabled/disabled in the monitoring output. Use "... (to)" parameter to specify range of ports <from - to>.

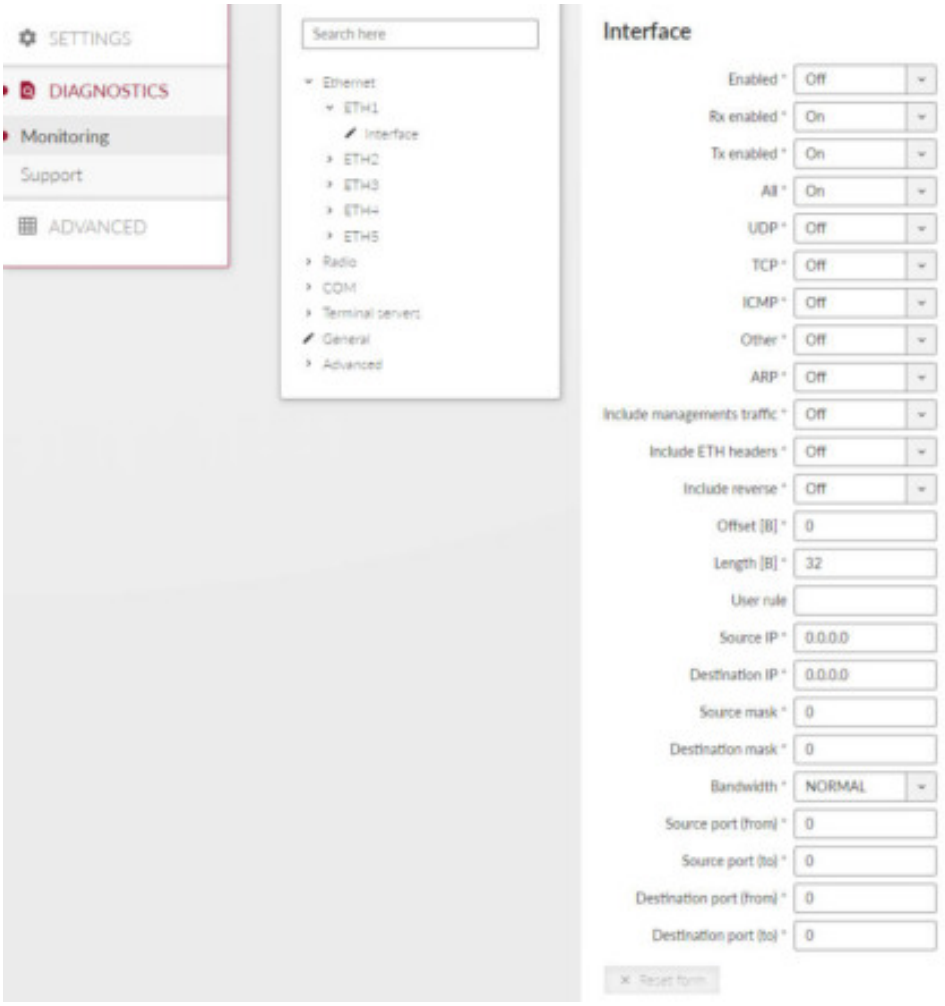
- **Destination port (from) (to)**

  TCP/UDP destination port to be enabled/disabled in the monitoring output. Use "... (to)" parameter to specify range of ports <from - to>.

- **Dropped frames**

  List box {On, Off}, default Off

  When On, monitoring shows packets which are dropped (e.g. CRC is not valid, buffer overflow, ...).



ETH interfaces

- **Include management traffic**

  List box {On, Off}, default = Off

  Enable/disable management packets monitoring output.

- **Include ETH headers**

  List box {On, Off}, default = Off

  Enable/disable ETH headers 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.

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**

  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.

- **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.

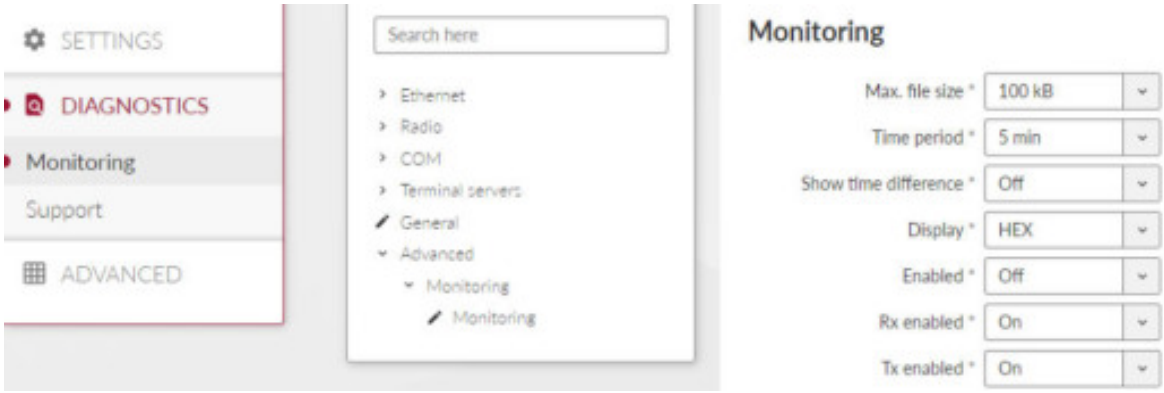
- **Source IP / mask, Destination IP / mask (router)**

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.

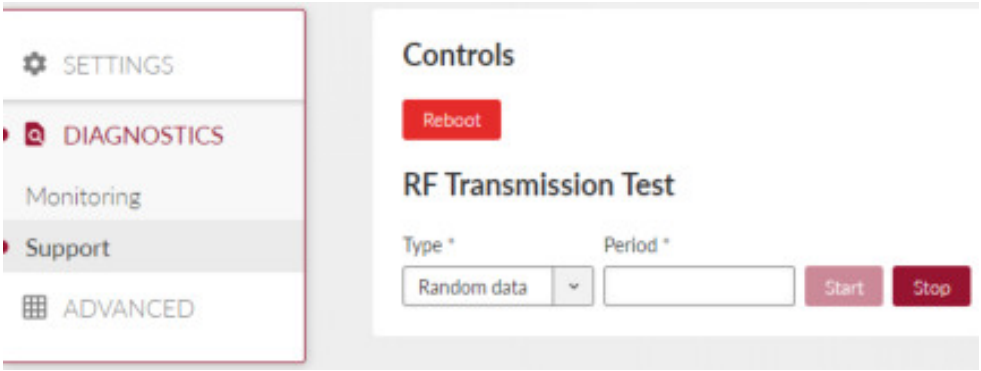
- **Source IP / mask, Destination IP / mask (radio)**

  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.

Menu DIAGNOSTICS/Monitoring/Advanced groups together all setting across all monitoring web pages, mentioned above, in one web page.



8.2. Support



- **Reboot** button

  RipEX2 unit can be rebooted on request.

- **RF Transmission Test**

  Pre-defined type of RF signal can be transmitted for a specific purpose.

- **Type**

  Listbox {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 from 1 to 1000 s

  Transmission test pre-set duration.

- **Start** button

  Starts the transmission test

- **Stop** button

  Allows to stop the test before the pre-set time.

9. Technical parameters

Tab. 9.1: Technical parameters

Radio parameters	
Frequency bands	135-175 MHz 335-400 MHz 400-470 MHz
Channel spacing	6.25 / 12.5 / 25 / 50 / 100 / 150 / 200 kHz (250, 300 kHz RED pending)
Frequency stability	±1.0 ppm, ±0.01 ppm with GPS option (pending)
Modulation	QAM: 256QAM, 64QAM, 16DEQAM, D8PSK, π/4DQPSK, DPSK FSK: 4CPFSK, 2CPFSK
FEC (Forward Error Correction)	2/3, 3/4, 5/6, Off. Trellis code with Viterbi soft-decoder
Transmitter	
RF Output power (Both Carrier and Modulated)	QAM: 0.1- 5.0 W (20 - 37 dBm) in 1dB step[1][2] FSK: 0.1 - 10 W (20 - 40 dBm) in 1 dB step
Duty cycle	Continuous
Rx to Tx Time	< 1.5 ms / 25 kHz channel
Intermodulation Attenuation	> 40 dB, > 70 dB (with external circulator/isolator)
Spurious Emissions (Conducted)	< -36 dBm
Radiated Spurious Emissions	< -36 dBm
Adjacent channel power	< -60 dBc
Transient adjacent channel power	< -60 dBc
Receiver	
Sensitivity	*see details*
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 kHz
Tx to Rx Time	< 1.5 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

[1] Output power displayed as average power, Max peak envelope power (PEP) 10 W (40 dBm)

[2] Modulation dependent (DPSK 5 W … QAM256 2 W)

Electrical		
Primary power	10 to 30 VDC, negative GND	
Rx	8 W / 13.8 V	
Tx - FSK	typ. 40 W, max. 55 W @ 40 dBm	
Tx - QAM	typ. 33 W, max. 40 W @ 40 dBm PEP	
Sleep mode	0.01 W	
Save mode	5 W	
Interfaces		
Ethernet	10/100/1000Base-T Auto MDI/MDIX 10/100/1000Base-T 1000Base-SX / 1000Base-LX user exchangeable SFP power consumption max. 1.25 W	4×RJ45, 1×SFP
COM	RS232/RS485 SW configurable	DB9F
	300 b/s – 1 Mb/s	
USB	USB 3.0	Host A
Antenna	50 Ω	2×TNC female
DI / DO	2×DI, 2×DO, 1×DDI, AO, AI, SI	RJ45

Optional interfaces	
GNSS (optional, pending)	active antenna 3.3 VDC SMA female
	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
Cellular interface (optional)	
Frequency bands E	4G LTE Band 20 (800 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
	Ublox TOBY L-210 FCC ID XPYTOBL210
Frequency bands P	4G LTE Band 28 (750 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz

	Ublox TOBY L-280 FCC ID XPYTOBL280
Frequency bands A	4G LTE Band 17 (700 MHz), Band 5 (850 MHz), Band 4 (1700 MHz), Band 2 (1900 MHz), Band 7 (2600 MHz)
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 4 (AWS, i.e. 1700 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
	Ublox TOBY L-200 FCC ID XPYTOBL200
Specification	4G LTE 3GPP Release 9 Long Term Evolution (LTE) Evolved Uni. Terrestrial Radio Access (E-UTRA) Frequency Division Duplex (FDD) DL Multi-Input Multi-Output (MIMO) 2×2
	3G UMTS/HSDPA/HSUPA 3GPP Release 8 Dual-Cell HS Packet Access (DC-HSPA+) UMTS Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD) DL Rx diversity
	2G GSM/GPRS/EDGE 3GPP Release 8 Enhanced Data rate GSM Evolution (EDGE) GSM EGPRS Radio Access (GERA) Time Division Multiple Access (TDMA) DL Advanced Rx Performance Phase 1
	Data rates up to 150 Mb/s downlink / 50 Mb/s uplink

LED panel	
5× tri-color status LEDs	SYS, AUX, RX, TX, COM
Environmental	
IP Code (Ingress Protection)	IP42, (IP52 - see *Section 4.1.3, “IP52 mounting”*)
MTBF (Mean Time Between Failure)	> 900.000 hours (> 100 years)
Operating temperature	-40 to +70 °C (-40 to +158 °F)
Operating humidity	5 to 95 % non-condensing
Storage	-40 to +85 °C (-40 to +185 °F) / 5 to 95 % non-condensing
Mechanical	
Casing	Rugged die-cast aluminium
Dimensions	H × W × D: 60 × 185 × 125 mm (2.34 × 7.2 × 4.9 in)
Weight	1.55 kg (3.4 lbs)
Mounting	DIN rail, L-bracket, Flat-bracket, 19" Rack chassis
SW	
Operating modes	Bridge / Router

User protocols on COM	Transparent, Async Link, DF1, DNP3, IEC101
User protocols on Ethernet	Modbus TCP, IEC104, DNP3 TCP, Comli TCP, Terminal server…
Serial to IP convertors	DNP3 / DNP3 TCP
Protocol on Radio channel	
Multi master applications	Yes
Report by exception	Yes
Collision Avoidance Capability	Yes
Remote to Remote communication	Yes
Addressed & acknowledged serial SCADA protocols	Yes
Radio channel data integrity	CRC 32
Radio channel Encryption	AES256-CCM
Diagnostic and Management	
SNMP	SNMPv1, SNMPv2c, SNMPv3 Trap / Inform alarms generation as per settings
Monitoring	Real time analysis of all physical interfaces (RADIO, ETH, COM) and some internal interfaces between software modules (e.g. Terminal servers)

Standards	
CE	RED, RoHS, WEEE
FCC, IC	pending: 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 V2.1.1 ETSI EN 301 489-5 V2.1.1 EN 61850-3:2014
Safety	EN 62 368-1:2004 + A1:2017
SAR	EN 50385:2017 EN 50383ed.2:2010
Electric power substations environment	IEEE 1613:2009 IEEE 1613.1:2013 EN 61850-3:2014
ATEX	pending
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

Tab. 9.2: 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
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
AUX (used for GPS)	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

9.1. Detailed Radio parameters

Tab. 9.3: 12.5 kHz

12.5 kHz Rx Baudrate 10.42 kBaud (ETSI EN 300 113)						
Classification			Sensitivity [dBm]			Co-Channel Rejection Ratio
Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	
3.91	3/4	2CPFSK	-120	-119	-117	-7
5.21	Off	2CPFSK	-120	-118	-115	-10
7.81	3/4	4CPFSK	-119	-117	-114	-11
10.42	Off	4CPFSK	-118	-115	-112	-6
7.81	3/4	DPSK	-119	-118	-114	-6.5
10.42	Off	DPSK	-119	-117	-112	-5
15.62	3/4	π/4-DQPSK	-118	-117	-113	-9
20.83	Off	π/4-DQPSK	-117	-115	-110	-10
23.44	3/4	D8PSK	-116	-113	-108	-12
31.25	Off	D8PSK	-113	-109	-103	-14
31.25	3/4	16DEQAM	-112	-109	-103	-16
41.67	Off	16DEQAM	-109	-106	-99	-18.5
41.67	2/3	64QAM	-112	-108	-101	-16
46.88	3/4	64QAM	-110	-106	-99	-19
52.08	5/6	64QAM	-109	-104	-97	-20
62.50	Off	64QAM	-105	-101	-94	-22.5
55.56	2/3	256QAM	-106	-103	-97	-21
62.50	3/4	256QAM	-105	-102	-95	-22
69.44	5/6	256QAM	-103	-100	-93	-24
83.33	Off	256QAM	-100	-97	-90	-28.5

12.5 kHz				
Bitrate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 5.21 kBaud (ETSI EN 300 113)				
5.21	2CPFSK	7K00F1DBN	7.0	11.5
10.42	4CPFSK	7K00F1DDN	7.0	11.5
Baudrate 8.68 kBaud (ETSI EN 300 113)				
8.68	DPSK	10K0G1DBN	10.0	11.5
17.36	π/4-DQPSK	10K0G1DDN	10.0	11.5
26.04	D8PSK	10K0G1DEN	10.0	11.5
34.72	16DEQAM	10K0G1DEN	10.0	11.5
52.08	64QAM	10K0G1DEN	10.0	11.5
69.44	256QAM	10K0G1DEN	10.0	11.5
Baudrate 10.42 kBaud (ETSI EN 300 113)				
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

Tab. 9.4: 25 kHz

25 kHz Rx Baudrate 20.83 (ETSI EN 300 113)						
Classification			**Sensitivity [dBm]**			**Co-Channel Rejection Ratio**
Bitrate [kb/s]	**FEC**	**Modulation**	**BER 10^{-2}**	**BER 10^{-3}**	**BER 10^{-6}**	
7.81	3/4	2CPFSK	-118	-117	-115	-6
10.42	Off	2CPFSK	-118	-116	-113	-7
15.63	3/4	4CPFSK	-117	-115	-112	-10
20.83	Off	4CPFSK	-115	-113	-109	-6
15.62	3/4	DPSK	-117	-116	-112	-6
20.83	Off	DPSK	-117	-115	-110	-6
31.25	3/4	π/4-DQPSK	-116	-115	-111	-9
41.66	Off	π/4-DQPSK	-115	-113	-108	-10
46.87	3/4	D8PSK	-113	-111	-106	-12
62.49	Off	D8PSK	-110	-107	-101	-14.5
62.49	3/4	16DEQAM	-110	-107	-101	-16
83.33	Off	16DEQAM	-108	-105	-98	-18.5
83.33	2/3	64QAM	-110	-106	-99	-16
93.75	3/4	64QAM	-108	-104	-97	-19
104.17	5/6	64QAM	-107	-102	-95	-20
125.00	Off	64QAM	-104	-99	-92	-22.5
111.11	2/3	256QAM	-104	-101	-95	-21
125.00	3/4	256QAM	-103	-100	-93	-22
138.89	5/6	256QAM	-101	-98	-91	-24
166.67	Off	256QAM	-98	-95	-88	-28.5

25 kHz				
Bitrate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 10.42 kBaud (ETSI EN 300 113)				
10.42	2CPFSK	13K8F1DBN	13.8	16
20.83	4CPFSK	13K8F1DDN	13.8	16
Baudrate 13.89 kBaud (ETSI EN 300 113)				
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 (ETSI EN 300 113, ETSI EN 302 561)				
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 (ETSI EN 302 561)				
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

Tab. 9.5: 50 kHz

50 kHz Rx Baudrate 41.67 kBaud (ETSI EN 300 561)						
Classification			Sensitivity [dBm]			Co-Channel Rejection Ratio
Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
31.25	3/4	DPSK	-114	-113	-109	-7
41.67	Off	DPSK	-114	-112	-107	-7
62.50	3/4	π/4-DQPSK	-113	-112	-108	-10
83.33	Off	π/4-DQPSK	-112	-110	-105	-11
93.75	3/4	D8PSK	-110	-108	-103	-13
125.00	Off	D8PSK	-107	-104	-98	-15
125.00	3/4	16DEQAM	-107	-104	-98	-17
166.67	Off	16DEQAM	-105	-102	-95	-19
166.67	2/3	64QAM	-107	-103	-96	-17
187.50	3/4	64QAM	-105	-101	-94	-20
108.33	5/6	64QAM	-104	-99	-92	-21
250.00	Off	64QAM	-101	-96	-89	-23
222.22	2/3	256QAM	-101	-98	-92	-22
250.00	3/4	256QAM	-100	-97	-90	-23
277.78	5/6	256QAM	-98	-95	-88	-25
333.33	Off	256QAM	-95	-92	-85	-31

50 kHz				
Bitrate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 34.72 kBaud (ETSI EN 302 561)				
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 (ETSI EN 302 561)				
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

Tab. 9.6: 100 kHz

100 kHz Rx Baudrate 69.44 kBaud (ETSI EN 300 561)						
Classification			Sensitivity [dBm]			Co-Channel Rejection Ratio
Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
52.08	3/4	DPSK	-112	-110	-106	-7
69.44	Off	DPSK	-111	-109	-104	-7
104.17	3/4	π/4-DQPSK	-111	-109	-105	-10
138.89	Off	π/4-DQPSK	-110	-108	-102	-11
156.25	3/4	D8PSK	-108	-105	-100	-13
208.33	Off	D8PSK	-105	-101	-95	-15
208.33	3/4	16DEQAM	-104	-101	-95	-17
277.78	Off	16DEQAM	-102	-99	-92	-19
277.78	2/3	64QAM	-104	-100	-93	-17
312.50	3/4	64QAM	-102	-98	-91	-20
347.22	5/6	64QAM	-101	-96	-89	-21
416.66	Off	64QAM	-98	-93	-86	-23
370.37	2/3	256QAM	-99	-95	-89	-22
416.66	3/4	256QAM	-98	-94	-86	-23
462.96	5/6	256QAM	-96	-92	-85	-25
555.55	Off	256QAM	-93	-89	-83	-31

100 kHz				
Bitrate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 69.44 kBaud (ETSI EN 302 561)				
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

Tab. 9.7: 150 kHz

150 kHz Rx Baudrate 115.74 kBaud (ETSI EN 300 561)						
Classification			**Sensitivity [dBm]**			**Co-Channel Rejection Ratio**
Bitrate [kb/s]	**FEC**	**Modulation**	**BER 10^{-2}**	**BER 10^{-3}**	**BER 10^{-6}**	**[dB]**
86.71	3/4	DPSK	-110	-108	-104	-7
115.74	Off	DPSK	-109	-107	-102	-7
173.61	3/4	π/4-DQPSK	-109	-107	-103	-10
231.48	Off	π/4-DQPSK	-108	-106	-100	-11
260.42	3/4	D8PSK	-106	-103	-98	-13
347.22	Off	D8PSK	-103	-99	-93	-15
347.22	3/4	16DEQAM	-102	-99	-93	-17
462.96	Off	16DEQAM	-100	-97	-90	-19
462.96	2/3	64QAM	-102	-98	-91	-17
520.83	3/4	64QAM	-100	-96	-89	-20
587.71	5/6	64QAM	-99	-94	-87	-21
694.45	Off	64QAM	-96	-91	-84	-23
617.29	2/3	256QAM	-97	-93	-87	-22
694.45	3/4	256QAM	-96	-92	-84	-23
771.61	5/6	256QAM	-94	-90	-83	-25
925.93	Off	256QAM	-91	-87	-81	-31

150 kHz				
Bitrate [kb/s]	**Modulation**	**Emission code**	**OBW [kHz]**	**OBW limit [kHz]**
Baudrate 115.74 kBaud (ETSI EN 302 561)				
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

Tab. 9.8: 200 kHz

200 kHz Rx Baudrate 138.89 kBaud (ETSI EN 300 561)						
Classification			Sensitivity [dBm]			Co-Channel Rejection Ratio
Bitrate [kb/s]	FEC	Modulation	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	[dB]
104.17	3/4	DPSK	-109	-107	-103	-7
138.89	Off	DPSK	-108	-106	-101	-7
208.33	3/4	π/4-DQPSK	-108	-106	-102	-10
277.78	Off	π/4-DQPSK	-107	-105	-99	-11
312.50	3/4	D8PSK	-105	-102	-97	-13
416.67	Off	D8PSK	-102	-98	-92	-15
416.67	3/4	16DEQAM	-101	-98	-92	-17
555.55	Off	16DEQAM	-99	-96	-89	-19
555.55	2/3	64QAM	-101	-97	-90	-17
625.00	3/4	64QAM	-99	-95	-88	-20
694.45	5/6	64QAM	-98	-93	-86	-21
833.33	Off	64QAM	-95	-90	-83	-23
740.74	2/3	256QAM	-96	-92	-86	-22
833.33	3/4	256QAM	-95	-91	-83	-23
925.93	5/6	256QAM	-93	-89	-82	-25
1111.11	Off	256QAM	-90	-86	-80	-31

200 kHz				
Bitrate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 138.89 kBaud (ETSI EN 302 561)				
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

Tab. 9.9: 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

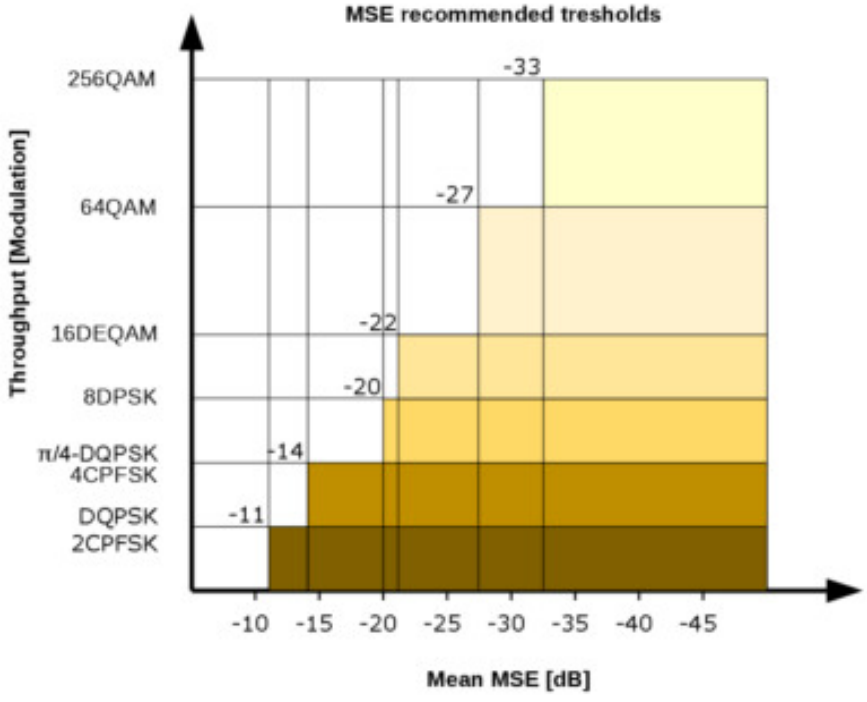


Fig. 9.1: MSE recommended tresholds

Tab. 9.10: Maximal power for individual modulations

Maximum PEP, RMS and PAPR levels			
Modulation	**PEP Peak Envelope Power [dBm]**	**RMS Average Power [dBm]**	**PAPR Peak to Average Power Ratio [dB]**
2CPFSK	40	40	0
4CPFSK	40	40	0
DPSK	40	37	3
π/4-DQPSK	40	37	3
D8PSK	40	36	4
16DEQAM	40	35	5
64QAM	40	34	6
256QAM	40	33	7

9.2. Occupied Bandwidth limits overview

Tab. 9.11: 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
OBW [kHz]	3.6	5.0
Baud rate [kBaud]	2.6	4.34
Compliance	FCC Part 90	FCC Part 90

Tab. 9.12: 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
OBW [kHz]	7.0	10.0	11.9
Baud rate [kBaud]	5.21	8.68	10.42
Compliance	RED FCC Part 90	RED FCC Part 90	RED

Tab. 9.13: Channel spacing 25 kHz

Channel spacing [kHz]	**25**			
Occupied BW limit [kHz]	**16**	**16**	**20**	**25**
Modulation type	**FSK**	**QAM**		
RipEX 1 "Mode"	CE	Narrow	FCC	CE
OBW [kHz]	13.8	15.9	19.8	24.0
Baud rate [kBaud]	10.42	13.89	17.36	20.83
Compliance	RED FCC Part 90	RED FCC Part 90	RED FCC Part 90	RED

Tab. 9.14: Channel spacing 50 kHz

Channel spacing [kHz]	**50**	
Occupied BW limit [kHz]	**40**	**50**
Modulation type	**QAM**	
RipEX 1 "Mode"	CE	Unlimited
OBW [kHz]	40.0	45.0
Baud rate [kBaud]	34.72	41.67
Compliance	RED	RED

Tab. 9.15: Channel spacing 100 kHz

Channel spacing [kHz]	**100**	
Occupied BW limit [kHz]	**80**	**100**
Modulation type	**QAM**	
OBW [kHz]	80.0	90.0
Baud rate [kBaud]	69.44	83.3
Compliance	RED	

Tab. 9.16: Channel spacing 150 kHz

Channel spacing [kHz]	**150**	
Occupied BW limit [kHz]	**125**	**150**
Modulation type	**QAM**	
OBW [kHz]	125	135
Baud rate [kBaud]	115.74	124.01
Compliance	RED	

Tab. 9.17: Channel spacing 200 kHz

Channel spacing [kHz]	**200**	
Occupied BW limit [kHz]	**175**	**200**
Modulation type	**QAM**	
OBW [kHz]	150	180
Baud rate [kBaud]	138.89	166.67
Compliance	RED	

Tab. 9.18: Channel spacing 250 kHz

Channel spacing [kHz]	**250**	
Occupied BW limit [kHz]	**225**	**250**
Modulation type	**QAM**	
OBW [kHz]	205	225
Baud rate [kBaud]	189.39	208.33

Tab. 9.19: Channel spacing 300 kHz

Channel spacing [kHz]	**300**
Occupied BW limit [kHz]	**300**
Modulation type	**QAM**
OBW [kHz]	280
Baud rate [kBaud]	260.42

10. Safety, environment, licensing

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.

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 table below when the transmitter is operating. More information on RF exposure can be found online at the following website:

www.fcc.gov/oet/info/documents/bulletins[1]

Concentré d'énergie à partir d'une antenne directionnelle peut poser un risque pour la santé humaine. Ne pas permettre aux gens de se rapprocher de l'antenne que les distances indiquées dans le tableau ci-dessous lorsque l'émetteur est en marche. Plus d'informations sur l'exposition aux RF peut être trouvé en ligne à l'adresse suivante:

www.fcc.gov/oet/info/documents/bulletins[2]

Tab. 10.1: Minimum Safety Distance

10 W RF power				
Antenna	Gain G [dBi]	Gain G [–]	Dist. where the FCC limits are met for	
			General Population / Uncontrolled Exposure [cm]	General Population / Controlled Exposure [cm]
single dipole	4.6	2.9	130	60
stacked double dipole	7.6	5.8	180	80
3 element directional Yagi	7.6	5.8	180	80
5 element directional Yagi	8.7	7.4	200	90
9 element directional Yagi	12.5	17.8	310	140

[1] http://www.fcc.gov/oet/info/documents/bulletins
[2] http://www.fcc.gov/oet/info/documents/bulletins

5 W RF power				
Antenna	Gain G [dBi]	Gain G [–]	Dist. where the FCC limits are met for	
			General Population / Uncontrolled Exposure [cm]	Occupational / Controlled Exposure [cm]
single dipole	4.6	2.9	90	40
stacked double dipole	7.6	5.8	130	60
3 element directional Yagi	7.6	5.8	130	60
5 element directional Yagi	8.7	7.4	140	70
9 element directional Yagi	12.5	17.8	220	100

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. RoHS and WEEE compliance

RoHS compliant

WEEE compliant

This product is fully compliant with the European Parlament's 2011/65/EU RoHS (Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment) and 2012/19/EU WEEE (Waste Electrical and Electronic Equipment) environmental directives.

Used equipment must be collected separately, and disposed of properly. RACOM has instigated a programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive.

Battery Disposal - This product may contain a battery. Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste within the European Union. See the product documentation for specific battery information. Batteries are marked with a symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point.

RACOM
www.racom.eu

EU DECLARATION OF CONFORMITY

Equipment	RipEX, RipEX2 RAy2, RAy3 M!DGE, M!DGE2 MRxxx, MDxxx
Manufacturer	RACOM s.r.o. Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic

This declaration of conformity is issued under the sole responsibility of the manufacturer.

The equipment described above is in conformity with the Directive 2011/65/EU of the European Parliament and of the Council on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS), as amended by Directive (EU) 2015/863, and Directive 2012/19/EU of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE).

RoHS Applicable Exemption: 7(b)

Compliance has been verified via internal design controls, supplier declarations and/or analytical test data.

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 11th July 2019
Jiri Hruska, CEO

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

ver. 1.0

Fig. 10.1: EU Declaration of Conformity RoHS, WEEE

10.5. 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.

10.6. Important Notifications

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.

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.

The maker does not provide the user with any kind of guarantee containing assurance of suitability and usability for his application. Products are not developed, designed nor tested for utilization in devices directly affecting health and life functions of persons and animals, nor as a part of another important device, and no guarantees apply if the company product has been used in these aforementioned devices.

RACOM Open Software License

Version 1.0, November 2009

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.

10.7. EU restrictions or requirements notice

Radio equipment used within the EU countries listed bellow:

* there are restrictions on putting into service or

* any requirements for authorisation of use.

Radio equipment used within the EU countries listed bellow:

- 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. 10.2: EU restrictions or requirements

The RipEX 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. EU Declaration of Conformity

RACOM
www.racom.eu

EU DECLARATION OF CONFORMITY

Radio equipment type	**Radio modem** **RipEX2-4**	**Radio SW version** **1.0.0**
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 V2.1.1
	EN 301 489-4 V2.2.1
Safety	EN 62368-1:2014 + A11:2017
SAR	EN 50385:2017
	EN 50383ed.2:2010

Signed for and on behalf of the manufacturer:

Nove Mesto na Morave, 22nd of May 2019
Jiri Hruska, CEO

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

ver. 1.0

Fig. 10.3: EU Declaration of Conformity RED

10.9. Simplified EU declaration of conformity

BG
С настоящото RACOM s.r.o. декларира, че този тип радиосъоръжение RipEX2 е в съответствие с Директива 2014/53/ЕС.

ES
Por la presente, RACOM s.r.o. declara que el tipo de equipo radioeléctrico RipEX2 es conforme con la Directiva 2014/53/UE.

CS
Tímto RACOM s.r.o. prohlašuje, že typ rádiového zařízení RipEX2 je v souladu se směrnicí 2014/53/EU.

DA
Hermed erklærer RACOM s.r.o., at radioudstyrstypen RipEX2 er i overensstemmelse med direktiv 2014/53/EU.

DE
Hiermit erklärt RACOM s.r.o., dass der Funkanlagentyp RipEX2 der Richtlinie 2014/53/EU entspricht.

ET
Käesolevaga deklareerib RACOM s.r.o., et käesolev raadioseadme tüüp RipEX2 vastab direktiivi 2014/53/EL nõuetele.

EL
Με την παρούσα ο/η RACOM s.r.o., δηλώνει ότι ο ραδιοεξοπλισμός RipEX2 πληροί την οδηγία 2014/53/ΕΕ.

EN
Hereby, RACOM s.r.o. declares that the radio equipment type RipEX2 is in compliance with Directive 2014/53/EU.

FR
Le soussigné, RACOM s.r.o., déclare que l'équipement radioélectrique du type RipEX2 est conforme à la directive 2014/53/UE.

HR
RACOM s.r.o. ovime izjavljuje da je radijska oprema tipa RipEX2 u skladu s Direktivom 2014/53/EU.

IT
Il fabbricante, RACOM s.r.o., dichiara che il tipo di apparecchiatura radio RipEX2 è conforme alla direttiva 2014/53/UE.

LV
Ar šo RACOM s.r.o. deklarē, ka radioiekārta RipEX2 atbilst Direktīvai 2014/53/ES.

LT
Aš, RACOM s.r.o., patvirtinu, kad radijo įrenginių tipas RipEX2 atitinka Direktyvą 2014/53/ES.

HU
RACOM s.r.o. igazolja, hogy a RipEX2 típusú rádióberendezés megfelel a 2014/53/EU irányelvnek.

MT
B'dan, RACOM s.r.o., niddikjara li dan it-tip ta' tagħmir tar-radju RipEX2 huwa konformi mad-Direttiva 2014/53/UE.

NL
Hierbij verklaar ik, RACOM s.r.o., dat het type radioapparatuur RipEX2 conform is met Richtlijn 2014/53/EU.

PL
RACOM s.r.o. niniejszym oświadcza, że typ urządzenia radiowego RipEX2 jest zgodny z dyrektywą 2014/53/UE.

PT
O(a) abaixo assinado(a) RACOM s.r.o. declara que o presente tipo de equipamento de rádio RipEX2 está em conformidade com a Diretiva 2014/53/UE.

RO
Prin prezenta, RACOM s.r.o. declară că tipul de echipamente radio RipEX2 este în conformitate cu Directiva 2014/53/UE.

SK
RACOM s.r.o. týmto vyhlasuje, že rádiové zariadenie typu RipEX2 je v súlade so smernicou 2014/53/EÚ.

SL
RACOM s.r.o. potrjuje, da je tip radijske opreme RipEX2 skladen z Direktivo 2014/53/EU.

FI
RACOM s.r.o. vakuuttaa, että radiolaitetyyppi RipEX2 on direktiivin 2014/53/EU mukainen.

SV
Härmed försäkrar RACOM s.r.o. att denna typ av radioutrustning RipEX2 överensstämmer med direktiv 2014/53/EU.

10.10. 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”

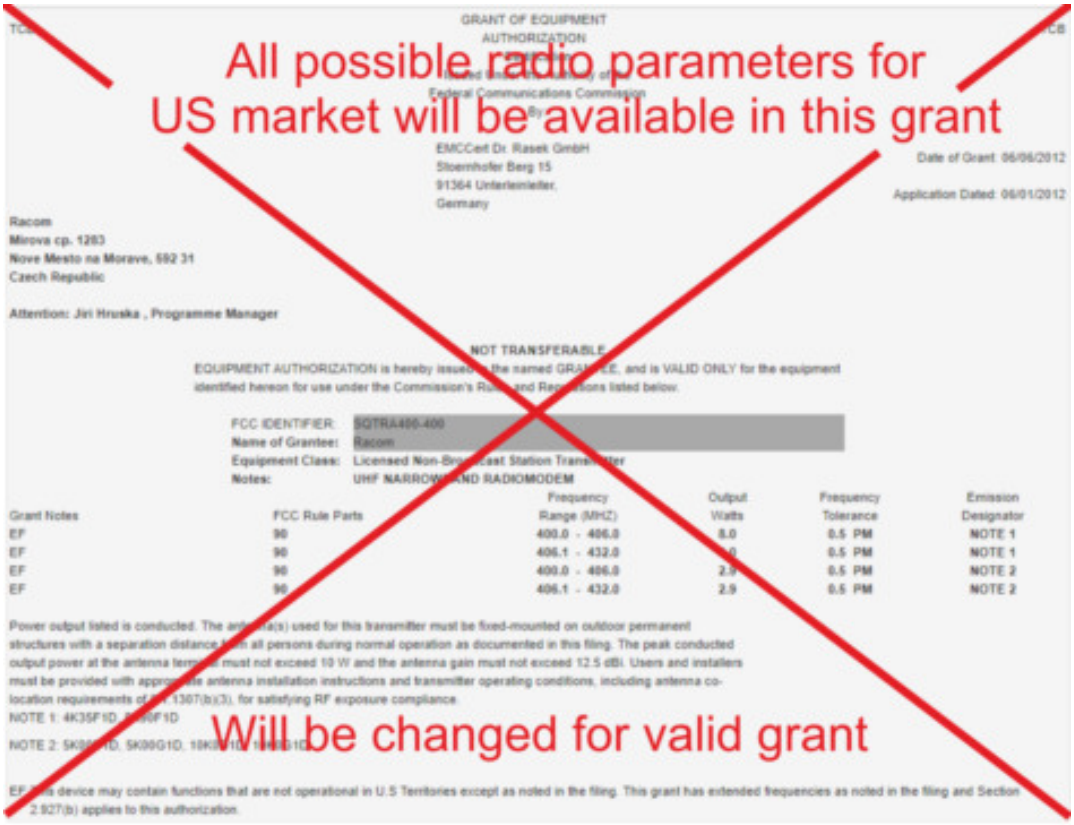
Tab. 10.2: Compliance FCC

Code	FCC part	FCC ID	ISED	IC number
RipEX2-1A	90	pending	RSS-102	pending
RipEX2-3A	90	pending	RSS-102	pending
RipEX2-3B	90	pending	RSS-102	pending
RipEX2-4A	90	SQT-RIPEX2-4A pending	RSS-102	pending

Possible values for channels, channel spacing and occupied bandwidth fulfilling FCC rules are shown in *Section 9.2, “Occupied Bandwidth limits overview”*.

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.



GRANT OF EQUIPMENT AUTHORIZATION

Federal Communications Commission

EMCCert Dr. Rasek GmbH
Stoernhofer Berg 15
91364 Unterleinleiter,
Germany

Date of Grant: 06/06/2012

Application Dated: 06/01/2012

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: SQTRA400-400
Name of Grantee: Racom
Equipment Class: Licensed Non-Broadcast Station Transmitter
Notes: UHF NARROWBAND RADIOMODEM

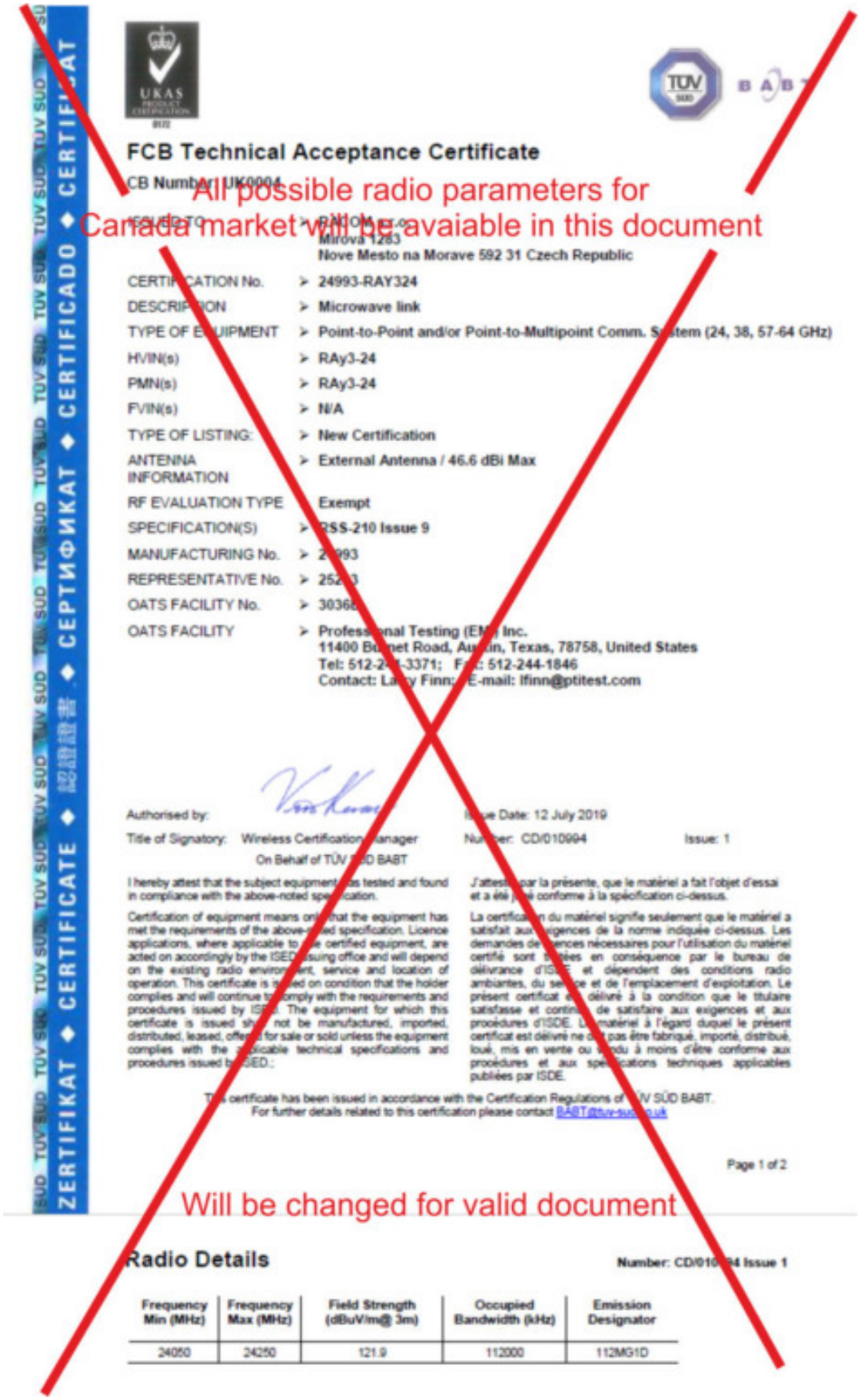
Grant Notes	FCC Rule Parts	Frequency Range (MHZ)	Output Watts	Frequency Tolerance	Emission Designator
EF	90	400.0 - 406.0	8.0	0.5 PM	NOTE 1
EF	90	406.1 - 432.0	8.0	0.5 PM	NOTE 1
EF	90	400.0 - 406.0	2.9	0.5 PM	NOTE 2
EF	90	406.1 - 432.0	2.9	0.5 PM	NOTE 2

Power output listed is conducted. The antenna(s) used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance from all persons during normal operation as documented in this filing. The peak conducted output power at the antenna terminal must not exceed 10 W and the antenna gain must not exceed 12.5 dBi. Users and installers must be provided with appropriate antenna installation instructions and transmitter operating conditions, including antenna co-location requirements of 47 CFR 1307(b)(3), for satisfying RF exposure compliance.

NOTE 1: 4K35F1D, 8K00F1D

NOTE 2: 5K80G1D, 5K00G1D, 10K0G1D, 19K0G1D

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.



All possible radio parameters for Canada market will be avaiable in this document

FCB Technical Acceptance Certificate

CB Number: UK0004

Will be changed for valid document

Radio Details

Frequency Min (MHz)	Frequency Max (MHz)	Field Strength (dBuV/m@ 3m)	Occupied Bandwidth (kHz)	Emission Designator
24050	24250	121.9	112000	112MG1D

10.11. 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. 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 DQ values as a preventive measure against the failure of the connection. RSS and DQ values be similar to those at time of comissioning.	Monthly	
Check activity logs to detect abnormalities in data transmissions	Monthly	
Check if internal temperature alarm has been triggered	Monthly	
Check that firmware is latest stable version – upgrading FW recommended when new features required	As required	

If you are unsure on any of the above please contact RACOM technical support.

Appendix A. Abbreviations

ACK	Acknowledgement
AES	Advanced Encryption Standard
BER	Bit Error Rate
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
CTS	Clear To Send
dBc	decibel relative to the carrier
dBi	decibel relative to the isotropic
dBm	decibel relative to the milliwat
DCE	Data Communication Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DQ	Data Quality
DTE	Data Terminal Equipment
EMC	Electro-Magnetic Compatibility
FCC	Federal Communications Commission
FEC	Forward Error Correction
FEP	Front End Processor
GPL	General Public License
https	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LAN	Local Area Network
LOS	Line-of-sight
MAC	Media Access Control
MDIX	Medium dependent interface crossover
MIB	Management Information Base
NMS	Network Management System
N.C.	Normally Closed
N.O.	Normally Open
NTP	Network Time Protocol
MRU	Maximum Reception Unit
MTU	Maximum Transmission Unit
OS	Operation System
PC	Personal Computer
PER	Packet Error Rate
PWR	Power
RF	Radio Frequency
RoHS	Restriction of the use of Hazardeous Substances
RPT	Repeater
RSS	Received Signal Strength
RTS	Request To Send
RTU	Remote Terminal Unit
RX	Receiver
SCADA	Supervisory control and data acquisition
SDR	Software Defined Radio
SNMP	Simple Network Management Protocol

TCP	Transmission Control Protocol
TS5	Terminal server 5
TX	Transmitter
UDP	User Datagram Protocol
VSWR	Voltage Standing Wave Ratio
WEEE	Waste Electrical and Electronic Equipment

Index

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.