

User manual



RipEX2 Radio modem & Router

fw 2.0.3.0
2021-05-18
version 1.12

Quick start



Hardware



Configuration



Parameters



Table of Contents

Important Notice	7
1. Quick guide	8
1.1. Bench testing	9
2. Product	11
2.1. Dimensions	12
2.2. Connectors	15
2.3. Indication LEDs	22
2.4. Ordering codes	24
3. Accessories	27
4. Installation	28
4.1. Mounting	29
4.2. Antenna installation	33
4.3. Antenna feed line	34
4.4. Grounding	34
4.5. Connectors	34
4.6. Power supply	34
5. RipEX2 in detail	36
5.1. Bridge mode	36
5.1.1. Functionality example	37
5.1.2. Configuration examples	39
5.2. Router mode	40
5.2.1. Router - Base driven	40
5.2.2. Router - Flexible	43
5.3. Combination of IP and serial communication	47
5.3.1. Detailed Description	47
6. Web interface	49
6.1. Supported web browsers	51
6.2. Changes to commit	51
6.3. Notifications	52
6.4. User menu	53
6.5. Help	53
6.6. Remote access	54
7. Settings	56
7.1. Interfaces	56
7.1.1. Ethernet	56
7.1.2. Radio	58
7.1.2.1. Radio channel parameters	59
7.1.2.2. Transparent protocol (Bridge mode)	61
7.1.2.3. Base driven protocol (Router mode)	62
7.1.2.3.1. Radio protocol - Base station	63
7.1.2.3.2. Base station - List of Remote stations	63
7.1.2.3.3. Radio protocol - Remote station	64
7.1.2.4. Flexible Protocol (router mode)	64
7.1.2.5. Advanced radio parameters	65
7.1.2.5.1. Radio parameters - advanced	65
7.1.2.5.2. Queues	66
7.1.2.5.3. Flexible - advanced	67
7.1.3. COM	67
7.1.3.1. COM port parameters	67
7.1.3.2. Common Protocol parameters	69
7.1.3.3. Individual protocol parameters	72

7.1.3.3.1. None	72
7.1.3.3.2. Transparent protocol	72
7.1.3.3.3. Async link	72
7.1.3.3.4. DNP3	73
7.1.3.3.5. DF1	74
7.1.3.3.6. IEC101	75
7.1.3.3.7. Modbus RTU	75
7.1.3.3.8. PR2000	76
7.1.3.3.9. Siemens 3964(R)	76
7.1.3.3.10. RDS	79
7.1.3.3.11. UNI	80
7.1.4. Terminal servers	82
7.1.5. Cellular	83
7.2. Routing	86
7.2.1. Static	86
7.2.2. OSPF	88
7.2.2.1. Description	88
7.2.2.2. Common - Common settings	89
7.2.2.3. Network - Areas and interfaces - Areas	89
7.2.2.4. Network - Areas and interfaces - Interfaces	90
7.2.2.5. Network - Areas and interfaces - Neighbors	91
7.2.2.6. Network - Areas and interfaces - Networks	92
7.2.2.7. Static rules	92
7.2.2.8. Import filter	93
7.2.2.9. Export filter	94
7.2.3. BGP	95
7.2.3.1. Description	95
7.2.3.2. Common - Common settings	96
7.2.3.3. Neighbors	97
7.2.3.4. Static rules	99
7.2.3.5. Import IGP filter	99
7.2.3.6. Export IGP filter	100
7.2.3.7. Import OUT rules	101
7.2.3.8. Export OUT filter	103
7.3. Firewall	104
7.3.1. Firewall L2	104
7.3.2. Firewall L3	105
7.4. VPN	106
7.4.1. IPsec	106
7.4.1.1. Advanced menu	113
7.4.2. GRE L2	114
7.4.3. GRE L3	115
7.5. Security	116
7.5.1. Local authentication	117
7.5.2. Remote authentication	119
7.6. Device	119
7.6.1. Unit	119
7.6.1.1. General	119
7.6.1.2. Service USB	119
7.6.1.3. Time	121
7.6.1.4. Hot standby	123
7.6.1.4.1. Hot standby settings	123

7.6.1.4.2. Hot standby LAN interface settings	125
7.6.2. Configuration	126
7.6.3. Events	127
7.6.4. SNMP	127
7.6.5. SW keys	130
7.6.6. Firmware	131
7.7. Advanced	132
8. Diagnostics	135
8.1. Overview	135
8.2. Events	135
8.3. Statistics	136
8.4. Monitoring	142
8.5. Tools	149
8.6. Support	149
8.7. Syslog	150
9. Technical parameters	151
9.1. Detailed radio channel parameters	160
9.2. Recommended MSE thresholds	176
10. Safety, regulations, warranty	177
10.1. Frequency	177
10.2. Safety distance	177
10.3. High temperature	178
10.4. Battery disposal	178
10.5. Instructions for Safe Operation of Equipment	178
10.6. SW license	179
10.7. EU Compliance	180
10.7.1. RoHS, WEEE and WFD	180
10.7.2. EU restrictions or requirements notice	181
10.7.3. EU Declaration of Conformity RED	182
10.7.4. Simplified EU declaration of conformity	182
10.8. Compliance Federal Communications Commission and Innovation, Science and Eco- nomic Development Canada	184
10.9. Compliance ANATEL Brasil	189
10.10. Warranty	189
10.11. RipEX2 Availability and service life time	189
10.12. RipEX2 maintenance	189
A. Abbreviations	191
Index	193
Revision History	195

Important Notice

Copyright

© 2021 RACOM. All rights reserved.

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

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

Disclaimer

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

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

Trademark

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

Important Notice

- Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e. have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the RipEX2 are used in an appropriate manner within a well-constructed network. RipEX2 should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. RACOM accepts no liability for damages of any kind resulting from delays or errors in data transmitted or received using RipEX2, or for the failure of RipEX2 to transmit or receive such data.
- Under no circumstances is RACOM or any other company or person responsible for incidental, accidental or related damage arising as a result of the use of this product. RACOM does not provide the user with any form of guarantee containing assurance of the suitability and applicability for its application.
- RACOM products are not developed, designed or tested for use in applications which may directly affect health and/or life functions of humans or animals, nor to be a component of similarly important systems, and RACOM does not provide any guarantee when company products are used in such applications.

1. Quick guide

RipEX2 is a widely configurable compact radio modem, more precisely a radio IP router. All you have to do to put it into operation is to connect it to an antenna and a power supply and configure it using a PC (tablet, smartphone) and a web browser.

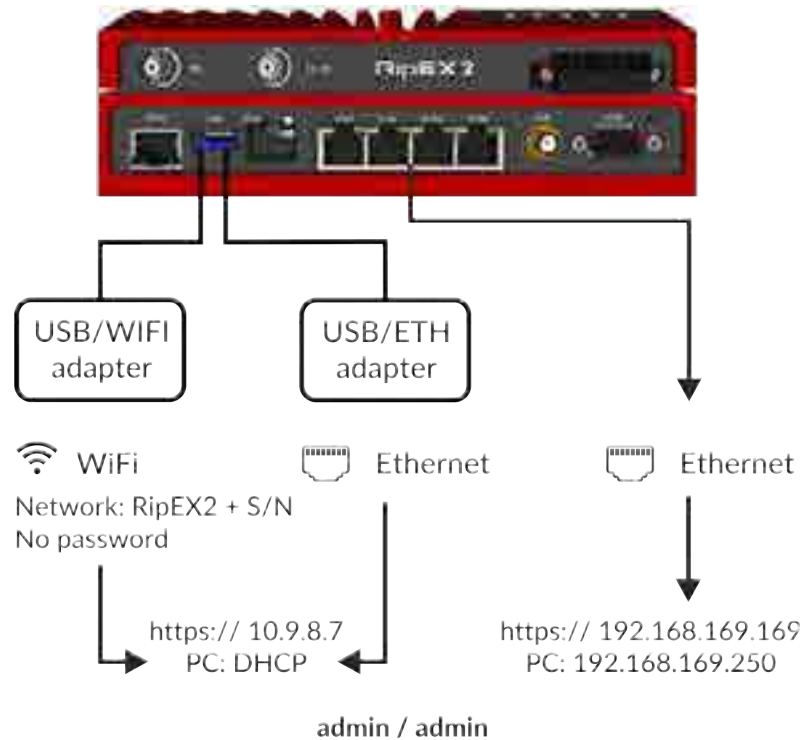


Fig. 1.1: Connecting RipEX2 to a PC over WiFi, ETH/USB adapter, ETH interface

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

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

- **PC (tablet, smartphone) connected via WiFi adapter**

External WiFi adapter Part No. OTH-USB/WIFI-W2 (an optional accessory of the RipEX2 see *ETH/USB adapter*¹) needs to be used. Any other adapter will not work correctly when connected to RipEX2 unit. Connect your PC, tablet or smartphone to RipEX2 WiFi AP first. Its default SSID is RipEX2 S/N. By default, the WPA2 PSK is disabled, so no password is required. The WiFi adapter contains a built-in DHCP server, so if you have a DHCP client in your PC (as most users do), you do not need to set anything up. The default IP address of RipEX2 unit, for access over the ETH/USB adapter, is 10.9.8.7.

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

External ETH/USB adapter Part No. OTH-USB/ETH-XR (an optional accessory of the RipEX2 see *ETH/USB adapter*²). The ETH/USB contains a built-in DHCP server, so if you have a DHCP client in your PC as most users, you do not need to set anything up. The default IP address of RipEX2 unit, for access over the ETH/USB adapter, is 10.9.8.7.

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

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

- **PC connected directly to an ETH port**

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

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

**Important**

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

**Note**

https - For security reasons the http protocol with ssl encryption can be used for the communication between the PC and RipEX2. The https protocol requires a security certificate. You must install this certificate into your web browser. The first time you connect to the RipEX2, your computer will ask you for authorisation to import the certificate into your computer. The certificate is signed by the certification authority RACOM s.r.o. It meets all security regulations and you need not to be concerned about importing it into your computer. Confirm the import with all warnings and exceptions that your browser may display during installation.

**Warning**

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

**Note**

If you do not have the USB adapter or you have forgotten the password, you can reset the access parameters to defaults, see *Section 2.2.9, "HW button"*.

1.1. Bench testing

Before installing a RipEX2 network in the field, a bench-test should be performed in the lab. The RipEX2 Demo case is great for this as it contains everything necessary: 3× RipEX2 unit, Power supply, dummy load antennas, etc.

If you use your own installation for lab tests, do not forget:

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

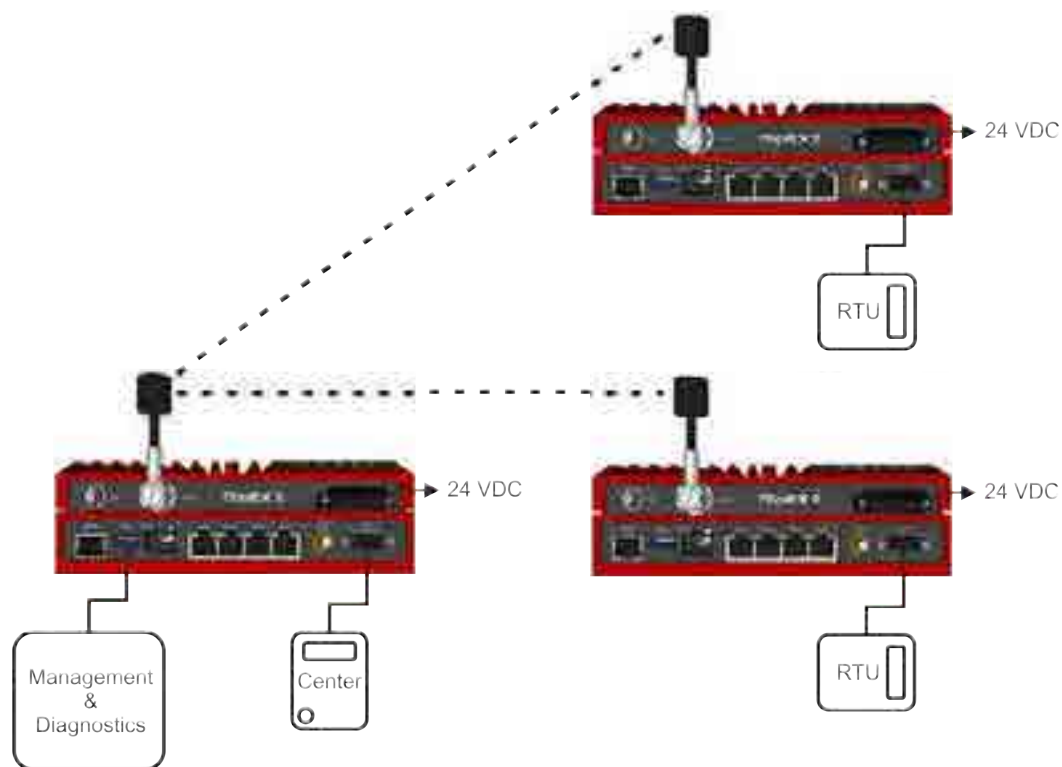


Fig. 1.2: RipEX2 bench testing

2. Product



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

RipEX2 is built into a rugged die-cast aluminium casing that allows for multiple installation possibilities, see *Section 4.1, "Mounting"*.

2.1. Dimensions

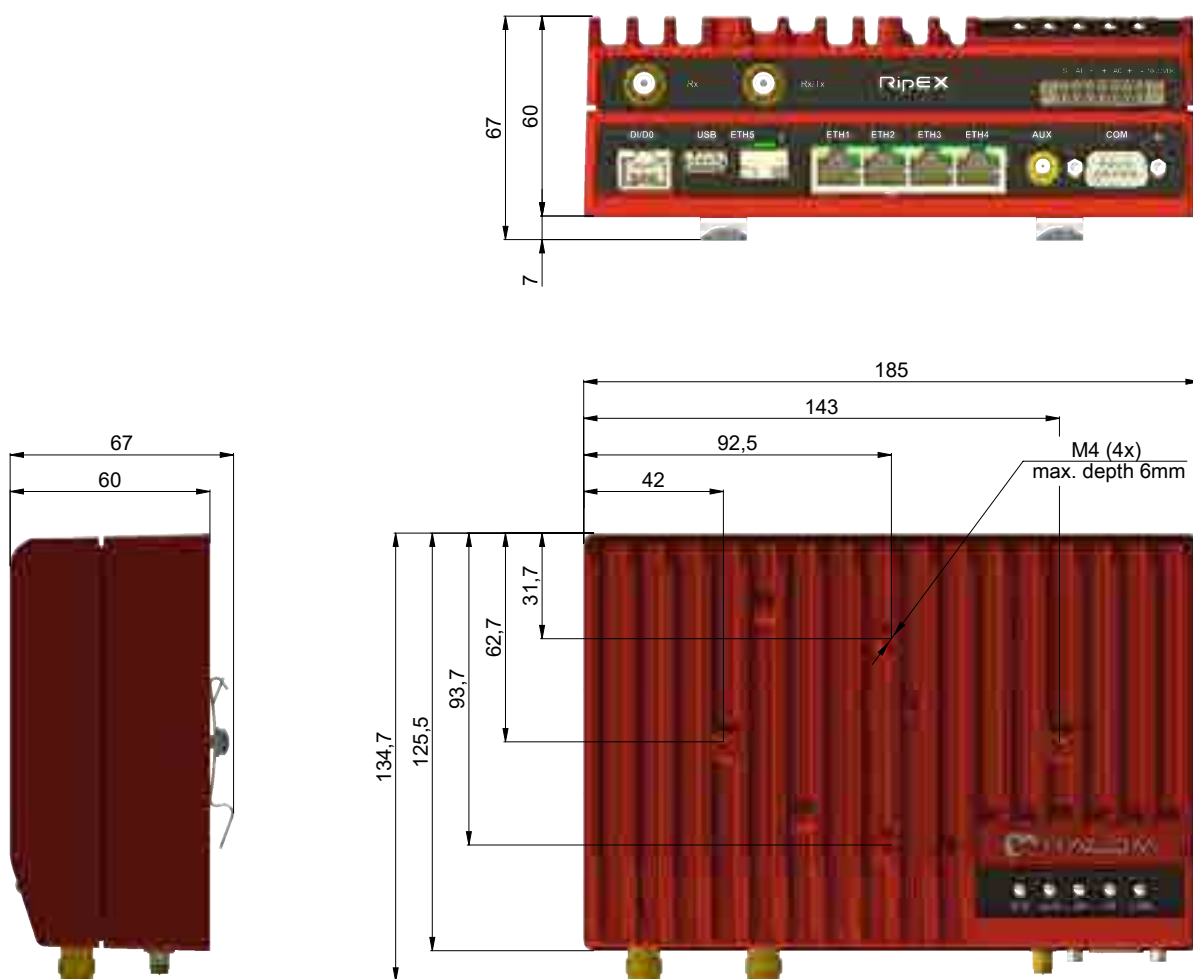


Fig. 2.1: RipEX2 dimensions

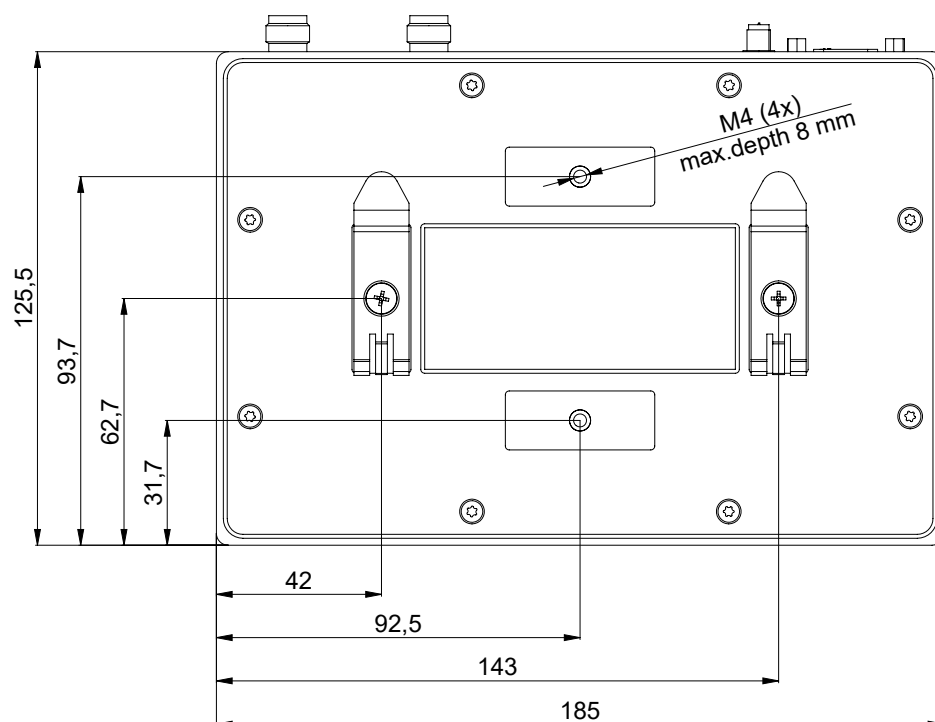


Fig. 2.2: RipEX2 dimensions – bottom

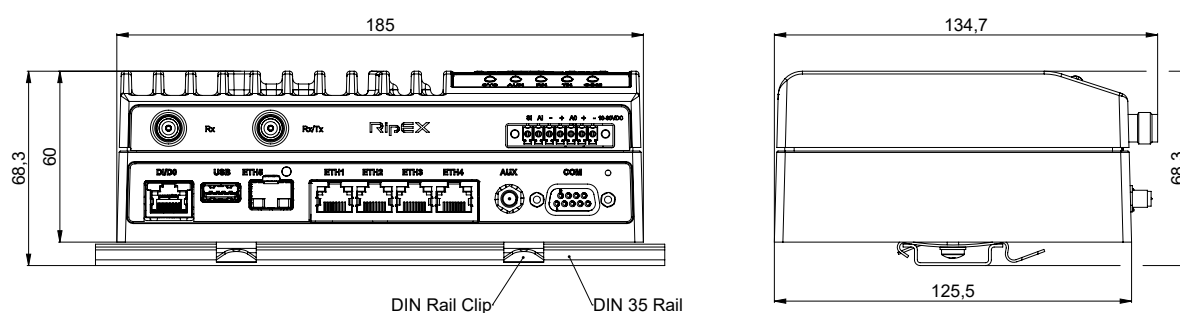


Fig. 2.3: RipEX2 with DIN rail

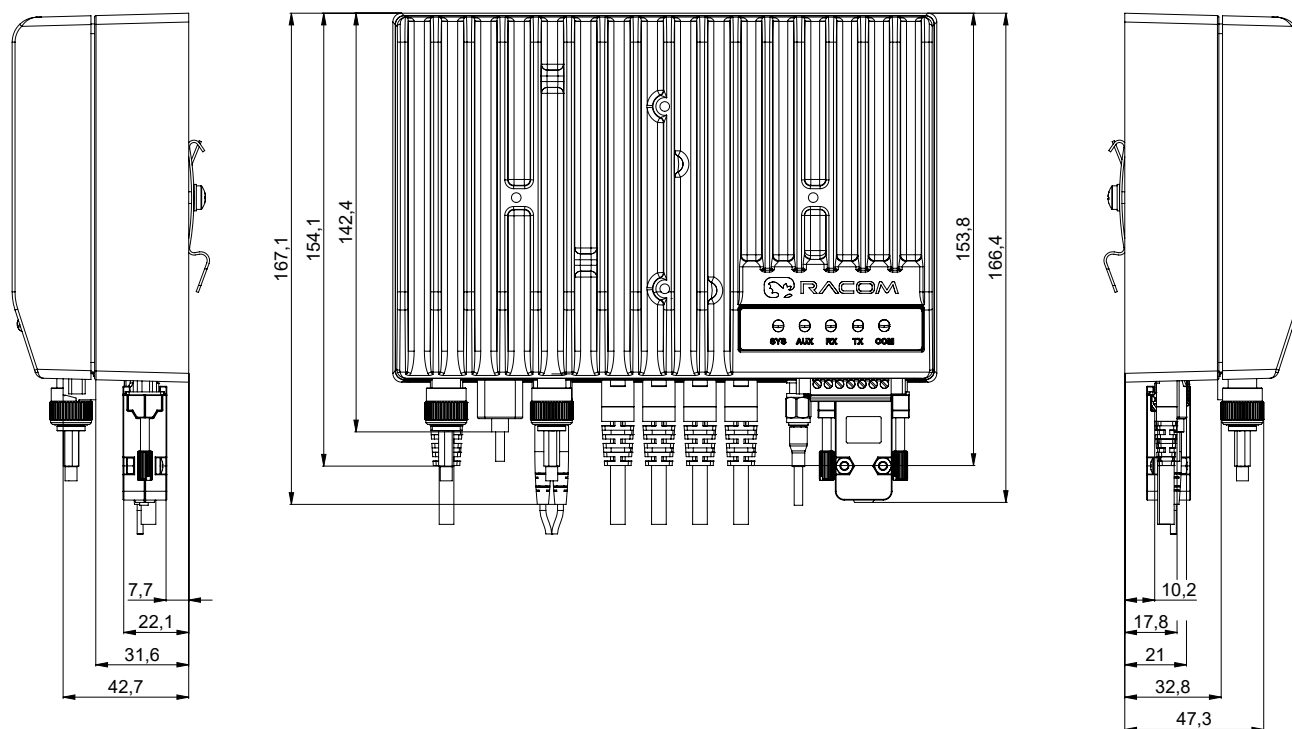


Fig. 2.4: RipEX2 dimensions with connectors

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

2.2.2. Power and Control

This rugged connector connects to a power supply and it contains control signals. A Plug with screw-terminals and retaining screws for power and control connector is supplied with each RipEX2. It is Tyco 7 pin terminal block plug, part No. 1776192-7, contact pitch 3.81 mm. The connector is designed for electric wires with a cross section of 0.5 to 1.5 mm². Strip the wire leads to 6 mm (1/4 inch). Isolated cables should receive PKC 108 or less end sleeves before they are inserted in the clip. Insert the cables in the wire ports, tightening securely.

Tab. 2.1: Pin assignment

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

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



Fig. 2.7: Supply connector

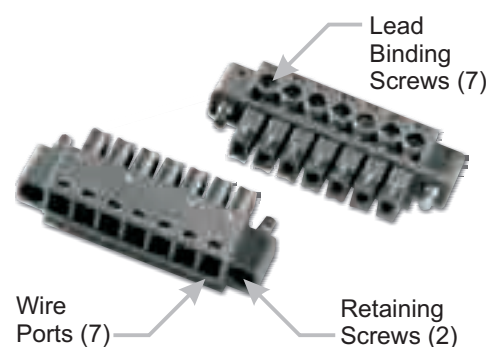
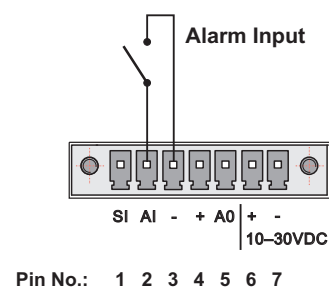


Fig. 2.8: Power and Control - cable plug

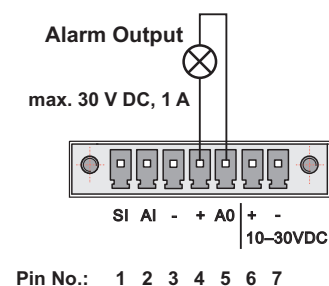
HW ALARM INPUT

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*.

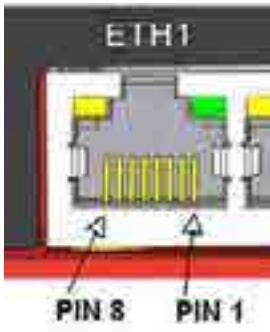
2.2.3. ETH1 - ETH4

Standard RJ45 connectors for Ethernet connection. RipEX2 has 10/100/1000Base-T Auto MDI/MDIX interfaces so it can connect to 10 Mb/s, 100 Mb/s or 1000 Mb/s Ethernet network. The speed can be selected manually or recognized automatically by RipEX2. RipEX2 is provided with Auto MDI/MDIX function which allows it to connect over both standard and cross cables, adapting itself automatically.

Pin assignment

Tab. 2.2: Ethernet to cable connector connections

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



2.2.4. ETH5 (SFP)

ETH5 is a standard SFP slot for 10/100/1000 Mb/s Ethernet SFP modules, user exchangeable with maximal power consumption 1.25 W. Both fibre optic and metallic Ethernet SFP modules are supported. For optical both single and dual mode fibre optics Ethernet modules (= 2 or 1 fibers) can be used. CSFP modules are not supported. RACOM offers all mentioned types of SFP modules, tested to be RipEX2 compatible as a standard accessory.

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

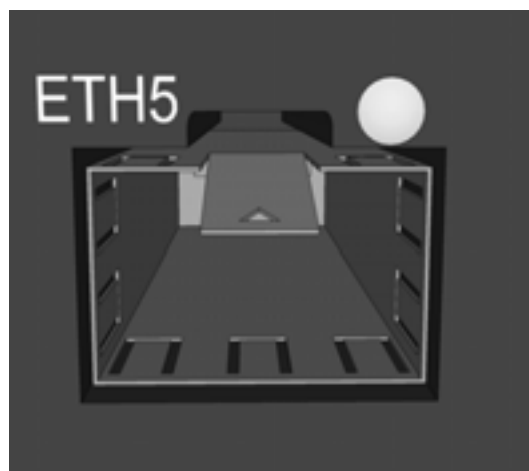


Fig. 2.9: SFP slot



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.

2.2.5. 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. 2.3: 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.

Expansion board 'C' (2 x RS232)

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

COM2 and COM3 parameters:

- COM2: RS232 - 5 pin (RxD, TxD, GND, RTS, CTS) 600 b/s to 2 Mb/s
- COM3: RS232 -3 pin (RxD, TxD, GND) 2.4 kb/s to 921.6 kb/s

Tab. 2.4: DI/DO output

Pin	Signal
1	RxD COM3
2	TxD COM3
3	GND
4	CTS COM2
5	RTS COM2
6	GND

Pin	Signal
7	RxD COM2
8	TxD COM2

This interface is not compatible with RipEX2-HS.

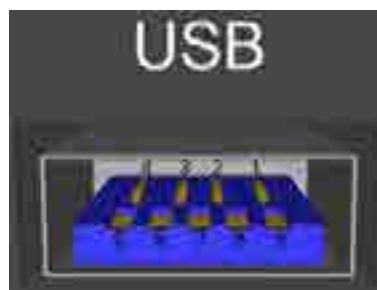
If the RipEX2 unit is installed in the RipEX2-HS (Hot Standby chassis), the DI/DO interface is dedicated for the Hot Standby operation.

2.2.6. USB

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

Tab. 2.5: 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 www.ripex/accessories¹. The adapters are used for service access to web configuration interface of RipEX2 unit.

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

2.2.7. 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. 2.10: AUX connector SMA

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

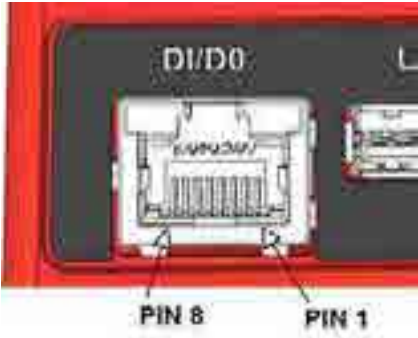
RipEX2 can be equipped with an internal GPS (Expansion board 'G'). The GPS module is used for time synchronization of the NTP server inside RipEX2. In this case the AUX connector serves for connecting the GPS antenna:

- active antenna
- 3.3 VDC supply *see details*

2.2.8. DI/DO

Tab. 2.6: Digital Inputs and Outputs

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



- Digital Outputs:
 - Open drain output max. 30 VDC, 0.2 A
- Isolated differential digital input:
 - Input voltage difference (P-N) > 1.9 VDC Logic "H"
 - Input voltage difference (P-N) < 1.1 VDC Logic "L"
 - Maximum differential voltage 30 V
- Digital inputs:
 - Schmitt-triggered inverted input
 - Pull below 1.1 VDC to activate (1.1 VDC / 1.9 VDC threshold hysteresis)
 - Max. 30 VDC

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

2.2.9. HW button



Fig. 2.11: HW button

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

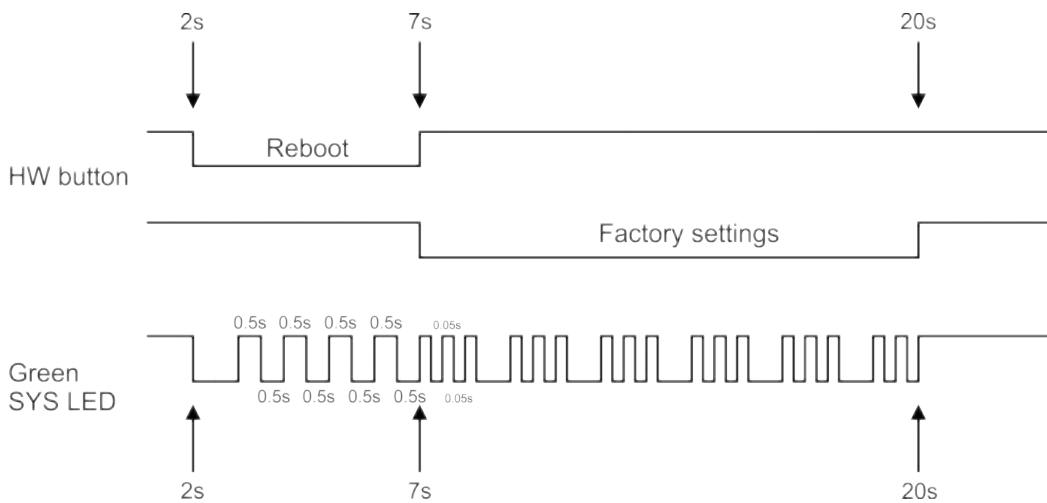


Fig. 2.12: HW button scheme

HW button operation

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

2.3. Indication LEDs



Fig. 2.13: Indication LEDs

Tab. 2.7: Key to LEDs

LED	Colour	Style	Function
SYS	Green	Permanently lit	System OK
		Flashing - period 500 ms	Reset button pushed
		Three fast (50 ms) flashes - pause (500 ms)	Reset button factory reset
	Red	Permanently lit	Alarm
		Flashing regularly - period 500 ms	Serious system error
	Orange	Permanently lit	Unit is starting
AUX	Green	Permanently lit	Activity of mPCIe connected equipment (like GPS fix, LTE connected, ...)
	Red	Permanently lit	Alarm of mPCIe connected equipment
Rx	Green	Permanently lit	Receiver is synchronized to a packet
	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
COM	Green	Permanently lit	Data receiving
	Yellow	Permanently lit	Data transmitting

Alarm

An Alarm is triggered by any event with severity Error or higher (see *Section 8.2, "Events"*).

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.

2.4. Ordering codes

RipEX2-4A-G-E (Master)

Trade name	Gen.	Band	Exp.	Var.	SW keys
Type					
Code					
Order code					

Trade name - trade and marketing name of the product. This name is used for all products within the same product family.

Possible values: **RipEX**

Gen. - generation of the product of specific Trade name. The very first generation does not have any number in this position.

Possible values: **none, 2**

Band - frequency band and sub-band

Possible values:

1A: 135-175 MHz

3A: 285-335 MHz

3B: 335-400 MHz

4A: 400-470 MHz

4B: 450-520 MHz

Exp. - Expansion board module embedded in mPCIe slot

Possible values:

N – not used

E – Expansion cellular module, Bands E; Part No.: mPCIe-E

P – Expansion cellular module, Bands P; Part No.: mPCIe-P

A – Expansion cellular module, Bands A; Part No.: mPCIe-A

Bands:

E – 4G/3G/2G, Europe, Middle East, Africa

P – 4G/3G/2G, Asia, Pacific, South America

A – 4G/3G/2G, Americas

For frequency bands *see details*

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. These variants can't be ordered and included in the unit later on.

Possible values:

Processor type – X or N or E

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

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:

Master – enables all functionalities of all possible SW feature keys; Part No.: RipEX2-SW-MASTER

Protocols - enables additional Radio protocols, BGP, OSPF; Part No.: RipEX2-SW-PROTOCOLS

Speed - enables 256QAM, Channels > 50kHz, Full duplex; Part No.: RipEX2-SW-SPEED

Power - enables RF power 40 dBm PEP; Part No.: RipEX2-SW-POWER

Security - enables IPsec, GRE, RADIUS, Multiple users, Tamper detection; Part No.: RipEX2-SW-SECURITY

SFP - enables SFP interface; Part No.: RipEX2-SW-SFP

Region – used for countries where specific restrictions are required. Available only on special request when ordering. If used, it is indicated in bracket along with the SW keys.

Possible values:

US – USA, Allowed freq. according to FCC part 90

RipEX2 - 4A: 406.1 - 454.0, 456 - 462.5375, 462.7375 - 467.5375, 467.7375 - 470.0 MHz; Reg. ID: 4A-FCC_Part_90

RU – Russia, Allowed freq. according to Russian regulations

RipEX2 - 1A: 146.0 - 174.0 MHz; Reg. ID: 1A-Russia

RipEX2 - 4A: 403.0 - 410.0, 433.0 - 450.0 MHz; Reg. ID: 4A-Russia

BR – Brazil, 6.25 kHz channel not allowed

RipEX2 - 4A: Anatel sticker 16763; Reg. ID: 4A-Brazil

MX – Mexico, Import sticker on paper box, SOL0903113T3

Type – specific product type

Possible values:

RipEX2-1

RipEX2-3

RipEX2-4

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

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

In order to find out the correct Order code, please use *RACOM WebService*².

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

* 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 http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm. In the case of export from the country where the units were delivered by Racom, the exporter must inform Racom of the new country of delivery.

3. Accessories

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

1. **L-bracket**

(see https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting)



Note

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

2. Flat-bracket

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

3. RipEX2 Hot Standby

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

4. RipEX2-RD

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

5. RipEX2-RS

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

6. USB adapters (ETH, WiFi)

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



Note

WiFi adapter Part No.: OTH-USB/WIFI-W1, which was suitable for previous generation of RipEX does not work with RipEX2 units. Please use OTH-USB/WIFI-W2 adapter instead.

7. Demo case

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

8. Ingress Protection IP52

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

9. Dummy load antenna

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

¹ <https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories>

² https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting

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

⁴ https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting

⁵ https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting

4. Installation

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 2.2, "Connectors"*).
6. Apply power supply to RipEX2.
7. Connect configuration PC (*Ripex2 "Connecting"*).
8. Configure RipEX2.
9. Test radio link quality (e.g. using Monitoring tool).
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

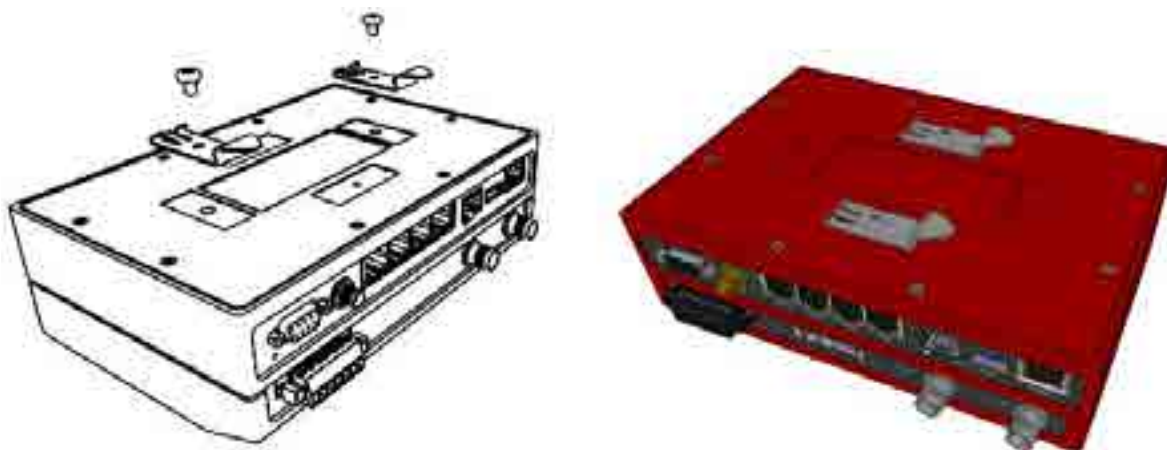


Fig. 4.2: Flat widthwise mounting to DIN rail

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

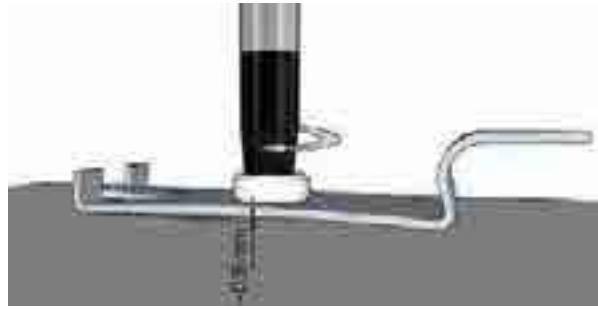


Fig. 4.3: Clip mounting

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

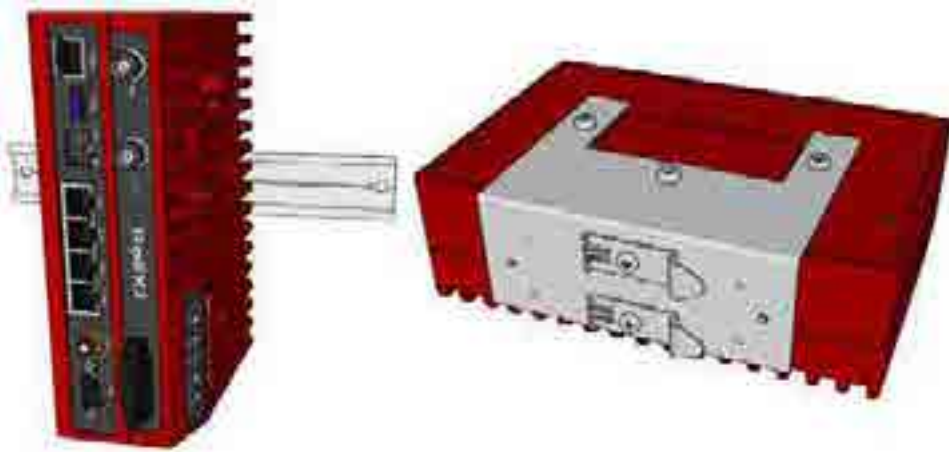


Fig. 4.4: Vertical widthwise mounting to DIN rail

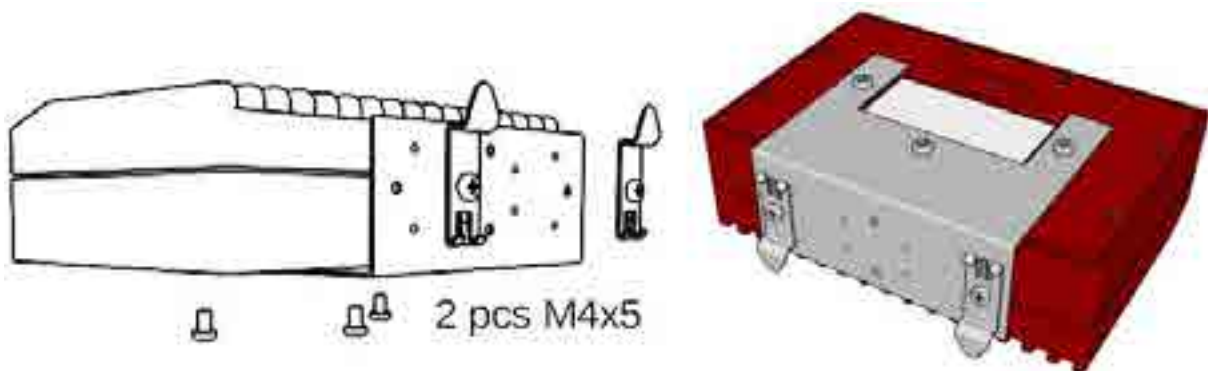


Fig. 4.5: Vertical lengthwise mounting to DIN rail

For more information see *L-bracket*¹.

¹ <https://www.racom.eu/eng/products/radio-modem-ripex.html#HOL-RipEX-L>

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

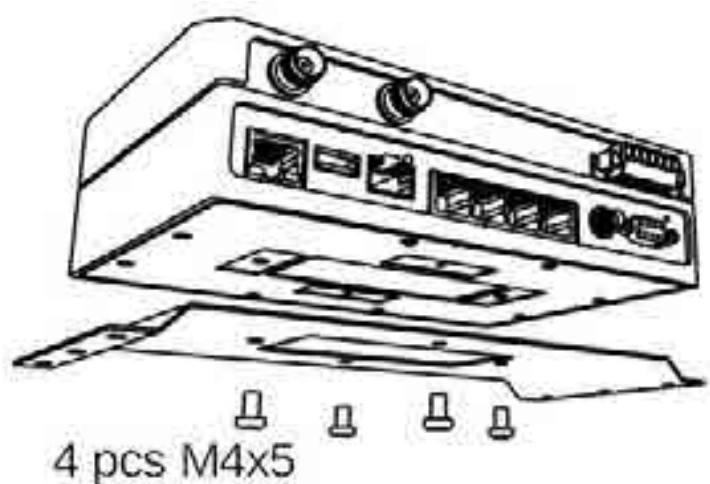


Fig. 4.7: Flat mounting using Flat bracket

For more information see *Flat-bracket*².

² <https://www.racom.eu/eng/products/radio-modem-ripex.html#HOL-RipEX-FLAT>

4.1.3. Full duplex mounting

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

When full duplex mode with high power is used in temperatures above +45°C it is recommended to use an external source of time pulse or the internal GPS. This will increase the frequency stability of the radio.

4.1.4. IP52 mounting

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

To obtain **IP5x protection**: plug in all connectors and cover unused ports (COM port does not need to be covered) with dust covers from the *SET-RipEX2-IP52*³.

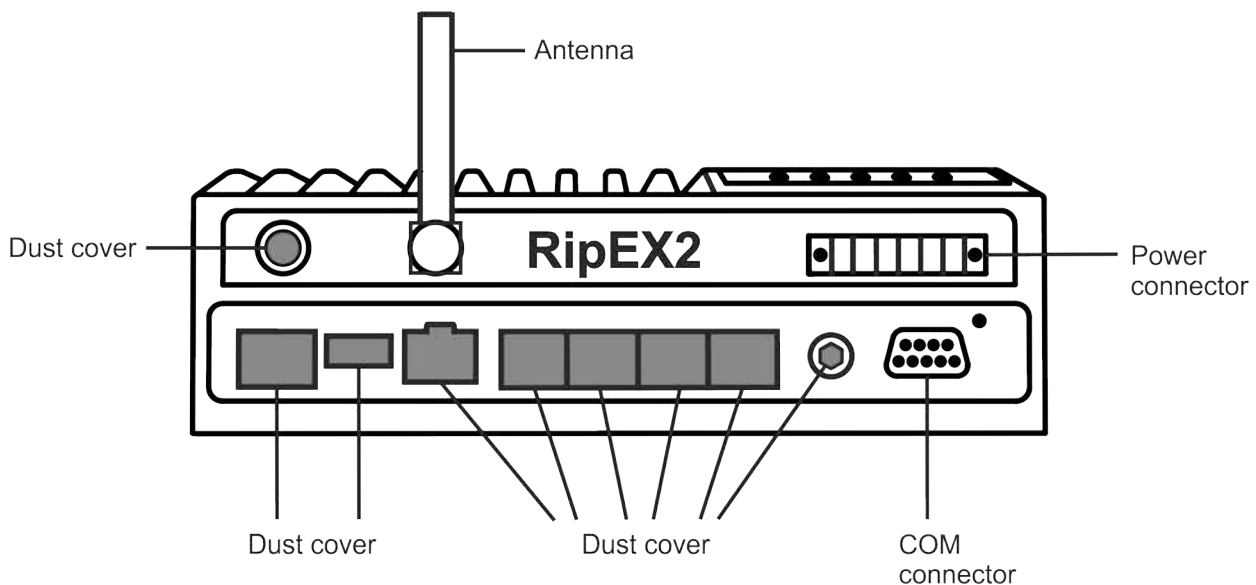


Fig. 4.8: IP5x protection

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

³ <https://www.racom.eu/eng/products/radio-modem-ripex.html#SET-RipEX-52>



Fig. 4.9: IPx2 mounting

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 2.2, "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. 4.10: 10–30 VDC Supplying

5. RipEX2 in detail

5.1. Bridge mode

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

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

Bridge mode operation depends on the following system settings:

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

Radio channel

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

Ethernet ports

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

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

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

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

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

COM port

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

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

Terminal Servers

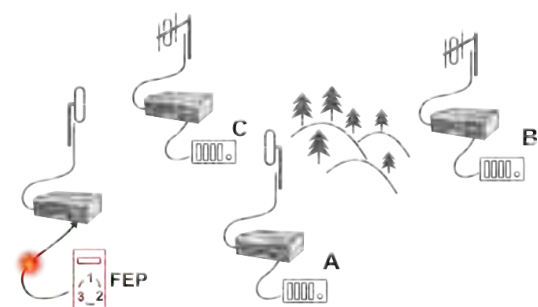
Behavior of Terminal Servers is similar to COM port. "Transparent" protocol needs to be selected when transparent data transfer to whole network (broadcasts) is needed. The other protocol types can be used for "Router mode" type of addressed communication.

5.1.1. Functionality example

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

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

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



Step 1

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



Step 2

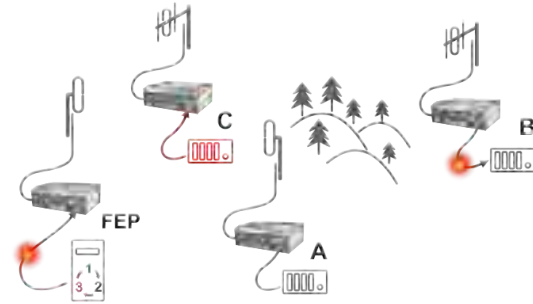
RipEX2 FEP broadcasts this packet on Radio channel.
RipEX2 C and RipEX2 A receive this packet.
RipEX2 B does not receive this packet, because it is not within radio coverage of RipEX2 FEP .



Step 3

RipEX2 C and RipEX2 A send the received packet to their COM ports.

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



Step 4

RipEX2 B sends repeated packet to its COM.

RTU B does not react, because the packet is addressed to RTU C.

RipEX2 C and RipEX2 FEP **do not** send the repeated packet to their COM ports, because it has already been sent (RipEX2 C) or received (RipEX2 FEP) on their COM (anti-duplication mechanism).

RTU C sends the reply packet.



Step 5

RipEX2 C broadcasts the reply packet from RTU C on Radio channel.

Packet is received by RipEX2 A and RipEX2 FEP.



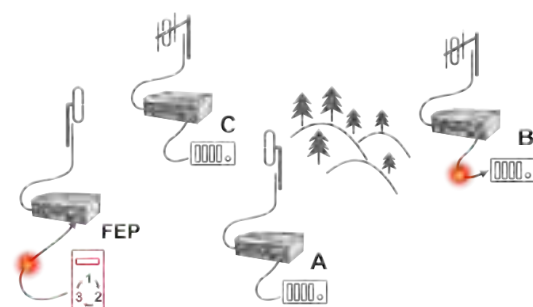
Step 6

RipEX2 FEP sends the packet (the reply from RTU C) to FEP through COM.

RipEX2 A sends this packet to RTU A. RTU A does not react, because the packet is addressed to FEP.

RipEX2 A repeats the packet on Radio channel.

All RipEX2 units receive the packet.



Step 7

RipEX2 B sends repeated packet to its COM.

RTU B does not react, because the packet is addressed to FEP.

RipEX2 C and RipEX2 FEP units **do not** send the repeated packet to their COM ports, because it has been handled already.

FEP processes the reply from RTU C and polling cycle continues...

5.1.2. Configuration examples

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

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

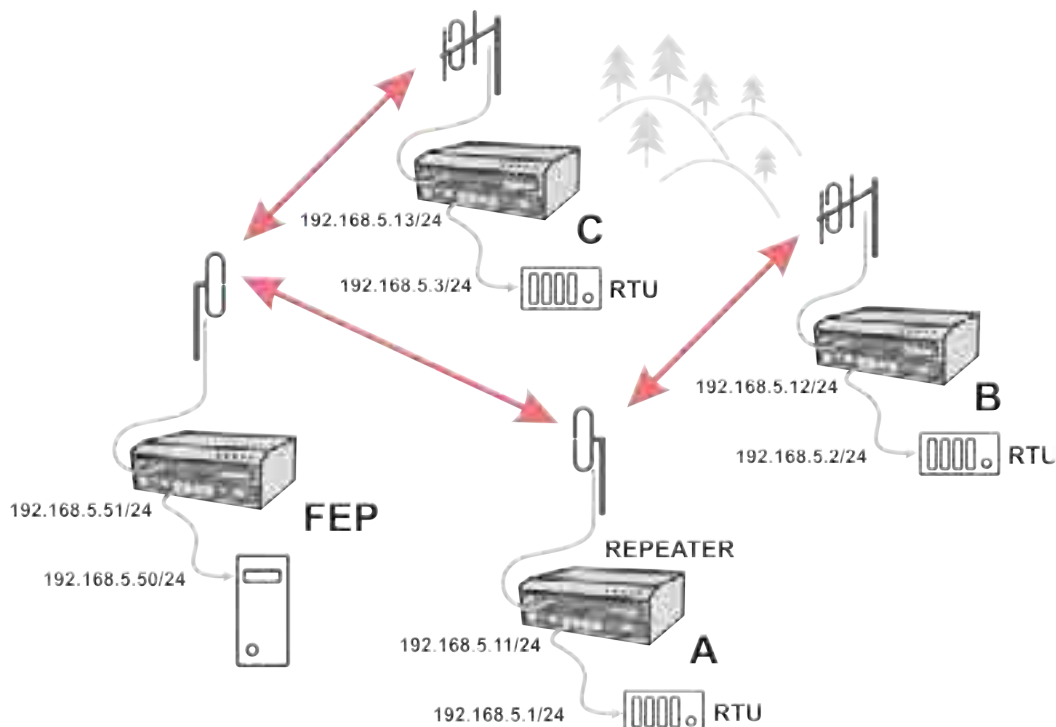


Fig. 5.1: Bridge mode example

Repeater

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

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

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

5.2. Router mode

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

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

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

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

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

- **Base driven**
This protocol is optimized for TCP/IP traffic and/or 'hidden' Remotes in report-by-exception networks, when a Remote is not heard by other Remotes and/or different Rx and Tx frequencies are used. It is suitable for a star network topology with up to 255 Remotes under one Base station, where each Remote can simultaneously work as a Repeater for one or more additional Remotes.
- **Flexible**
Suitable for master or even multi master-slave polling and report by exception from remotes concurrently. No limits in network design – each radio can work as base station, a repeater, a remote, or all of these simultaneously

5.2.1. Router - Base driven

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

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

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

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

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

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

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

5.2.1.1. Router - Base driven, Functionality example

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

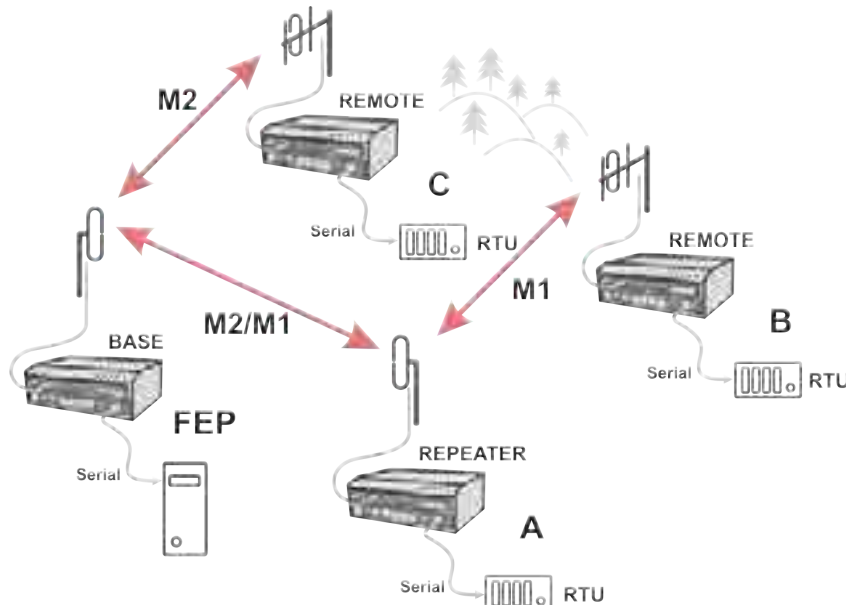


Fig. 5.2: Router - Base driven, Functionality example

Step 1

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

Step 2

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

Step 3

RTU A processes the request

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

Step 4

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

5.2.1.2. Router - Base driven, Configuration example

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

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

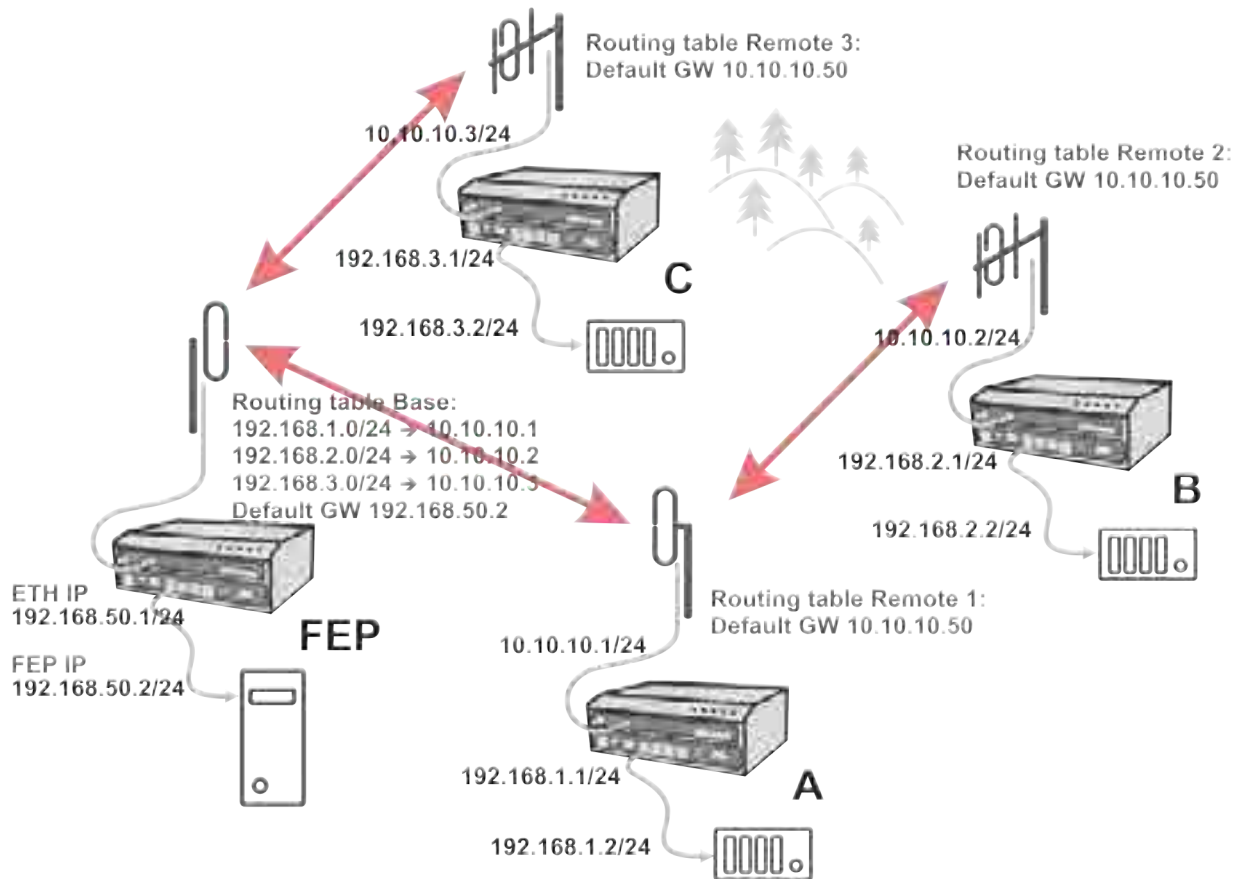


Fig. 5.3: Router - Base driven, Addressing

**Important**

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

**Note**

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

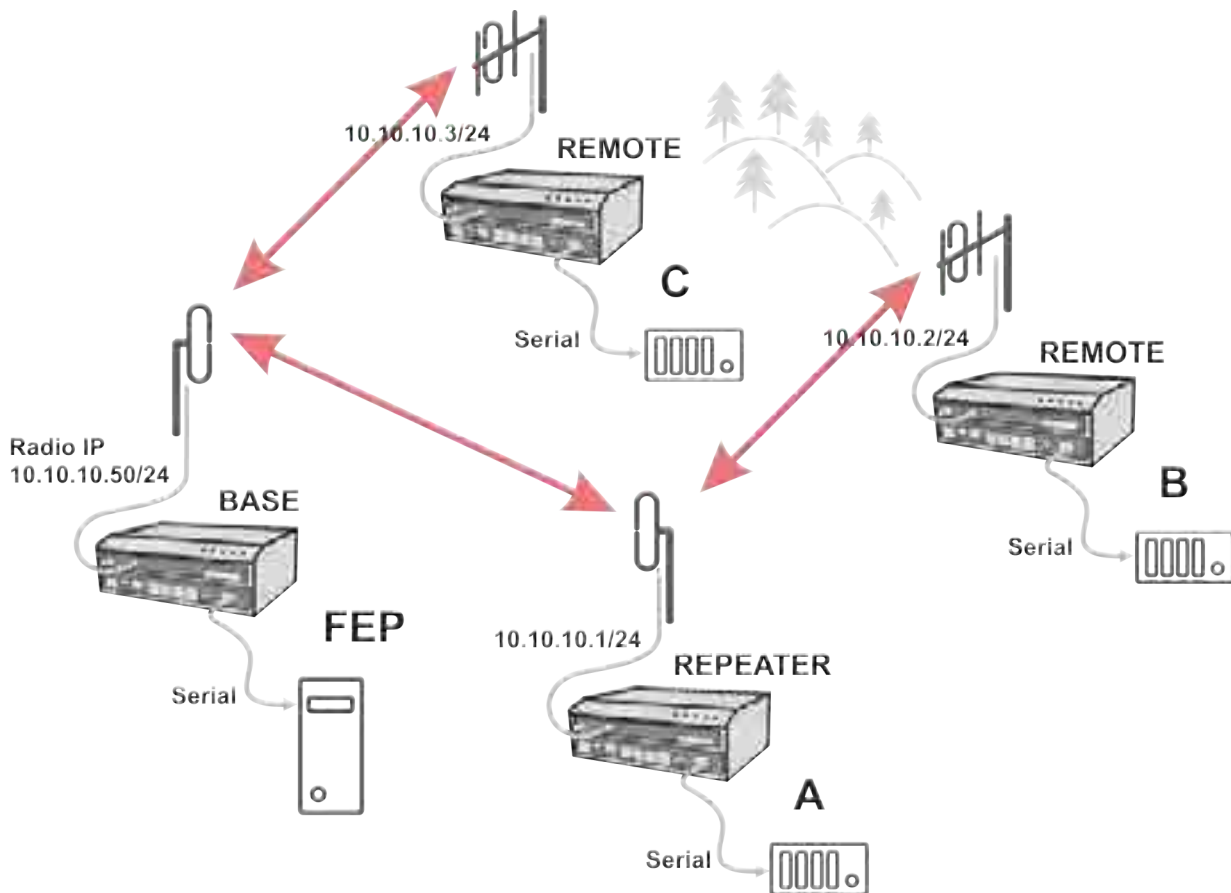


Fig. 5.4: Router - Base driven, Addressing - Serial

5.2.2. Router - Flexible

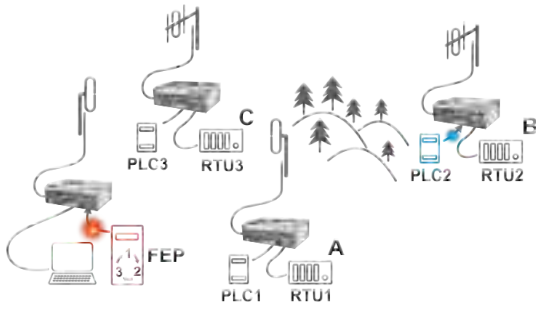
Router mode with Flexible protocol is suitable for Multipoint networks of all topologies with unlimited number of repeaters on the way, and all types of network traffic where Multi-master applications and any combination of simultaneous polling and/or report-by-exception protocols can be used.

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

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

5.2.2.1. Functionality example

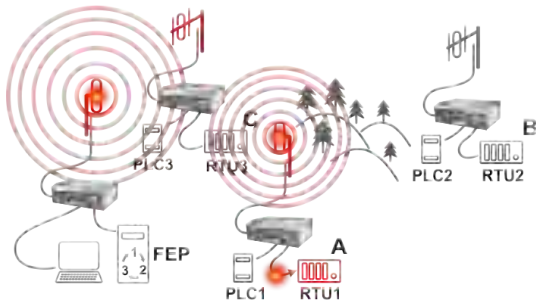
In the following example, there are two independent SCADA devices connected to RipEX2's ports (COM and ETH). One is designated RTU (Remote Telemetry Unit) and is assumed to be polled from the centre by the FEP (Front End Processor). The other is labelled PLC (Programmable Logic Controller) and is assumed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



Step 1

FEP sends a request packet for RTU1 through COM to its connected RipEX2.

Simultaneously PLC2 sends a packet for PLC1 to RipEX2 B through ETH4.



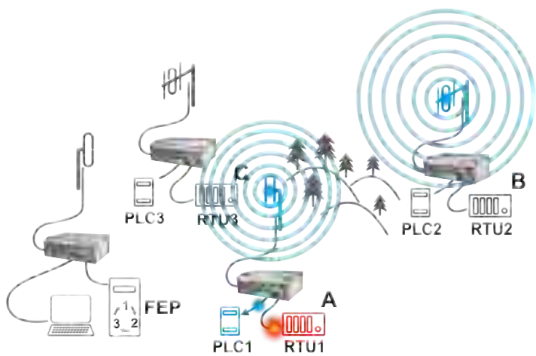
Step 2

FEP's RipEX2 transmits an addressed packet for RTU1 on Radio channel.

RipEX2 1 receives this packet, checks data integrity and transmits the acknowledgement.

At the same time packet is sent to RTU1 through COM.

RipEX2 3 receives this packet too. It doesn't react, because this packet is directed to RipEX2 1 only.



Step 3

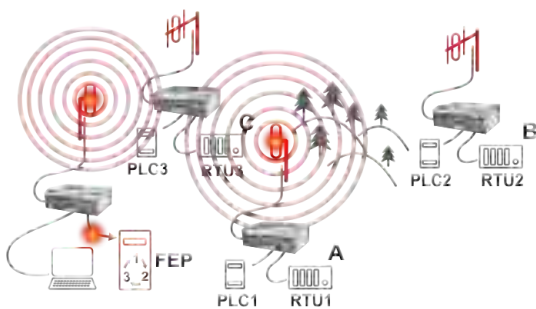
RipEX2 2 waits until previous transaction on Radio channel is finished (anti-collision mechanism).

Then RipEX2 2 transmits on Radio channel the addressed packet for PLC1.

RipEX2 1 receives this packet, checks data integrity and transmits acknowledgement.

At the same time packet is sent to PLC1 through ETH4.

Simultaneously the reply packet from RTU1 for FEP is received on COM.



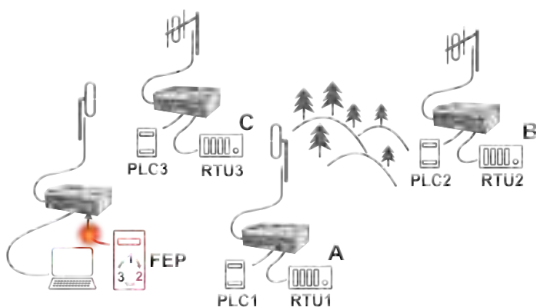
Step 4

RipEX2 1 transmits the reply packet from RTU1 for FEP on Radio channel.

All RipEX2 units receive this packet. This packet is addressed to FEP's RipEX2, so only FEP's RipEX2 reacts.

It checks data integrity and transmits the acknowledgement to RipEX2 1.

At the same time the packet is sent to FEP through COM.



Step 5

FEP receives the response from RTU1 and polling cycle continues...

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

5.2.2.2. Configuration example

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

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

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



Note

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

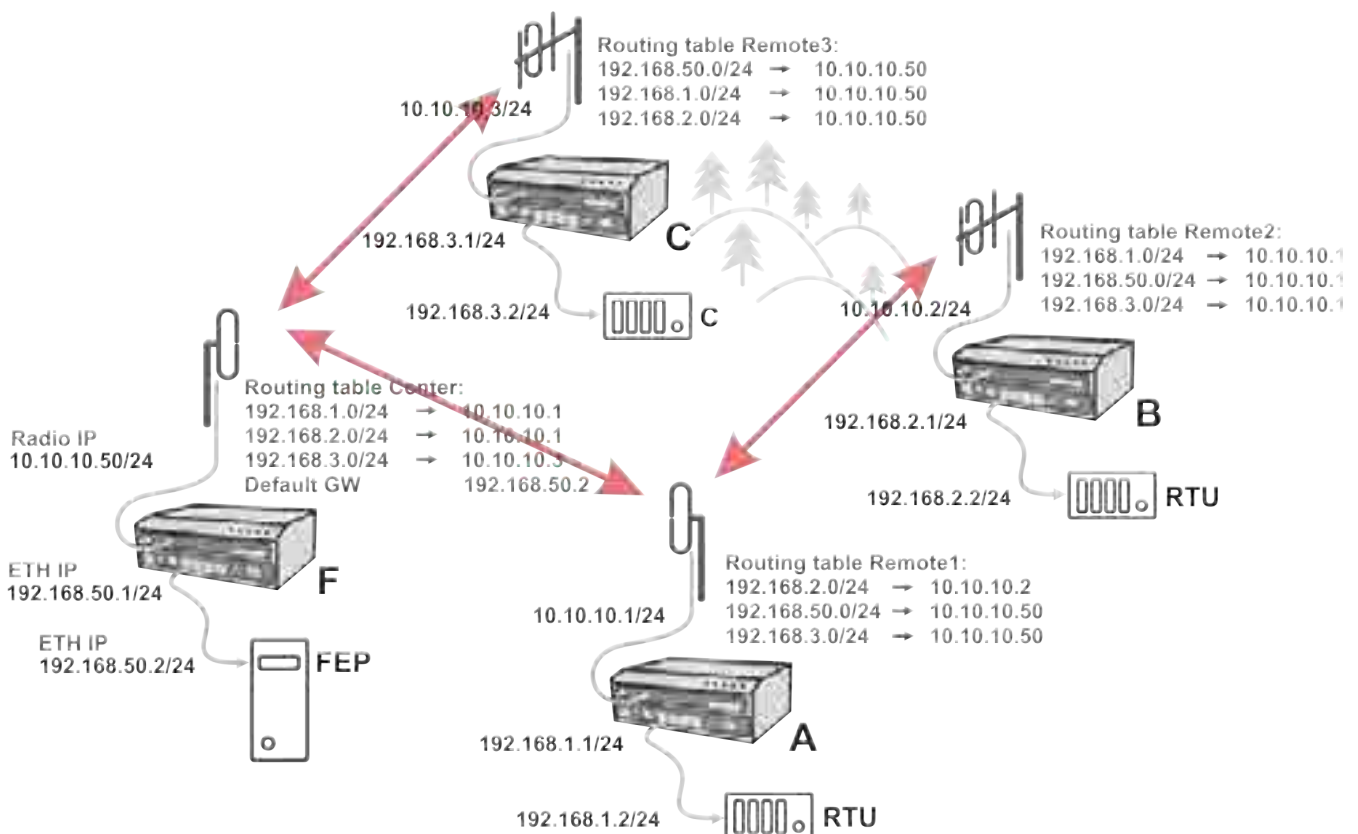


Fig. 5.5: Router - Flexible, Addressing

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

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

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

5.2.2.3. Addressing hints

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

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

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

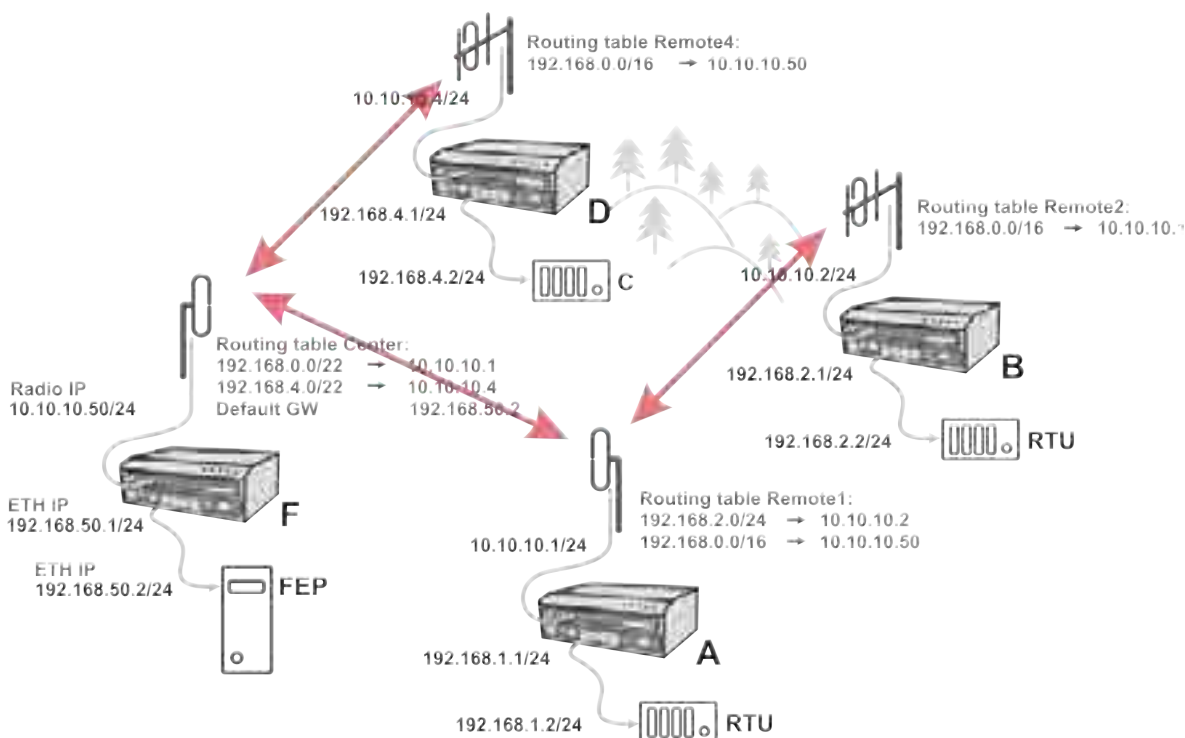


Fig. 5.6: Router - Flexible, Optimised addressing

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

5.3. Combination of IP and serial communication

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

Five independent terminal servers are available in RipEX2. Terminal server is a virtual substitute for devices used as serial-to-TCP(UDP) converters. It encapsulates serial protocol to TCP(UDP) and vice versa eliminating the transfer of TCP overhead over the radio channel.

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

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 (Local RipEX2) and the destination IP (Remote RipEX2) needs to be configured properly.

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

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

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

- **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

Supported Web browsers for mobile equipment are current versions of:

- Safari for iOS
- Chrome for android

6.2. Changes to commit

All changes of configuration parameters are marked by different color.

Type	RS485
Bandwidth (bps)	9600
Data bits	8
Priority	Event
Stop bits	1
Idle ID	15
Link ID	1000
Flow control	None

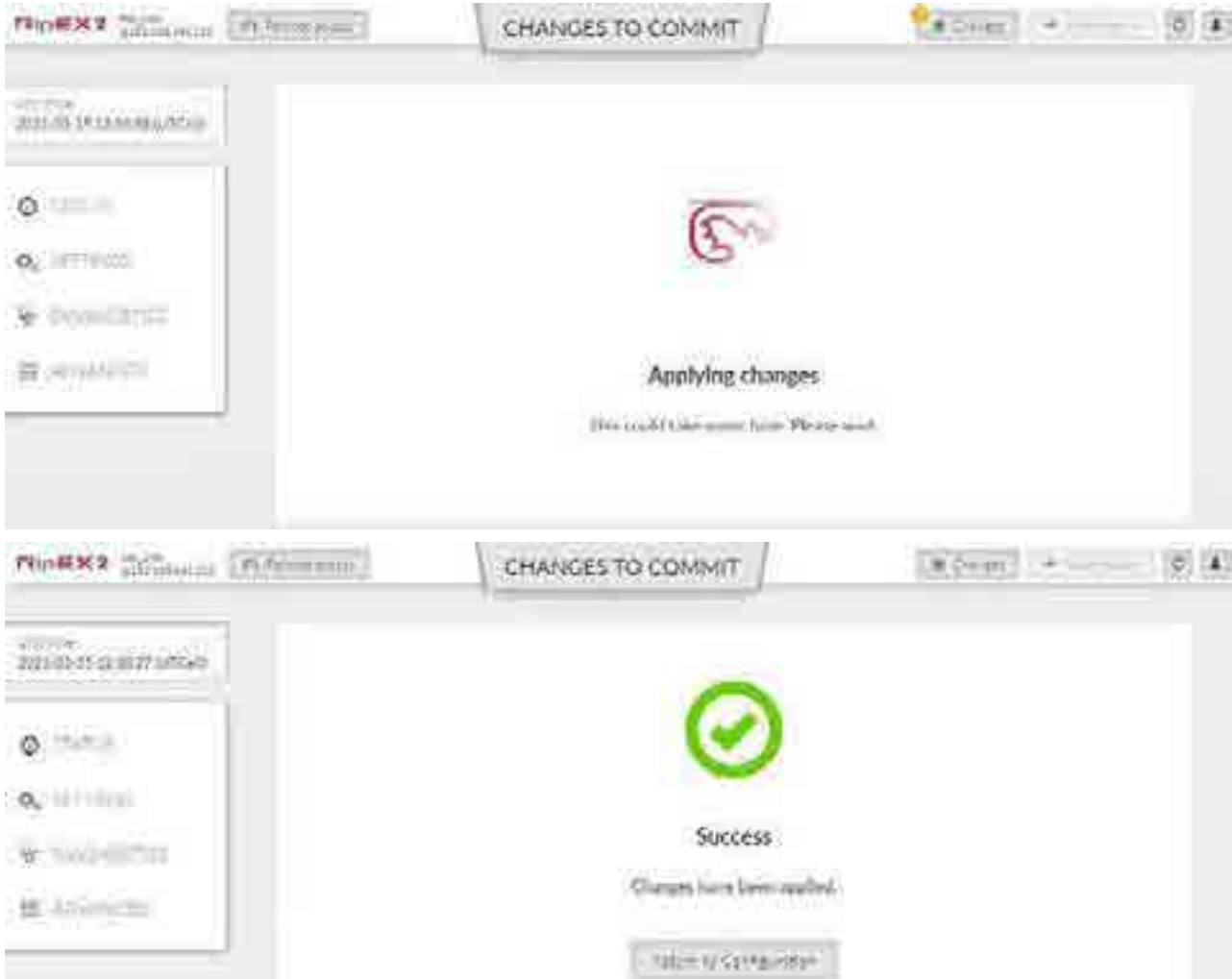
Multiple configuration changes in various menus can be prepared prior to final Commit.

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

6.3. Notifications

With RipEX2 new way of showing important system events to the user is introduced. It is called Notification Centre and is used consistently throughout the interface. Notification Centre is located on the top right corner of the interface. It exists in two forms: active notification display and full Notification Center. Both the active notification display and the full Notification Centre are displayed either below the top header of the interface or in the right hand sidebar depending on the size of user's display. The behaviour is responsive so in case the user needs to make the browser window narrower the notification center automatically changes place to use the most efficient location.



Notifications are mostly triggered by user actions in the interface, for example success or failure of Fast Remote Access connection. They are not to be confused with Events, which are triggered mostly by

the system and are not shown in the Notification Centre, but on Diagnostics > Events page. In other words Notifications are caused by the user, Events are caused by changing status of the unit.

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



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

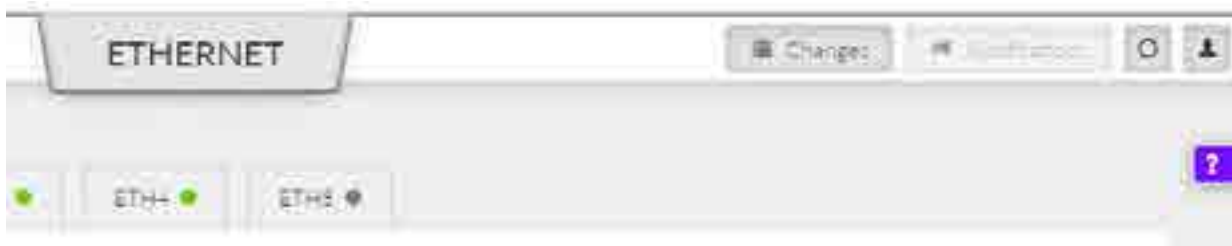
6.4. User menu



It is strongly recommended to change the default password.

6.5. Help

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

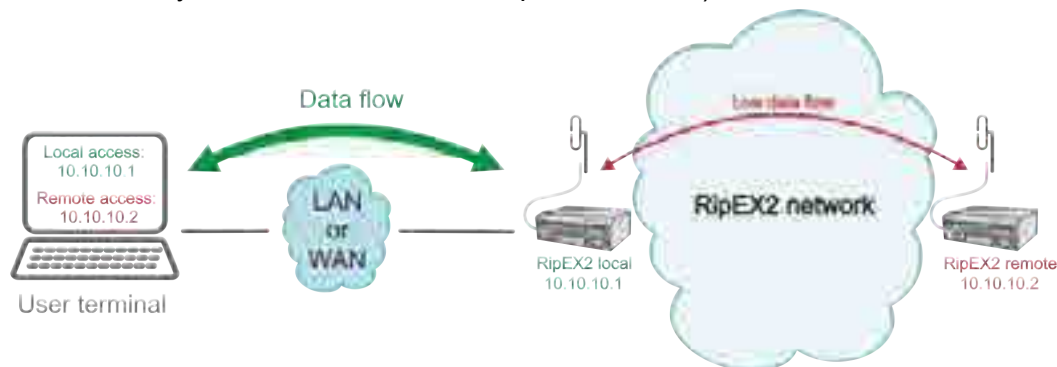




The content of the help is identical with the respective sub-chapter of the User manual.

6.6. 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).

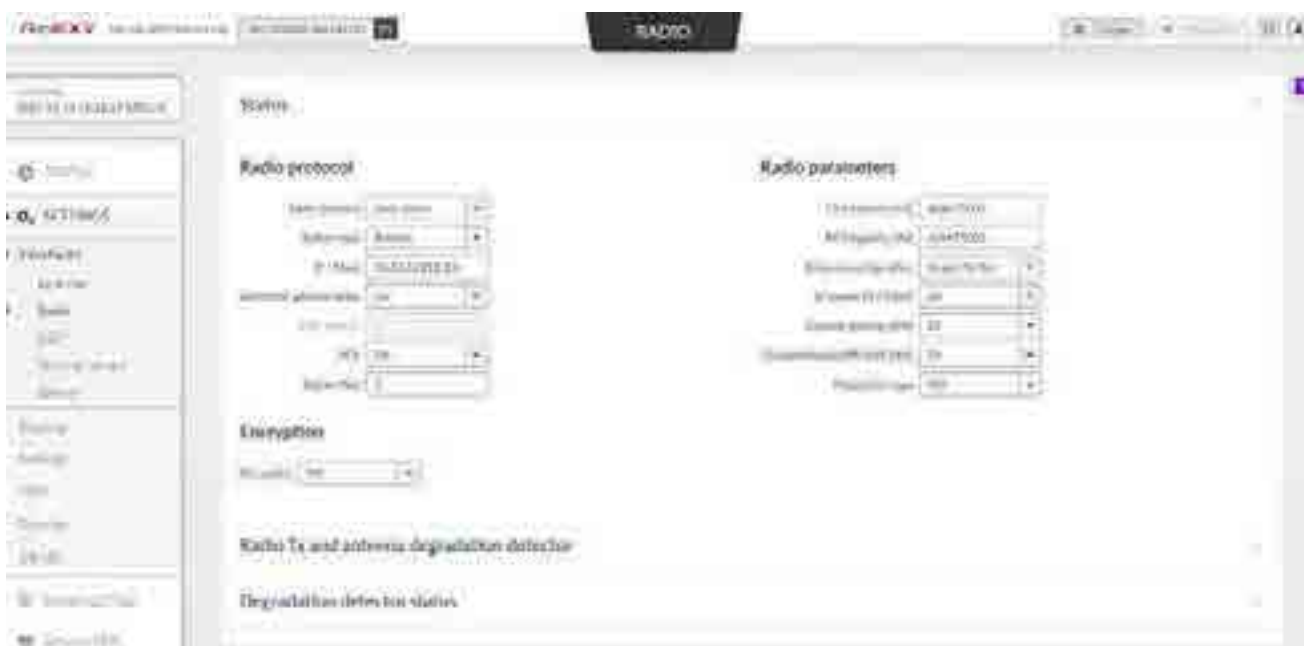


RipEX2 local unit must have the highest firmware version in the whole network to ensure proper Remote access functionality. Nevertheless it is recommended to keep the same version of firmware in the whole network. See details in chapter *Section 7.6.6, "Firmware"*

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.

7. Settings

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

7.1. Interfaces

7.1.1. Ethernet

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 Ethernet subnet description (optional).



Note

VLAN (IEEE 802.1Q) settings are accessible via ADVANCED menu only.

7.1.2. Radio

Radio interface behavior is heavily affected by a Radio protocol. There are several protocols available:

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

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

The screenshot displays the 'Radio' settings page. On the left is a sidebar menu with options: Status, Settings, Interfaces, General, Radio, COM, Network, Building, Forward, LRU, Security, and Tools. The main content area is titled 'Status' and contains three sections:

- Radio protocol:** Includes fields for 'Radio protocol' (set to 'Flexible'), 'IP / Host' (192.168.1.100), 'NCK' (ON), 'Radio ID' (0), 'Frequency (MHz)' (433.000), and 'Power (dBm)' (0).
- Radio parameters:** Includes fields for 'TX Power (dB)' (12.6), 'RF Frequency (MHz)' (433.000), 'Antenna gain (dBi)' (2.1), 'RF power (dBm)' (20), 'Channel access (MHz)' (25), 'Channel access (MHz)' (10), 'Channel access (MHz)' (10), 'Modulation type' (GFSK), 'Modulation' (GFSK), and 'FEC' (ON).
- Encryption:** Includes a dropdown menu for 'Encryption' (set to 'AES').
- Individual link options:** Includes fields for 'Encryption key (hex)' (00000000), 'Max retries' (10), 'Retry interval (s)' (1), and 'Retry timeout (s)' (10).

At the bottom, there is a button labeled 'Apply'.

7.1.2.1. Radio channel parameters

Radio parameters

TX frequency [Hz] * 424675000

RX frequency [Hz] * 424675000

Antenna configuration * Single (Tx/Rx) ▼

RF power PEP [dBm] * 20 ▼

Channel spacing [kHz] * 25 ▼

Occupied bandwidth limit [kHz] * 16 ▼

Modulation type * QAM ▼

Modulation * 64QAM ▼

FEC * Off ▼

- **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

RipEX2-3A: 285-335 MHz

RipEX2-3B: 335-400 MHz

RipEX2-4A: 400-470 MHz

RipEX2-4B: 450–520 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 *Section 7.1.2.3, "Base driven protocol (Router mode)"* of this manual.

- **Channel spacing [kHz]**

List box {possible values}, default = "25 kHz"



Note

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

- **Occupied bandwidth limit [kHz]**

List box {possible values}, default = "25 kHz"

Occupied bandwidth is limited by granted radio channel. The standards supported by using individual OBW limits are in *Section 9.1, "Detailed radio channel parameters"* of this manual.

- **Modulation type**

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

- **FSK**

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



Note

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

- **QAM**

Suitable for normal conditions offering higher data throughput.



Note

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

- **Modulation**

- FSK modulations:

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

- QAM modulations:

List box {DPSK; $\pi/4$ DQPSK; D8PSK; 16DEQAM; 64QAM; 256QAM}, default = "DPSK"

- **FEC**

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

FEC (Forward Error Correction) is a very effective method to minimize radio channel impairments. Basically, the sender inserts some redundant data into its messages. This redundancy allows the receiver to detect and correct errors; used is Trellis code with Viterbi soft-decoder. The improvement comes at the expense of the bitrate. The lower the FEC ratio, the better the capability of error correction and the lower the bitrate. Bitrate = Modulation rate $\times$ FEC ratio.

- **Encryption**

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

AES 256-CCM (Advanced Encryption Standard) can be used to protect your data from an intrusion on Radio channel. When AES 256 is On, control block of 16 Bytes length is attached to each frame on Radio channel. AES requires an encryption key. The length of key is 256 bits (32 Bytes, 64 hexa chars). The same key must be stored in all units within the network.

- **Mode**

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

- **Passphrase** The key can be automatically generated based on a Passphrase. Fill in your Passphrase (any printable ASCII character, min. 1 char, max. 128 char). The same Passphrase must be set in all units within the network
- **Key [64 hex digits]** The key can be configured manually (fill in 32 Bytes of 64 hexa chars). The same key must be in all units within the network.

7.1.2.2. Transparent protocol (Bridge mode)

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

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

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

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

The screenshot shows a configuration window titled "Radio protocol". It contains the following settings:

- Radio protocol: Transparent (dropdown menu)
- Communication mode: Half Duplex (dropdown menu)
- Unit is repeater: Off (dropdown menu)
- No of repeaters: 0 (text input)
- Tx delay (B): 0 (text input)

- **Radio protocol**

List box {Transparent; Base driven; None}, default = "Transparent"

- **Communication mode**

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

Full duplex mode is intended to be used mainly for Point-to-Point communication. Full duplex operation is not possible in networks with repeaters.

- **Unit is repeater**

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

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

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

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

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

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

- **No of repeaters**

Number {0 – 7}, default = 0

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

- **Tx delay [B]**

Number {0 – 1600}, default = 0

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

7.1.2.3. Base driven protocol (Router mode)

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

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



Note

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



Note

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

7.1.2.3.1. Radio protocol - Base station

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



Note

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

7.1.2.3.2. Base station - List of Remote stations

- **BDP address (from), BDP address (to)**
Protocol address [0 to 255] is the unique address assigned to each Remote and is only used by Base driven protocol. It is set in Remote unit in its Radio protocol settings. The default and recommended setting assigns Protocol address to be equal to the Radio IP last byte (Protocol address mode in Remote unit is set to Automatic then). If a specific address is required, fill both windows with the same number. If and interval is required, fill both windows with needed numbers.
- **Modulation type**
List box {2CPFSK; 4CPFSK; DPSK; $\pi/4$ DQPSK; D8PSK; 16DEQAM; 64QAM; 256QAM}, default = "2CPFSK"
- **FEC**
List box {Off; 2/3; 3/4; 5/6}, default = "Off"
- **ACK**
List box {On; Off}, default = "On"

- **Retries**

Number {0 – 15}, default = 3

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

- **CTS Retries**

Number {0 – 15}, default = 3

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

- **Connection**

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

7.1.2.3.3. Radio protocol - Remote station



The screenshot shows a configuration window titled "Radio protocol". It contains several settings:

- Radio protocol:** A dropdown menu set to "Base driven".
- Station type:** A dropdown menu set to "Remote".
- IP / Mask:** A text box containing "10.10.10.12/24".
- Automatic address mode:** A dropdown menu set to "Off".
- BDP address:** A text box containing "1".
- Ack:** A dropdown menu set to "On".
- Retries [Nul]:** A text box containing "3".

- **Automatic address mode**

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

- **BDP address**

- **ACK**

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

7.1.2.4. Flexible Protocol (router mode)

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

Radio protocol

Radio protocol	Flexible	▼
IP / Mask	10.10.10.210/24	
ACK	On	▼
Retries [No.]	3	
Foreign packets RSS threshold [-dBm]	120	
Repeat COM broadcast	Off	▼

- **IP / Mask**

IP address of the radio interface and the mask of the radio network.

- **ACK**

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

General setting of acknowledging of received packets. It can be set differently in individual link options.

- **Retries [No.]**

Number {0 .. 15}, default = 3

- **Foreign packets RSS threshold [-dBm]**

Number {50..150}, default = 120

When the received foreign packet (the packet which is not addressed to the actual unit) has weaker signal (the listed number bigger, e.g. the limit 120 - in minus dBm - compared with actual RSS -126 dBm), the channel is evaluated as free. If the foreign packet RSS is over this limit, the channel is occupied and the unit will wait till the end of it with the procedure of transmission.

- **Repeat COM broadcast**

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

When On the broadcasted COM packets will be retranslated into the radio channel. When Off these packets will not be repeated.

7.1.2.5. Advanced radio parameters

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

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

7.1.2.5.1. Radio parameters - advanced

There is only one advanced radio parameter

- **Maximal distance**

Number {0 to 200}, default = "100"

This parameter allows to set a maximal distance of a radio hop (in km). The same number shall be used for the whole network. We recommend to change the value only in case that the network uses radio hops longer than 100 km.

7.1.2.5.2. Queues

- **TX Buffers**

The Radio protocol transmission buffer handles data waiting to be transmitted. Its size is defined by both the number of records (Queue length) and total storage space (Queue size) requirement. Records are held in a queue which is considered full, if either the Queue length or Queue size is reached. New incoming frames are not accepted when the queue is full.

The TX buffer is active for all radio protocols.

This functionality is available in ADVANCED/Interfaces/Radio/Queues menu

- **Queue length [packets]**

Number {1 – 31}, default = 5

Queue length dictates the maximum number of records held in the queue.

- **Queue size [kB]**

Number {1 – 48}, default = 5

Queue size dictates the total size of all records that can be held in the queue.

- **TX Buffer timeout enabled**

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

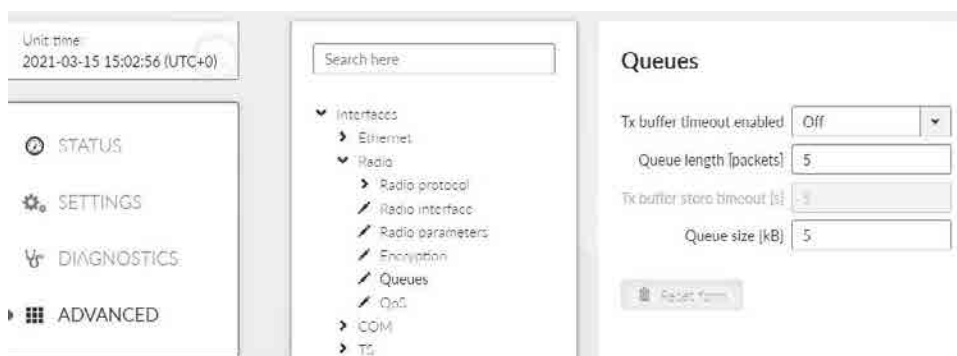
The frames waiting for transmission in the Radio protocol output frame queue will be discarded after the TX Buffer timeout expires. This parameter should be enabled for types of applications where sending old frames brings no benefit.

When the frame is discarded the event is recorded, both in the statistics (as “Rejected”) and in the monitoring (the respective frame is displayed with the “Tx buffer timeout” tag).

- **TX Buffer store timeout [s]**

Number {0.01 – 150}, granularity 0.01, default = 5

Radio protocol transmit buffer timeout. The “TX Buffer timeout” must be enabled for this parameter to be initiated.



7.1.2.5.3. Flexible - advanced

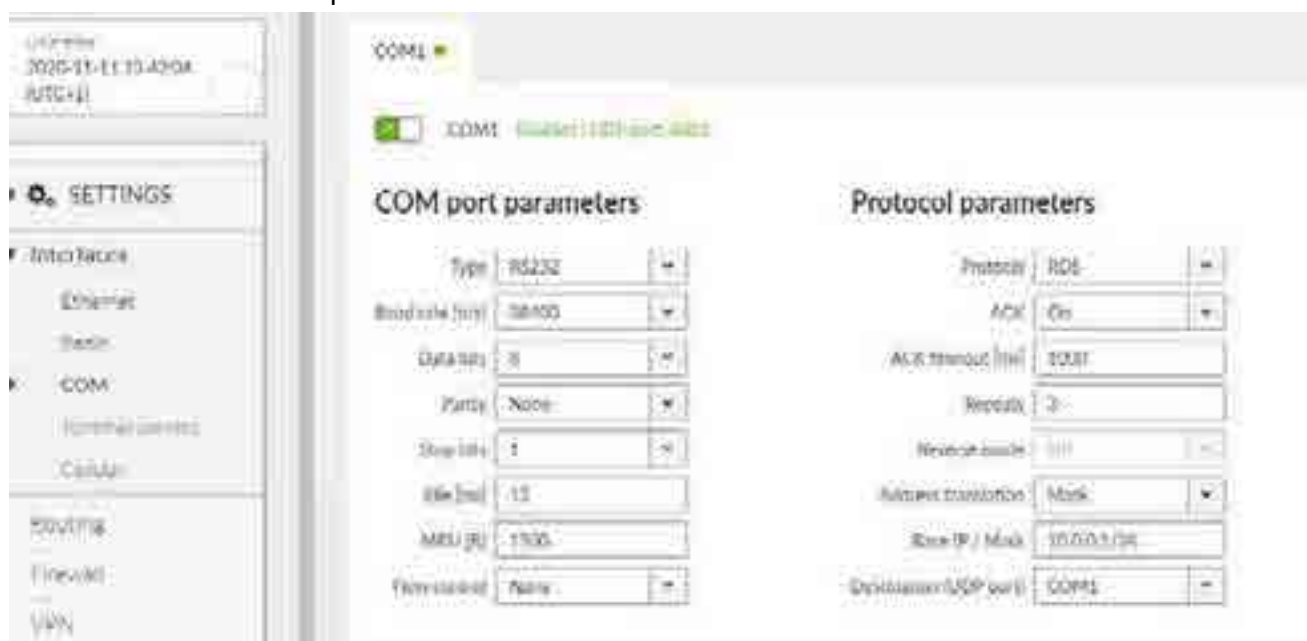
This settings allows to customize individual length and numbers of slots used for accessing of the radio channel or waiting with retransmissions of an undelivered packet.

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

7.1.3. COM

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

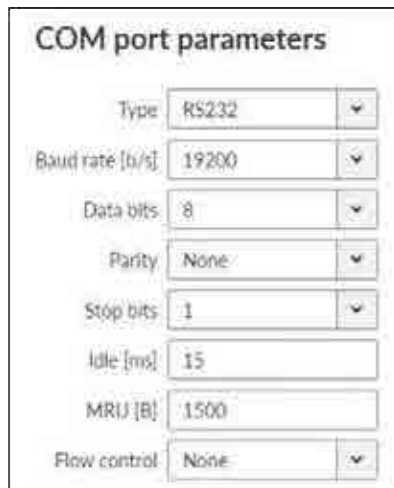
When expansion board "C" is installed two additional COM ports (RS232) are available. Their setting is similar to the COM1 port.



The menu is divided to two parts:

7.1.3.1. COM port parameters

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



COM port parameters	
Type	RS232
Baud rate [b/s]	19200
Data bits	8
Parity	None
Stop bits	1
Idle [ms]	15
MRU [B]	1500
Flow control	None

- **Type**

List box {possible values}, default = "RS232"

COM port can be configured to either RS232 or RS485.

- **Baud rate [b/s]**

List box {standard series of rates from 600 to 1152000 b/s}, default = "19200"

Select Baud rate from the list box: 600 to 1152000 b/s rates are available.

Serial ports use two-level (binary) signaling, so the data rate in bits per second is equal to the symbol rate in bauds.

- **Data bits**

List box {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 [ms]**

Number {10 – 16383}, default = 20

This parameter defines the maximum gap (in milliseconds) in the received data stream. If the gap exceeds the value set, the link is considered idle, the received frame is closed and forwarded to the network.

- **MRU [B]**

Number {1 – 2047}, default = 1500

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



Note

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



Note

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

- **Flow control**

List box {None; RTS/CTS}, default = "None"

RTS/CTS (Request To Send / Clear To Send) hardware flow control (handshake) between the DTE (Data Terminal Equipment) and RipEX2 (DCE - Data Communications Equipment) can be enabled in order to pause and resume the transmission of data. If RX buffer of RipEX2 is full, the CTS goes down.



Note

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

7.1.3.2. Common Protocol parameters

Each SCADA protocol used on serial interface is more or less unique. The COM port protocol module performs conversion to standard UDP datagrams to travel across RipEX2 Radio network.

The screenshot shows a window titled "Protocol parameters" with the following fields:

- Protocol: DNP3 (dropdown menu)
- Broadcast: On (dropdown menu)
- Address translation: Mask (dropdown menu)
- Base IP / Mask: 10.0.0.1/24 (text input)
- Destination (UDP port): COM1 (dropdown menu)

- **Protocol**

List box {None; Transparent; Async Link; DNP3; DF1; IEC101; Modbus RTU; PR2000; RDS; S3964R; UNI}, default = "None"

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

- **Broadcast**

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

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

- **Broadcast address**

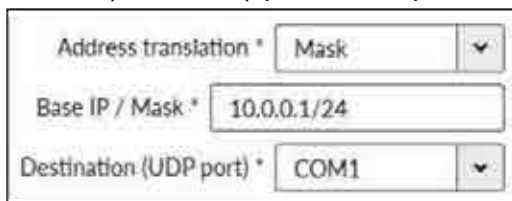
Number {0 – 65535}, default = "255"

The protocol address which is treated as broadcast address.

- **Address translation**

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

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



- **Mask**



Note

- all IP addresses used have to be within the same subnet, which is defined by this Mask
- the same UDP port is used for all the SCADA units, which results in the following limitations:
 - – SCADA devices on all sites have to be connected to the same interface
 - – only one SCADA device to one COM port can be connected, even if the RS485 interface is used.

- **Base IP / Mask**

A part of Base IP address defined by this Mask is replaced by 'Protocol address'. The SCADA protocol address is typically 1 byte long, so Mask 24 (255.255.255.0) is most frequently used.

- **Destination UDP port**

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

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

Address translation *

Protocol address translation

● First unit

Protocol address: 1

IP address: 10.11.12.1

● Second unit

Protocol address: 2

IP address: 10.11.15.1

● Third unit

Protocol address: 3

IP address: 10.12.17.6

+ Add protocol address translation

Edit protocol address translation

☐ Enabled

Note

Protocol address (Hex)

Protocol address (Dec)

IP address (Hex)

Destination UDP port



Note

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

- **Protocol address (from)**

This is the address which is used by SCADA protocol.

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

- **Protocol address (to)**

Several consecutive SCADA addresses shall be translated using one rule.

- **IP address (base)**

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

- **Destination (UDP port)**

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

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

7.1.3.3. Individual protocol parameters

In some protocols in the Slave mode of connected device is possible to choose the target of the response

- Response target mode

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

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

- Response target IP

IP address to which the response will be sent when TARGET is chosen in the Response targeted mode.

7.1.3.3.1. None

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

7.1.3.3.2. Transparent protocol

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

7.1.3.3.3. Async link

Async link creates an asynchronous link between two COM ports on different RipEX2 units. Received frames from COM port or from a Terminal server are sent without any processing transparently 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.

The screenshot shows the 'Protocol parameters' window with the following settings:

- Protocol: Async Link
- Destination IP: 192.168.0.0
- Destination (UDP port): COM1
- Transmit as broadcasts: Off
- Accept broadcasts: Off

- **Destination IP**

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

- **Transmit as broadcasts**

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

Allows sending of the packets incoming from COM port as broadcast.

- **Accept broadcasts**

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

On: Broadcast packets from the radio channel will be send to the COM port.

Off: Only unicast packets will be send to the COM port.

7.1.3.3.4. DNP3

Each frame in the DNP3 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in terms of the RipEX2 configuration. The DNP3 allows both Master-Slave polling as well as spontaneous communication from the remote units.

The screenshot shows the 'Protocol parameters' window with the following settings:

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

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

- **Broadcast**

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

**Note**

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

7.1.3.3.5. DF1

Each frame in the Allen-Bradley DF1 protocol contains the source and destination addresses in its header, so there is no difference between Master and Slave in the Full duplex mode in terms of RipEX2 configuration.

Protocol parameters

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

- **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**

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

7.1.3.3.6. IEC101

The screenshot shows a configuration window titled "Protocol parameters" for the IEC101 protocol. It contains several settings:

- Protocol:** A dropdown menu set to "IEC101".
- ComProt_IECMode:** A dropdown menu set to "Primary".
- ComProt_IECAddrMode:** A dropdown menu set to "8bit".
- Broadcast:** A dropdown menu set to "On".
- Address translation:** A dropdown menu set to "Mask".
- Base IP / Mask:** A text input field containing "10.0.0.1/24".
- Destination (UDP port):** A dropdown menu set to "COM1".

- **ComProt_IECMode**
List box {Primary; Secondary; Combined}, default = "Primary"
- **ComProt_IECAddrMode**
List box {8bit; 16 bit; 8bit w/o ctrl bytem 8bit swpctrl byte; No addr}, default = "8bit"
- **Broadcast**
List box {On; Off}, default = "On"

7.1.3.3.7. Modbus RTU

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

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

The screenshot shows a configuration window titled "Protocol parameters" for the Modbus RTU protocol. It contains several settings:

- Protocol:** A dropdown menu set to "Modbus RTU".
- Mode of Connected device:** A dropdown menu set to "Master".
- Broadcast:** A dropdown menu set to "On".
- Broadcast address:** A text input field containing "0".
- Address translation:** A dropdown menu set to "Mask".
- Base IP / Mask:** A text input field containing "10.0.0.1/24".
- Destination (UDP port):** A dropdown menu set to "COM1".

- **Mode of Connected device**
Listbox {Master; Slave}, default = "Master"
- **Mode of connected device: MASTER**
 - **Broadcast address**

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

- **Mode of connected device: SLAVE**

Protocol parameters

Protocol	Modbus RTU	▼
Mode of Connected device	Slave	▼
Broadcast	On	▼
Response timeout (ms)	300	⬆ ⬇ ⬇ ⬆
Response target mode	TARGET	▼
Response target IP	0.0.0.0	

- **Response timeout**

Number { 0 – 8190}, default = 300

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

7.1.3.3.8. PR2000

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

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

Protocol parameters

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

7.1.3.3.9. Siemens 3964(R)

The 3964 protocol is utilized by the Siemens Company as a Point-to-Point connection between two controllers. Meanwhile it has developed into an industry standard that can be found on many devices as a universal communications interface. 3964R is the same as 3964, in addition it only uses BCC

(Block Check Character). 3964(R) handles only the link layer (L2 in OSI model), hence RipEX uses a similar way to read "SCADA address" as in UNI protocol.

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

Communication goes as follows:

LocalRTU -> STX -> LocalRipEX

LocalRipEX -> DLE -> LocalRTU

LocalRTU -> DATA+DLE+ETX+BCC -> LocalRipEX

LocalRipEX -> DATA -> RemoteRipEX*

LocalRipEX -> DLE -> LocalRTU

RemoteRipEX -> STX -> RemoteRTU

RemoteRTU -> DLE -> RemoteRipEX

RemoteRipEX -> DATA+DLE+ETX+BCC -> RemoteRTU

RemoteRTU -> DLE -> RemoteRipEX

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

- **Master**

Protocol parameters

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

- **Address mode**

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

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

- **Address position**

Specify the sequence number of the byte, where the Protocol address starts.

**Note**

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

**Note**

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

• Slave**Protocol parameters**

Protocol	3964R	▼
Mode of Connected Device	Slave	▼
Broadcast	On	▼
DLE timeout [ms]	1000	⬆ ⬇ ⬈ ⬇ ⬆
Retries	3	⬆ ⬇ ⬈ ⬇ ⬆
Priority	High	▼
BCL	On	▼
Response target mode	TARGET	▼
Response target IP	0.0.0.0	

○ DLE timeout [ms]

Number {300 – 8190}, default = 1000

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

○ Retries [No]

Number {0 – 7}, default = 3

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

○ Priority

List box {Low; High}, default = "Low"

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

**Note**

Obviously, two pieces of equipment which are communicating together must be set so that one has High priority and the other has Low.

- **BCC**

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

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

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

7.1.3.3.10. RDS

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

The screenshot shows a 'Protocol parameters' window with the following settings:

- Protocol: RDS
- ACK: On
- ACK timeout [ms]: 1000
- Repeats: 3
- Reverse mode: Off
- Address translation: Mask
- Base IP / Mask: 10.0.0.1/24
- Destination (UDP port): COM1

- **ACK**

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

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

- **ACK timeout [ms]**

Number {0 – 16383}, default = 1000

**Note**

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

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

- **Repeats**

Number {0 – 31}, default = 3

Number of frame re-transmissions.

- **Reverse mode** (will be available in a future FW release)

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

If a frame is going to be transmitted over a wire channel, source and destination addresses in the frame must be reversed.

- **Reverse address (Hex)**

HEX number {0x00 – 0xFF}, default = 00

When Reverse mode is enabled, the frame destination address is overwritten by the Reverse address. It takes place after the frame reception from the wire channel before it is transmitted to the air channel. This only happens if the Reverse mode is enabled.

7.1.3.3.11. UNI

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

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

Protocol parameters

Protocol: UNI

Mode of Connected device: Master

Address mode: Binary (1B)

Address position: 1

Poll response control: Off

Broadcast: On

Broadcast address: 255

Address translation: Mask

Base IP / Mask: 10.0.0.1/24

Destination (UDP port): COM1

- **Mode of Connected device**

Listbox: {Master, Slave}, default = Master

- **Address mode**

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

Protocol address format and length (in Bytes). The ASCII 2-Byte format is read as 2-character hexadecimal representation of one-byte value. E.g. ASCII characters AB are read as 0xAB hex (10101011 binary, 171 decimal) value (the ASCII-2-Byte format function will be available in a future FW release).

- **Address position**

Number {1 – 255}, default = 1

Specify the sequence number of the byte, where the Protocol address starts. Note that the first byte in the packet has the sequence number 1, not 0

- **Poll response control**

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

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



Note

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

"Off" – The Master does not check packets incoming from the RF channel - all packets are passed to the application, including broadcasts. That allows e.g. spontaneous packets to be generated at

remote sites. This mode is suitable for Master-Master communication scheme or a combination of the UNI and ASYNC LINK protocols.

- **Mode of Connected device: SLAVE**



Mode of Connected device	Slave	▼
Broadcast	On	▼

- **Accept broadcasts**

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

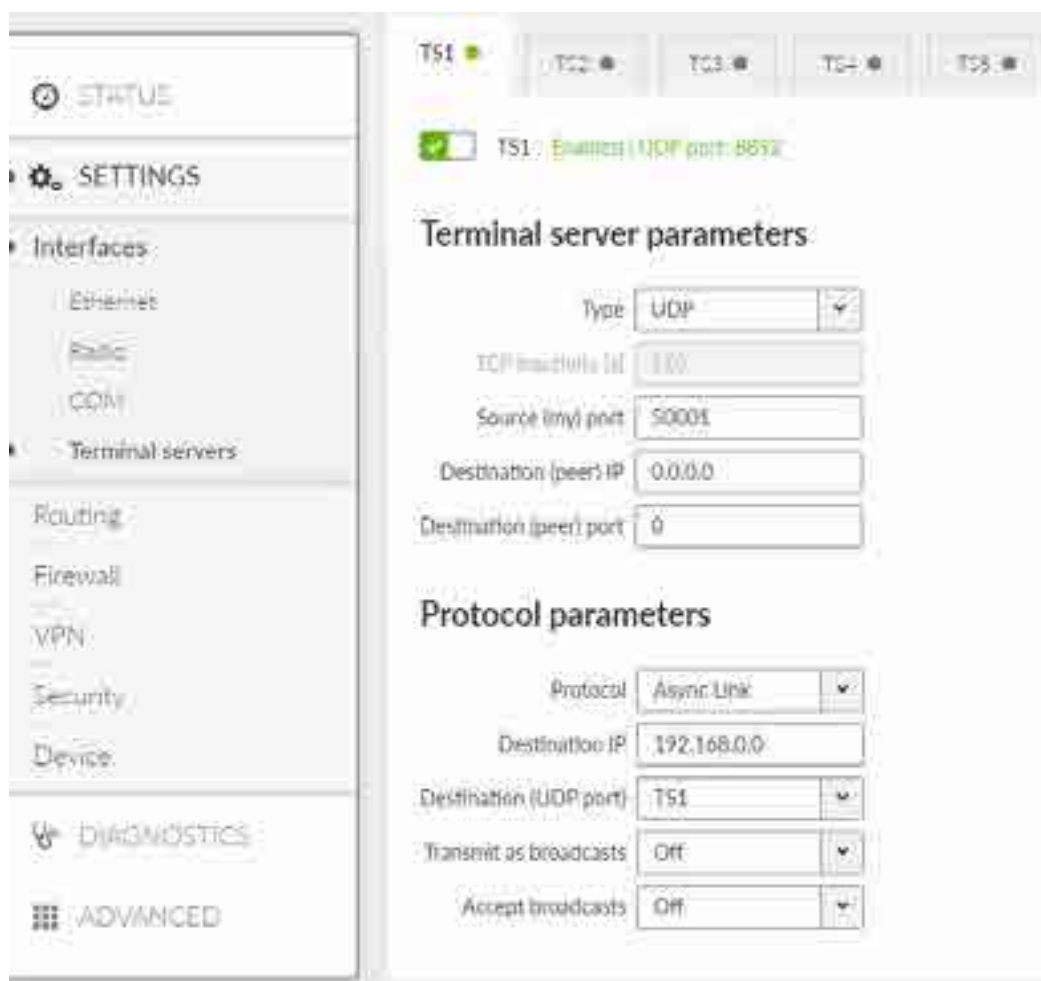
"On" – Broadcast packets received at the radio channel are forwarded to the COM port.

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

7.1.4. Terminal servers

Generally, a Terminal Server (also referred to as a Serial Server) enables connection of devices with serial interface to a RipEX2 over the local area network (LAN). It is a virtual substitute for devices used as serial-to-TCP(UDP) converters.

In some special cases, the Terminal server can be also used for reducing the network load from applications using TCP. A TCP session can be terminated locally at the Terminal server in RipEX2, user data extracted from TCP messages and processed like it comes from a COM port. When data reaches the destination RipEX2, it can be transferred to the RTU either via a serial interface or via TCP (UDP), using the Terminal server again.



Up to 5 independent Terminal servers can be set up. Each one can be either TCP or UDP Type, **TCP Inactivity** is the timeout in seconds for which the TCP socket in RipEX2 is kept active after the last data reception or transmission. As source IP address of a Terminal server will be used the IP address of the RipEX2 ETH interface (**Local preferred source address** if exists see *Section 7.2.1, “Static”*), **Source (my) port** can be set as required. **Destination (peer) IP** and **Destination (peer) port** values belong to the locally connected application (e.g. a virtual serial interface). In some cases, applications dynamically change the IP port with each datagram. In such a case set Destination port=0. RipEX2 will then send replies to the port from which the last response was received. This feature allows to extend the number of simultaneously opened TCP connections between a RipEX2 and locally connected application to any value up to 10 on each Terminal server. **Protocol** follows the same principles as a protocol on COM interface.



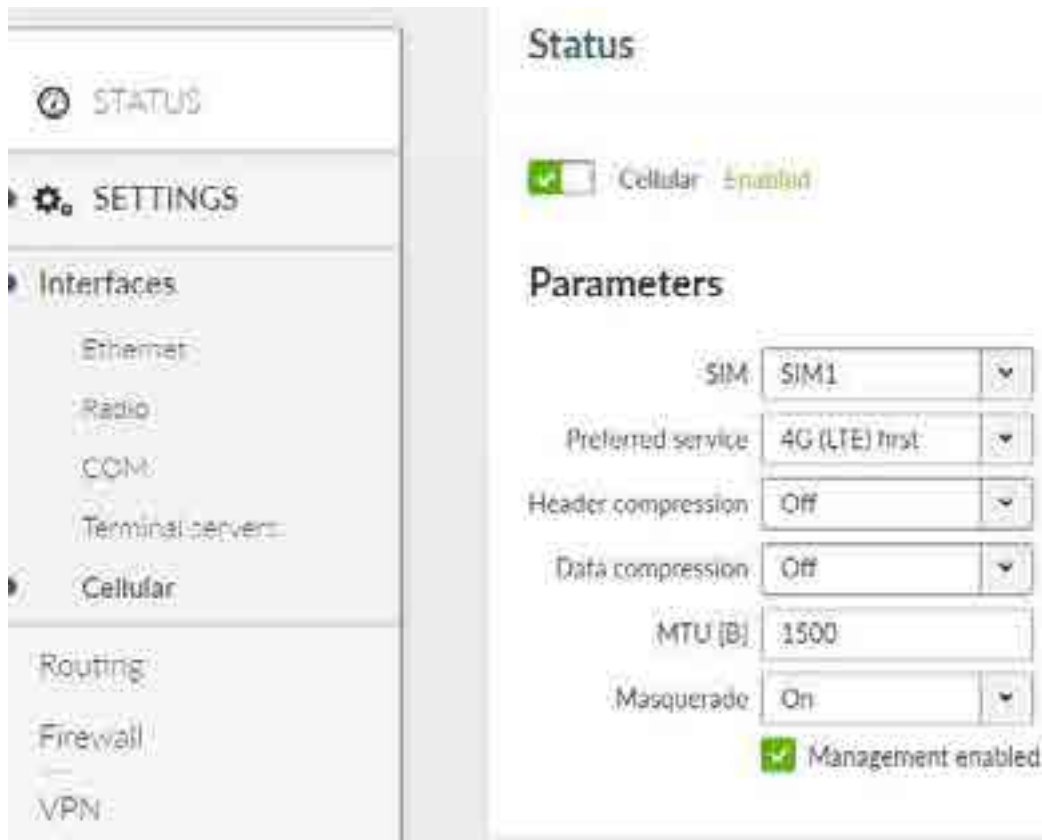
Note

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

7.1.5. Cellular

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

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



- **Enable / Disable:** enables / disables the cellular WWAN connection. When disabled, the module power is off.
- **SIM**
List box {SIM1; SIM2}, default = "SIM1"

Active SIM card selection.
- **Preferred service**
List box {2G (GSM) first; 2G (GSM) only; 3G (UMTS) first; 3G (UMTS) only; 2G/3G (GSM/UMTS) only; 4G (LTE) first; 4G (LTE) only; 3G/4G (UMTS/LTE) only}, default = "4G (LTE) first"

Sets preferences and/or permission of the individual cellular network services. Sets preferences and/or permission of the individual cellular network services.
- **Header compression**
List box {On; Off}, default = "Off"

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

Enables / disables the user data traffic data compression. Not used with 4G service.
- **MTU [B]**
Number {70 – 1500}, default = 1500

Outgoing packets MTU.

- **Masquerade**

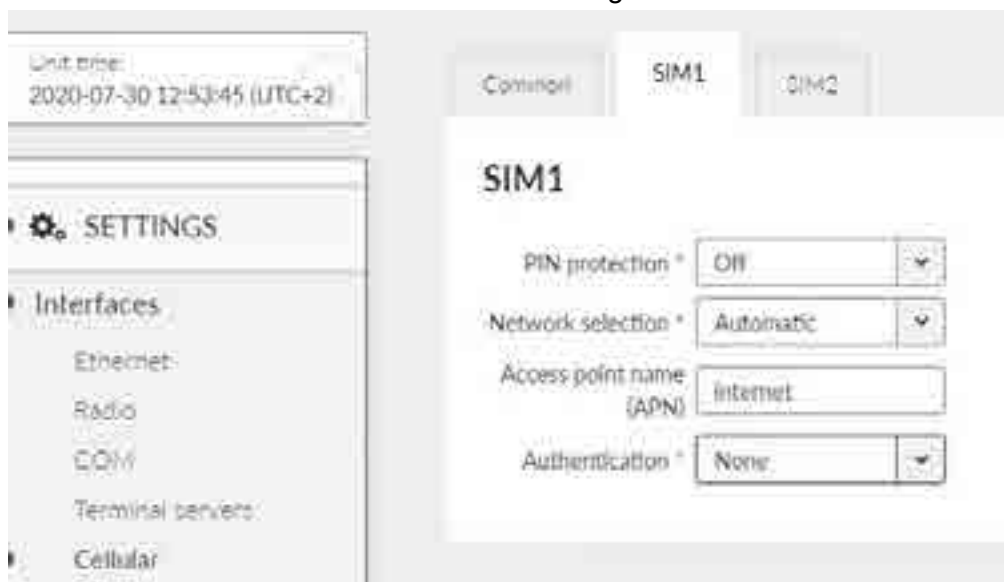
List box {On; Off}, default = "On"

Enables / disables SNAT (MASQUERADE) for the packets outgoing to the WWAN interface.

When on, the source address of packets outgoing via the cellular WWAN interface will be changed to the address assigned to this interface. Returning packets will be correctly routed to this interface.

- **Management enabled**

Enables / disables access into the unit's management via the cellular WWAN interface.



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

- **PIN protection**

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

Enables / disables the SIM module PIN protection. It has to be switched on if the PIN is required. The parameter is ignored if the SIM does not require a PIN.

- **PIN code**

String {0000 – 9999}, default = 0000

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

- **Network selection**

List box {Automatic; Prefer manual; Lock to manual; Lock to home}, default = "Automatic"

Defines the network selection preferences:

- **Automatic** – network is selected automatically.
- **Prefer manual** – the network according to the **Location area identity (LAI)** is preferred. Other network will be selected when the preferred network is not available.
- **Lock to manual** – the network according to the LAI can only be used.
- **Lock to home** – only the home network can be used (if the SIM supports PLMN reading).

- **Location area identity (LAI)**

String {00000 – 999999}, default = 00000

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

- **Access point name (APN)**

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

The APN for the access into the cellular network.

- **Authentication**

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

- **None** – no authentication is used for the APN access.
- **PAP (legacy)** –PAP (Password Authentication Protocol) authentication. We do not recommend to use this option because of security issues (the option is provided to offer legacy systems compatibility). Username and Password are required.
- **CHAP** – CHAP (Challenge-Handshake Authentication Protocol) authentication. Username and Password are required.

**Note**

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

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

7.2. Routing

RipEX router supports both static and dynamic IP routing.

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

7.2.1. Static

RipEX2 works as a standard IP router with multiple independent interfaces: Radio interface, Network interfaces (bridging physical Ethernet interfaces), COM ports, Terminal servers, optional Cellular interface etc. Each of the interfaces has its own IP addresses and Masks. All IP packets are processed according to the Routing table.

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

The COM ports are treated in the standard way as router devices, messages can be delivered to them as UDP datagrams to selected UDP port numbers. Destination IP address of COM port is either IP of a Network interface (bridging Ethernet interfaces) or IP of Radio interface. The IP address source of outgoing packets from COM ports is equal to IP address of interface (either Radio or Network interface) through which packet has been sent. The source address can also be assigned to **Local preferred**

source address value - see description below. Outgoing interface is determined in Routing table according to the destination IP.

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



- **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:

Static

Static routes

Static routes configuration interface showing two entries:

- Entry 1: Destination IP: 0.0.0.0, Active: ☒, Mask: 0, Mode: static, Gateway: 192.168.0.1/24, Local preferred source address: 0.0.0.0, Name: 0.0.0.0.
- Entry 2: Destination IP: 10.10.10.0, Active: ☒, Mask: 24, Mode: static, Gateway: 10.10.10.1, Local preferred source address: 0.0.0.0, Name: what you need.

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.

7.2.2. OSPF

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

7.2.2.1. Description

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

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

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

Routers in a specific area are always connected via interfaces.

- An address range can be defined for an interface where is the OSPF working. Multiple address ranges can be defined (behaving as another interface).
- Router to router interconnection can be protected by encryption with the password.”
- Specific “Cost” is defined for each interface which is added to metric ‘Type 1.’
- There are multiple types of interfaces:
 - **Stub** – interface only announces to OSPF: its presence and its address ranges to be propagated further to the network.

- **Broadcast** – to be used in the network where all the participants always hear each other (Ethernet). Designated Router (DR) and Backup DR (BDR) are setup between the neighbors. They are responsible for the update propagation (broadcast).
- **NBMA** (Non-Broadcast Multiple Access) – to be used in the network where only specific participants can communicate between each other; all the participants hear each other but multicast is not available. DR and BDR is setup.
- **Point2Point** – network having only two participants. They discover each other using multicast.
- **Point2Multipoint** – network where only predefined pairs of participants can hear each other (e.g. star topology); multicast is not available.
- Static rules can be defined. Such a routing rules are propagated to the network from this router.
- It is possible to define exported routing rules aggregation or specific routing rule hiding.
- It is possible to control the routing rules which are imported into the RipEX unit from the OSPF protocol and those that are exported into the OSPF protocol from the unit by using 'filters'.
 - Export filters – to control rules exported from the unit to the OSPF protocol which is propagating them further.
 - Import filters – to control rules imported from the OSPF into the unit.

7.2.2.2. Common - Common settings

- **Active**
List box {On; Off}, default = "Off"
Enables the dynamic routing and the OSPF protocol.
- **Router ID**
IP address, default = 0.0.0.0
RipEX unit acts in the OSPF network as a dynamic router. Every router is identified by an ID having the format of IP address. This IP address does not have to be 'real'.
Router ID is shared with the BGP protocol.
- **Instance ID**
Number {0 – 255}, default = 0
OSPF protocol instance number. This number is needed in case of running multiple OSPF protocols (for example on the border of 2 independent OSPF networks).

7.2.2.3. Network - Areas and interfaces - Areas

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

- **Active**
List box {On; Off}, default = "Off"
Enables / disables the area.
- **Area ID**
IP address, default = 0.0.0.0

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

- **Stub area**

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

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

- **Stub default GW**

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

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

- **Note**

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

7.2.2.4. Network - Areas and interfaces - Interfaces

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

- **Active**

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

Enables / disables the interface.

- **Interface**

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

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

- LAN – "if_" prefix must be used followed by Network interface name, e.g. "if_LAN-141"
- VLAN – "if_" prefix must be used followed by Network interface name, '.' dot and VLAN number, e.g. "if_LAN-141.29"
- Radio – "radio"
- Hot standby – "hstdby"
- GRE L3 – "gre_tunX" where 'X' is the tunnel number, starting from zero
- Cellular – "aux"

- **Network IP / Network mask**

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

- **Network type**

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

- **Cost**
Number {1 – 65535}, default = 10
The cost of traffic over this interface. The higher the Cost, the worse the path. It is added to OSPF metric 'Type 1'.
- **Hello interval**
Number {1 – 3600}, default = 10
Interval (in seconds) of sending Hello packets. The interval must be the same for the all participants of the given interface.
- **Poll interval**
Number {1 – 3600}, default = 20
Interval (in seconds) of sending Hello packets to inactive neighbors in the NMBA type of interface.
- **Retransmit interval**
Number {1 – 3600}, default = 5
Interval (in seconds) of repeating unacknowledged packets.
- **Dead count**
Number {2 – 64}, default = 4
Number of lost Hello packets from the neighbor to treat the connection as interrupted.
- **TTL security**
List box {On; Off}, default = "On"
Protection against OSPF packets spoofing.
- **Authentication, Password**
List box {None; Keyed MD5 (OSPFv2); HMAC SHA256; HMAC SHA384; HMAC SHA512}, default = "None"

Selection of a method to authenticate the OSPF messages. Password is used as a secret key for the selected hash function. Maximum length of the password is 128 characters.
- **Priority**
Number {0 – 255}, default = 1
Priority is used to select primary or backup router responsible for the routing updates propagation. The higher the number, the higher the priority. '0' states the router cannot be used as a primary or backup router.
- **Use broadcast**
List box {On; Off}, default = "Off"
Defines if OSPF packets distribution is provided using multicasts (default behavior) or broadcasts (nonstandard behavior).
- **Note**
Informational note. It is possible to enter some descriptive OSPF interface name. This value is used (when filled) instead of the original **Interface** identification as an **Interface** name in other configuration dialogs (e.g. Neighbors configuration).

7.2.2.5. Network - Areas and interfaces - Neighbors

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

- **Active**

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

- **Interface**

List box {list of existing OSPF interfaces}
OSPF interface the neighbor belongs to. The interface – **Note** value is used when defined. The interface – **Interface** value is used otherwise.

- **IP**

IP address of the neighbor.

- **Note**

Informational note

7.2.2.6. Network - Areas and interfaces - Networks

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

- **Active**

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

- **Area**

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

- **IP / mask**

IP address and mask of the range (i.e. network) which will be aggregated or hidden.

- **Action**

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

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

Example:

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

- **Note**

Informational note

7.2.2.7. Static rules

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

- **Active**

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

- **Destination IP / Destination mask**

IP address, default = 0.0.0.0/0

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

- **Metric type**

List box {Type 1; Type 2}, default = "Type 1"

Metric type of the routing rule. Metric 1 is added to the path cost. Metric 2 stays apart and compared to metric 1 is always bigger.

- **Metric**

Number {1 – 65535}, default = 1000

Routing rule metric value.

- **OSPF tag**

Number {0 – $2^{32}-1$ }, default = 0

OSPF tag is added to a rule at the moment of its insertion to the network. The tag travels through the OSPF without any modification so it can be used to distinguish the rule in the filters.

- **Note**

Informational note.

7.2.2.8. Import filter

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

- **Active**

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

Enables / disables the filter rule.

- **Filter network**

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

Method of the routing rule target range comparison.

- **Network IP / Network mask**

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

- **Mask from**

Number {0 – 32}, default = 0

- **Mask to**

Number {0 – 32}, default = 32

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

Examples:

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

- **Filter source**

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

- **Source**

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

Source types comments:

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

- **Filter OSPF tag**

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

- **OSPF tag**

Number {0 – 2³²-1}, default = 0
OSPF tag to be compared.

- **Action**

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

- **Set preference**

List box {On; Off}, default = "Off"
When enabled, the **Preference** (see next parameter) will be set to this rule.

- **Preference**

Number {0 – 65535}, default = 200
Routing rule preference in the routing table (to be used when **Set preference** is enabled). The higher the number the better the preference.

- **Local preferred source address**

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

- **Note**

Informational note

7.2.2.9. Export filter

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

- **Active**

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

- **Note**

Informational note

- **Filter network**

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

Selects a method of the routing rule destination range comparison.

- **Network IP / Network mask**

IP address, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared

- **Mask from**

Number {0 – 32}, default = 0

- **Mask to**

Number {0 – 32}, default = 32

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

- **Filter protocol**

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

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

- **Protocol**

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

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

- **Filter BGP path**

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

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

- **Action**

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

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

7.2.3. BGP

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

7.2.3.1. Description

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

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

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

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

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

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

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

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

- Import IGP filter – controls which of the routing rules from the BGP are accepted to the dynamic routing table and how
- Export IGP filter – controls which of the routing rules from the dynamic routing table are exported to the BGP and how
- Import OUT filter – controls which of the routing rules from the other AS are accepted to the BGP and how
- Export OUT filter – controls which of the routing rules are exported from the BGP to other AS and how
- Routing rules passed on between iBGP and BGP tables are not filtered

7.2.3.2. Common - Common settings

- **Active**
List box {On; Off}, default = "Off"
Enables the dynamic routing and the BGP protocol.
- **Router ID**
IP address, default = 0.0.0.0
RipEX unit acts in the BGP network as a dynamic router. Every router is identified by an ID having the format of an IP address. This IP address does not have to be 'real'.
Router ID is shared with the OSPF protocol.
- **Local AS**
Number $\{0 - 2^{32}-1\}$, default = 65000
Local Autonomous System identification number. AS numbers are assigned by IANA. Part of the range is reserved for private network usage: 64512 – 65534 and 4200000000 – 4294967294. AS numbers from this range can be safely used by anyone.
- **Preference**
Number $\{0 - 2^{32}-1\}$, default = 100
Router preference within the local AS. The higher the number, the higher the preference.
- **MED (Multi-Exit Discriminator)**
List box {Off; Static; OSPF metric 1}, default = "Off"

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

- **Static MED**

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

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

- **Route reflector**

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

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

- **Cluster ID type**

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

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

- **Cluster ID**

IP address, default = 0.0.0.0

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

7.2.3.3. Neighbors

Neighboring BGP routers. Maximum number of neighbors is 256.

- **Active**

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

Enables the specific neighbor.

- **Note**

Informational note.

- **Neighbor type**

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

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

- **Neighbor AS**

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

Neighbor AS number.

- **Neighbor IP**

IP address, default = 0.0.0.0

Neighbor router IP address.

- **Local IP of the connection**

IP address, default = 0.0.0.0

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

- **Neighbor connection**

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

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

- **MD5 authentication**

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

Enables BGP packets authentication using TCP MD5 Signature extension.

- **Password**

String {up to 128 char}

Password for the **MD5 authentication**.

- **Passive**

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

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

- **Hold interval [s]**

Number {3 – 10800}, default = 240

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

- **Keepalive interval [s]**

Number {1 – 3600}, default = 80

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

- **Connection retry interval [s]**

Number {1 – 3600}, default = 120

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

- **TTL security**

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

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

- **Expected hops**

Number {2 – 32}, default = 2

Number of expected hops between the neighbors

- **Route reflector client**

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

Defines if this neighbor is a client of this (this unit) Route reflector.

- **Set cost**

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

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

- **Cost**

Number $\{0 - 2^{32}-1\}$, default = 10

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

- **Next hop self**

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

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

7.2.3.4. Static rules

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

- **Active**

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

Enables / disables the static routing rule.

- **Destination IP / Destination mask**

IP address, default = 0.0.0.0/32

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

- **Note**

Informational note.

7.2.3.5. Import IGP filter

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

- **Filter policy**

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

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

- **Active**

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

Enables / disables the filter rule.

- **Note**

Informational note.

- **Filter network**

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

Selects a method of the routing rule destination range comparison.

- **Network IP / Network mask**

IP address, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared

- **Mask from**

Number $\{0 - 32\}$, default = 0

- **Mask to**

Number {0 – 32}, default = 32

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

- **Filter source**

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

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

- **Filter BGP path**

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

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

- **Path position**

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

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

- **Path AS**

Number {0 – $2^{32}-1$ }, default = 65000

The number of the AS searched for.

- **Action**

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

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

- **Set preference**

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

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

- **Preference**

Number {0 – 65535}, default = 100

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

- **Local preferred source address**

IP address, default = 0.0.0.0

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

7.2.3.6. Export IGP filter

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

- **Filter policy**

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

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

- **Active**

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

Enables / disables the filter rule.

- **Note**
Informational note
- **Filter network**
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.
- **Network IP / Network mask**
IP address, default = 0.0.0.0/0
IP address and mask defines the network prefix to be compared
- **Mask from**
Number {0 – 32}, default = 0
- **Mask to**
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.
- **Filter protocol**
List box {Off; Match; Not match}, default = "Off"
Selects the way how the routing rule source protocol is compared.
- **Protocol**
List box {System; OSPF}, default = "System"
Selection of the protocol origin. "System" – stands for rules from the ordinary routing table. "OSPF" stands for rules from the OSPF protocol.
- **Filter OSPF source**
List box {Off; Match; Not match}, default = "Off"
Selects the OSPF routing rule source comparison mode.
- **OSPF source**
List box {Internal; Inter-area; External type 1; External type 2}, default = "External type 2"
OSPF sources. "Internal" – stands for internally generated rule (e.g. interface range). "Inter-area" – stands for rule generated on the area borders.
- **Filter OSPF tag**
List box {Off; Match; Not match}, default = "Off"
Selects the way of filtering based on OSPF tag.
- **OSPF tag**
Number {0 – $2^{32}-1$ }, default = 0
OSPF tag to be compared. The tag is added to a rule when inserted to OSPF.
- **Action**
List box {Accept; Reject; Pass}, default = "Accept"
Defines what action is taken on the routing rule. "Pass" continues in processing.

7.2.3.7. Import OUT rules

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

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

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

- **Filter limit**

Number {1 – 65535}, default = 1024

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

- **Active**

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

Enables / disables the filter rule.

- **Note**

Informational note.

- **Filter network**

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

Selects a method of the routing rule destination range comparison.

- **Network IP / Network mask**

IP address, default = 0.0.0.0/0

IP address and mask defines the network prefix to be compared

- **Mask from**

Number {0 – 32}, default = 0

- **Mask to**

Number {0 – 32}, default = 32

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

- **Filter BGP path**

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

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

- **Path position**

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

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

- **Path AS**

Number {0 – $2^{32}-1$ }, default = 65000

The number of the AS searched for.

- **Action**

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

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

- **Prepend local AS**

Number {0 – 8}, default = 0

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

7.2.3.8. Export OUT filter

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

- **Filter policy**
List box {Accept; Reject}, default = "Accept"
Defines what action is taken on the routing rules which were not captured (i.e. fallback) in the **Export OUT filter**.
- **Active**
List box {On; Off}, default = "On"
Enables / disables the filter rule.
- **Note**
Informational note.
- **Filter network**
List box {Off; Match; Not match}, default = "Off"
Selects a method of the routing rule destination range comparison.
- **Network IP / Network mask**
List box {Off; Match; Not match}, default = "Off"
IP address and mask defines the network prefix to be compared
- **Mask from**
Number {0 – 32}, default = 0
- **Mask to**
Number {0 – 32}, default = 32
Definition of the enabled range of the mask length of the processed routing rule.
- **Filter protocol**
List box {Off; Match; Not match}, default = "Off"
Selects the way how the routing rule source protocol is compared.
- **Protocol**
List box {System; OSPF; BGP; BGP external; BGP internal}, default = "System"
Selection of the protocol origin. "System" – stands for rules from the ordinary routing table.
- **Filter OSPF tag**
List box {Off; Match; Not match}, default = "Off"
Selects the way of filtering based on OSPF tag.
- **OSPF tag**
Number {0 – $2^{32}-1$ }, default = 0
OSPF tag to be compared. The tag is added to a rule when inserted to OSPF.
- **Filter BGP path**
List box {Off; Is empty; Not empty; Contain; Not contain}, default = "Off"
Filtering based on the BGP Path (routing rule path over different AS). "Is empty" – defines an empty path (routing rule from the local AS). "Contain" – defines paths containing specific AS.
- **Path position**
List box {Any; Neighbor; Source}, default = "Any"

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

- **Path AS**

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

The number of the AS searched for.

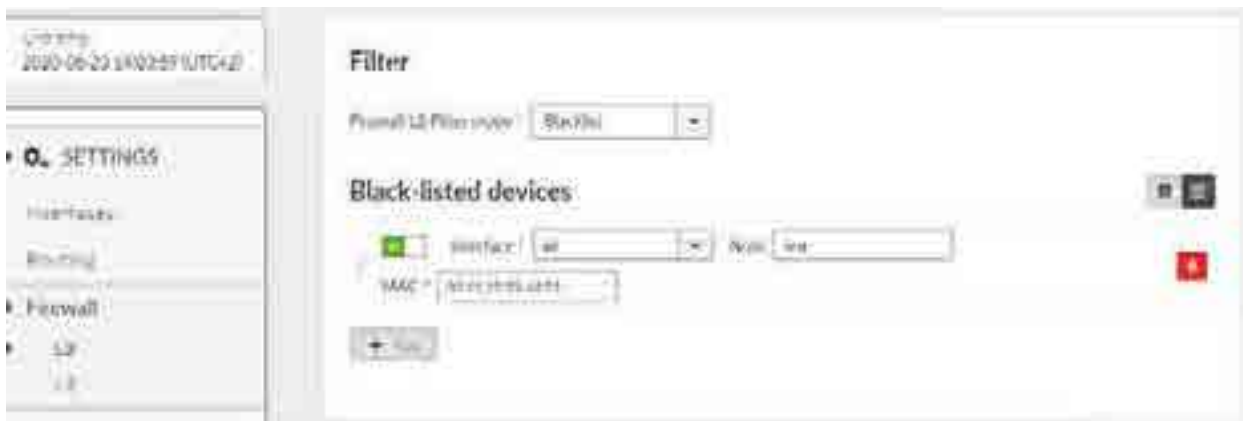
- **Action**

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

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

7.3. Firewall

7.3.1. Firewall L2



- **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.

- **Active**

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

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

- **Interface**

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

- **MAC**

IPv4 MAC address

7.3.2. Firewall 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}, default = "All"
- **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}, default = "All"
- **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}, default = "All"
- **Connection state New**
List box {Off; On}, default = "Off" - 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}, default = "Off" - 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} default = "Off", 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 units 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.

7.4. VPN

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

7.4.1. IPsec

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

Although there are 2 modes of operation 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).
- If 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).

Edit IPsec VPN tunnel configuration

Note: 1st tunnel

Start state: Passive

MOBIKE: On

Dead Peer Detection: Off

Phase 1 - IKE

IKE version: IKEv2

Authentication method: PSK

Encryption algorithm: AES192

Authentication algorithm: SHA256

Diffie-Hellman group (PFS): Group 15 (MODP)

Reauthentication: Off

SA lifetime (s): 14400

Phase 2 - IPsec

Encryption algorithm: AES256

Authentication algorithm: SHA512

Diffie-Hellman group (PFS): Group 20 (ECP384)

Payload compression: On

SA lifetime (s): 3600

PSK

Passphrase: abcd

Mode: Passphrase

Confirm and Close

- **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]**

Number {180 – 86400}, default = 14400 s (4 hours)

Time of SA validity. The new key exchange or re-authentication is triggered immediately the key expires. The true time of expiration is randomly selected within the range of 90-110%, 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]**

Number {180 – 86400}, default = 3600 s (1 hour)

Time of CHILD SA validity. The new key exchange or re-authentication is triggered immediately the key expires. The true time of expiration is randomly selected within the range of 90-110%, 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**

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.

7.4.1.1. Advanced menu

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

IPsec

Active

Make-before-break

IPsec associations

Encryption algorithm

Authentication method

Reauthentication Peer ID

DPD action Encryption algorithm

Authentication algorithm

Payload compression MOBIKE

Authentication algorithm

DPD period [s] Dead Peer Detection

SA lifetime [s] Start state

Diffie-Hellman group (PFS) Active

Note SA lifetime [s]

Peer address IKE version

TFC padding

Diffie-Hellman group (PFS) Local ID

 Add

Passphrases/Keys

Traffic selectors

- **DPD check period [s]**

Number {5 - 28800}, default = 30

Dead Peer Detection check period

- **DPD action**

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

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

- **Clear** – connection is closed and waiting
- **Hold** – connection is closed. Connection is established when first packet transmission through tunnel is attempted.
- **Restart** – connection is established immediately

7.4.2. GRE L2

GRE L2 tunnel is interconnected to the bridge (LAN interface) as one of the bridge's port, it captures Ethernet frames of the bridge and sends them to the other end of the tunnel. It enables to build bridge via the complex network and combine the local partial networks to one network.

GRE L2 tunnel can be used to tunnel the IPv6 traffic over the RipEX IPv4 network.



- **GRE L2 Enable** – switches all L2 tunnels On or Off

Individual L2 tunnels:

- **Enable** – enables actual L2 tunnel
- **Note** – Informational note
- **Peer address** – IP address of the equipment with the second end of the tunnel. This address is the expected source address of incoming GRE packets from the peer.
- **Network interface name** – has to be set as one of existing bridge's name in SETTING/Interfaces/Ethernet/ Network interface Name
- **Key enabled** – enables using key identification of the tunnel from/to the same peer
- **Key** – identification number of the tunnel
Number {0 – 4,294,967,295}, default = 0
- **MTU [B]** – MTU of the L2 tunnel.
Number {74 – 1500}, default = 1462

Overhead of the L2 tunnel is 38 B, so it should be GRE MTU = Path MTU - 38.

7.4.3. GRE L3

GRE L3 tunnel works as an additional unit's interface with its own IP address (and mask). The routing rules are used for sending packets to this interface. It bridges part of the network, so it seems to be one hop for the user traffic.



- **GRE L3 Enable** – switches all L3 tunnels On or Off

Individual L3 tunnels:

- **Enable** – enables actual L3 tunnel
- **Note** – Informational note
- **Peer address** – IP address of the equipment with the second end of the tunnel. This address is the expected source address of incoming GRE packets from the peer.
- **Tunnel address / Mask** – IP address and mask of the GRE tunnel interface
- **Key enabled** – enables using key identification of the tunnel from/to the same peer
- **Key** – identification number of the tunnel
Number {0 – 4,294,967,295}, default = 0
- **MTU** – MTU of the L2 tunnel.
Number {70 – 1476}, default = 1476

Overhead of the L3 tunnel is 24 B, so it should be GRE MTU = Path MTU - 24. If the MTU is bigger than is allowed along the route, the GRE packets will be discarded and ICMP report will be sent back to the source of the original packet (Path MTU discovery).

7.5. Security

User authentication is required to access RipEX unit management. There are two types of user authentication which differ in the user account location:

- Local authentication – user accounts are stored directly in the RipEX unit
- Remote authentication – user accounts are stored on a remote authentication server (RADIUS is implemented)

There are four different levels of user access privileges – they are bound with four different user access roles:

- **Guest (role_guest)**

Read only access for configuration parameters (except secured part of configuration). Diagnostics tools are available.

- **Technician (role_tech)**

All privileges of Guest role plus: write access for non-secured part of configuration.

- **Security technician (role_sectech)**

All privileges of Technician role plus: write access for secured part of configuration (except unit authentication related parts); unit firmware up/down-grade

- **Administrator (role_admin)**

No access level restrictions. All privileges of Security technician role plus: user accounts management; remote authentication configuration.

Limitations:

- At least one Administrator type of account must be defined in the unit.
- Maximal number of concurrently active sessions is 64. One user can have multiple sessions opened in the same time. If this limit is reached and a new session is to be opened, the oldest active session is deactivated and a new one is opened.
- Maximal number of Local user accounts (all roles together) is 100.

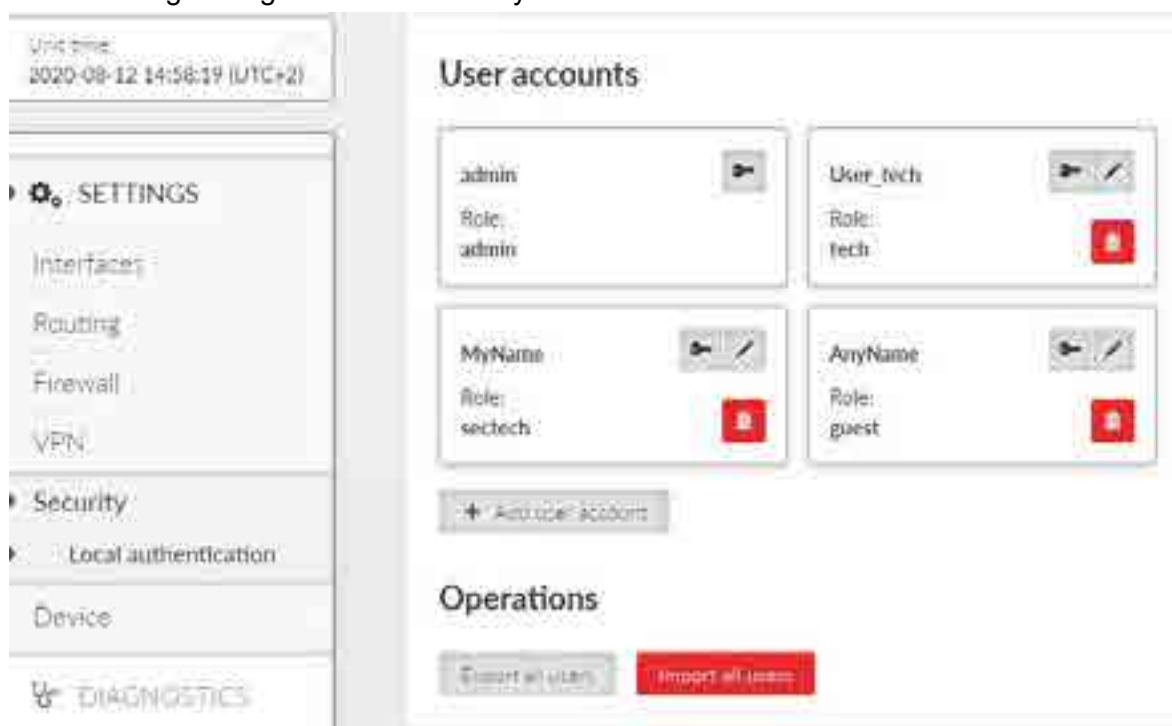


Note

The **Remote access** uses local identity and role of the user – there is no additional login to the remote unit (the login into local unit serves as login to the whole network).

7.5.1. Local authentication

The following settings are available only for user with the Administrator role.



Following user account parameters can be changed: password, user role. Any account (except the last one of Administrator role) can be deleted.

Export all users button provides backup of all Local user accounts into a file.

Import all user button provides restoration of all Local user accounts from a backup file. Active session is logged out automatically after this command.

+ **Add user account** button invokes new user account creation dialog:



- **Username**

String {1..128 char}, default = <empty>

New Username. Every username in the unit must be unique.

- **Password**

String {5..128 char}, default = <empty>

Password is stored in a secure way.

- **Role**

List box {Admin; Security Technician; Technician; Guest}, default = "Admin"



Note

It is highly recommended to create a new administrator type of account and delete the default "Admin" account.

Advanced feature

When the user account is not active for some time, the user will be automatically log-out. The inactivity timeout of the account is set for 1 day by default. It is possible to change in the range of 5 minutes up to 2 days (menu ADVANCED/Generic/UserAccess – **Web inactivity timeout**).



Note

It is necessary to install firmware version 1.4.5.0 or higher to assure proper functionality of Local and Remote authentication.

7.5.2. Remote authentication

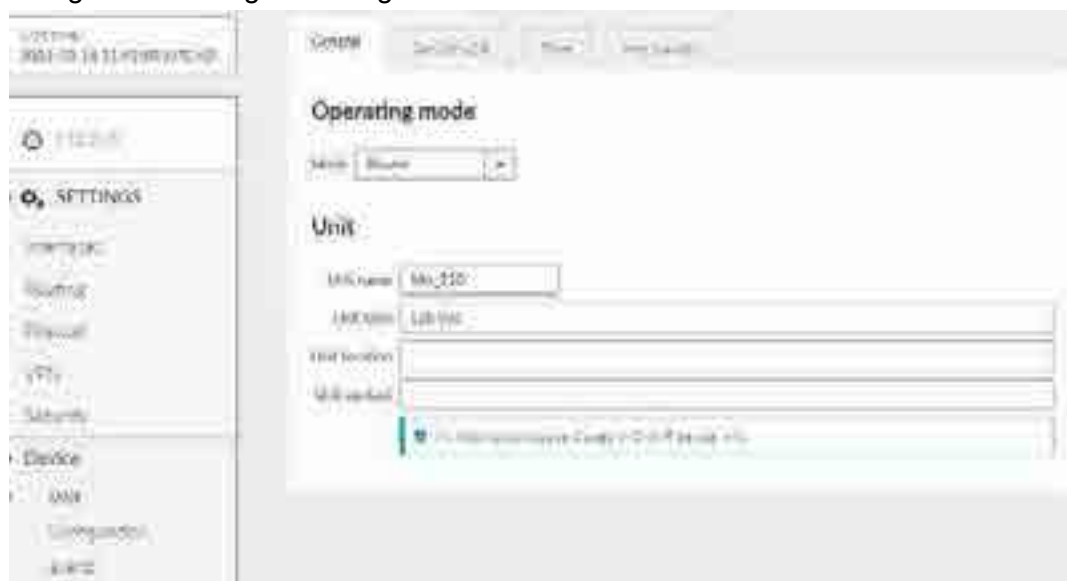
Settings of the remote authentication using RADIUS is available in ADVANCED/Security/RADIUS menu.

7.6. Device

7.6.1. Unit

7.6.1.1. General

The general settings affecting the whole unit.

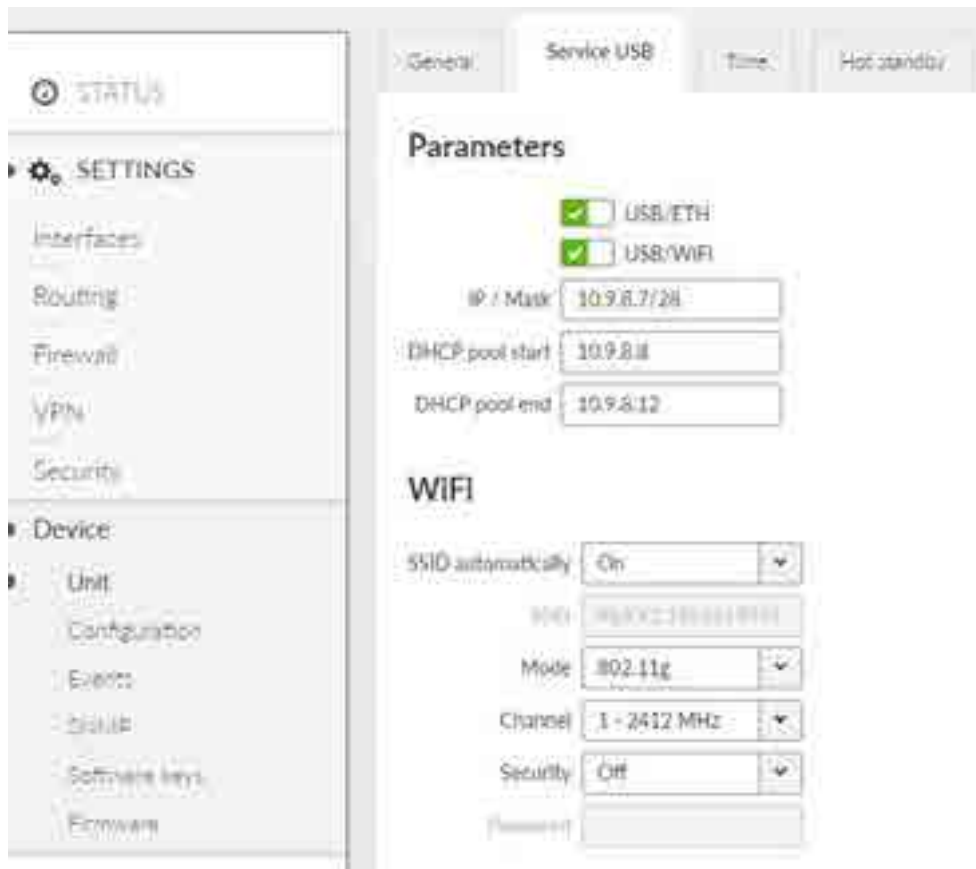


- **Mode**
List box {Bridge; Router}, default = "Bridge"
Selecting Bridge or Router mode affects many other parameters across the unit. See *Section 5.1, "Bridge mode"* and *Section 5.2, "Router mode"* for detailed description.
- **Unit name**
This name is used as a real name of the Linux router, so the allowed characters are strictly limited to:
_a..zA..Z0..9
- **Unit note**
Longer unit name without special characters restrictions.
- **Unit location, Unit contact**
Additional SNMP information. All the fields above are typically used in the NMS systems to identify the specific unit.

7.6.1.2. Service USB

The USB service interface primary purpose is to provide unit service and management access. Ethernet or WiFi connection can be established using an external ETH/USB or WiFi adapter. Please note that

only adapters listed in https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_ethusb can be used.



The DHCP server is running on this service interface to enable easier connection of the management device (PC, tablet or smart phone).

- **Enable / Disable**

Each of the ETH or WiFi service can be enabled or disabled separately. When the WiFi is enabled, the units acts as a WiFi Access Point (AP).

- **IP / Mask**

IP address of the DHCP server. This is the IP address to be used when accessing the unit management via this serial interface.

- **DHCP pool start**

Default = IP address of the DHCP server + 1

DHCP Server assigns addresses to connected clients starting from this address.

- **DHCP pool end**

DHCP server assigns IP addresses to connected clients in the range defined by **DHCP pool start** and **DHCP pool end** (inclusive).

- **WiFi**

WiFi AP parameters can be customized.

- **SSID automatically**

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

When automatic definition of SSID is enabled, the SSID contains unit Serial number.

- **SSID**

WiFi AP SSID. When entered manually, it must follow SSID naming conventions.

- **Mode**

List box {802.11g; 802.11g }, default = "802.11g "

WiFi AP mode.

- **Channel**

Selected WiFi channel.

- **Security**

List box {Off; WPA2-PSK}, default = "Off"

It is a good practice to use WPA2-PSK secured connection together with a strong password. It is highly recommended in case of permanent WiFi adapter installation.

7.6.1.3. Time

Unit Event time stamps, unit Statistics records and unit internal logs are using Unit time. It is good practice to keep the Unit time synchronized to ease unit and network diagnostics.

Unit time can be setup manually or it can be synchronized with an NTP server. NTP server synchronization is recommended.

The unit itself serves as an NTP server providing the time synchronization to another IP clients. If no NTP server is defined or no one is available, the unit runs in an "orphan" mode. The unit internal NTP server Stratum is set to 8 in this case. If the unit is synchronized with an NTP server, the unit NTP server Stratum is set a 1 higher comparing to Stratum of the NTP server providing the time synchronization to the unit.

If the unit is synchronized to a time source and the unit (synchronized) time differs from the unit RTC time (by more than 8 seconds), the RTC time is updated.



Note

Each unit can serve as NTP server for further IP equipment, this functionality is always on.

The screenshot shows the 'Time' configuration page. On the left is a sidebar with navigation links: STATUS, SETTINGS (selected), Interface, Routing, Firewall, VPN, Security, Service, Unit, Configuration, Events, DHCP, Software, and Firmware. Below these are sections for ANALYTICS and ADVANCED. The main content area has tabs for General, Service USB, Time (selected), and Hot Swapping. The 'Time' tab contains a 'Status' section showing NTP state as 'sync'd to server', stratum as '2', delay as '3.081', and dispersion as '166.290'. Below this is a 'Time' section with a 'Change device time manually' field set to '2021-09-16 13:50:38', an 'Update in device' button, and a 'Use browser time' checkbox. Further down are dropdowns for 'NTP client synchronization source' (set to 'NTP server'), 'NTP server minimum polling time' (set to '0.5 min.'), and 'Time zone' (set to 'Europe/Vienna'). At the bottom is an 'NTP servers' table with three entries, each with a status icon, a checkbox, an IP address, and a name.

Status	Checkbox	NTP server IP	Name
	☐	192.168.25.129	Secom Time Server
	☒	192.133.111.201	ELIUMTIME
	☒	192.133.111.201	ELIUMTIME

- **Status**

The Status field provides information about NTP synchronization status.

Refresh button is used to update the Status information.

- **Change device time manually**

This field is used to setup unit time manually.

- **Update in device**

Sets the given time to the unit.

- **Use browser time checkbox**

Permanently updates the Change device time manually field to minimize the delay between the time input and the moment of time setup.

- **NTP client synchronization source**

Synchronization source of the NTP client. The only option “NTP server” is implemented at this firmware version.

- **NTP server minimum polling time**

Minimal period of the NTP server queries. NTP client is allowed to prolong this time in case of poor quality of the server or connection to the server.

- **Time zone**

Time zone to represent unit internal time. All the unit timestamps are displayed using this time zone. Changing the time zone does not affect unit internal records – they are always recorded using UTC time zone.

- **NTP servers**

Multiple NTP servers can be configured to get more precise time synchronization or to have a backup solution in case of an individual NTP server unavailability. Maximum number of records in the list is 32. The unit runs in an “orphan” mode if the **NTP client synchronization source** is set to “NTP server” and there is no NTP server defined in this list.

7.6.1.4. Hot standby

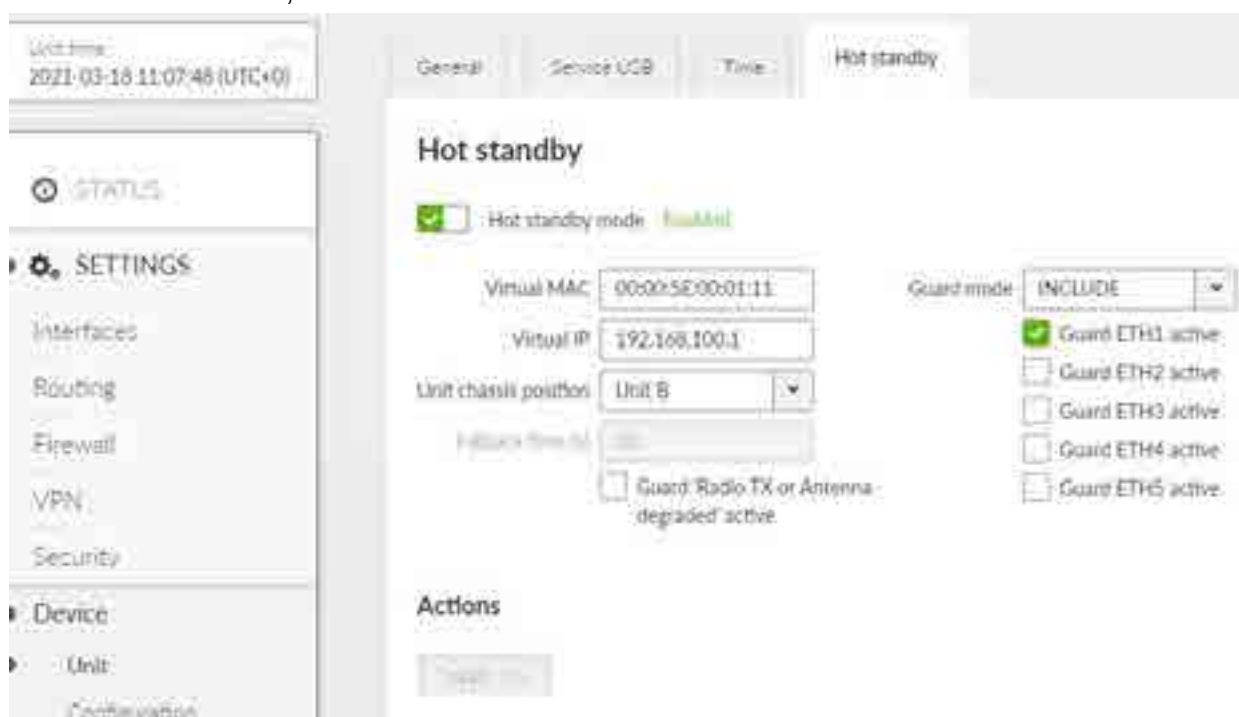
7.6.1.4.1. Hot standby settings

Following settings is supported by the controller version of the RipEX2-HS , where the controller manages the active and passive/standby RipEX2 units and their accessing to the shared channels (e.g. radio).

The communication between individual RipEX2 units and HS controller use DI/DO interfaces, so other use of this interface is not possible.

The HW switch (mode selector) has to be set to AUTO position for switching between units, otherwise the selected unit remains active even if an error occurs on the selected one.

AUTO regime allows switching to the standby unit when an error status occur in active unit – if both units are without alarms, the A unit will be active.



- **Hot standby mode enabled**

Listbox {On; Off }, default = "Off"
Switches Hot Standby functionality.

- **Virtual MAC**

MAC address of shared LAN interface. It should be same for both individual RipEX2 units. This MAC address has to differ from other MAC addresses used in unit. It is possible to use e.g. VRRP type of addresses: 00:00:5E:00:01:XX.

To prevent a collision with broadcast addresses (in case of Flexible protocol usage), the address must not be ended with :FF:FF:FF.

- **Virtual IP**

This address has to fit into range of addresses used for the relevant network interface (e.g. ETH 1) and will be used as shared IP address for LAN interface. The radio address use used according to setting in SETTINGS/Interfaces/Radio/IP - the same address has to be set in both radio modems.

- **Unit chassis position**

Listbox {Unit A; Unit B}, default = "Unit B"

Position of the unit in HS chassis, set Unit A for unit in A position and vice versa.

- **Fallback time**

Time in seconds. The time delay to stay on the standby unit, after all alarms are solved.

- **Guard mode**

Listbox {INCLUDE; EXCLUDE}, default = "INCLUDE"

Defines the behavior of guarding of ETH interfaces. INCLUDE requires all guarded lines in UP status – if one of these guarded lines is not in UP state, alarm occurs and the switching to the standby unit is executed.

- **Guard ETH1 .. ETH5 active**

Listbox {On; Off}, default = "Off"

Switches on guarding of the individual ETH link.

- **Toggle now**

This button allows to switch from unit Active status to the non-active.

It will not be possible if:

- The second unit is in alarm status.
- The HW MODE selector is not set to AUTO.
- The unit is in not-active status.



Note

It is possible to change the active status from the A to the B unit using shall command "**rrcmd rrhstdby web passivate**" and back from A to B using command "**rrcmd rrhstdby web activate**". Both units should be without errors for the SW sw itching.

7.6.1.4.2. Hot standby LAN interface settings

It is necessary to set LAN interface used for HS functionality.



The Range for virtual address parameter is in this menu available only when HS functionality in the menu SETTINGS/Device/Unit/Hot standby is enabled (see above).

The parameter Range for virtual address has to be set to On for the LAN address interconnected with shared ETH interface (Range for virtual address set to On).

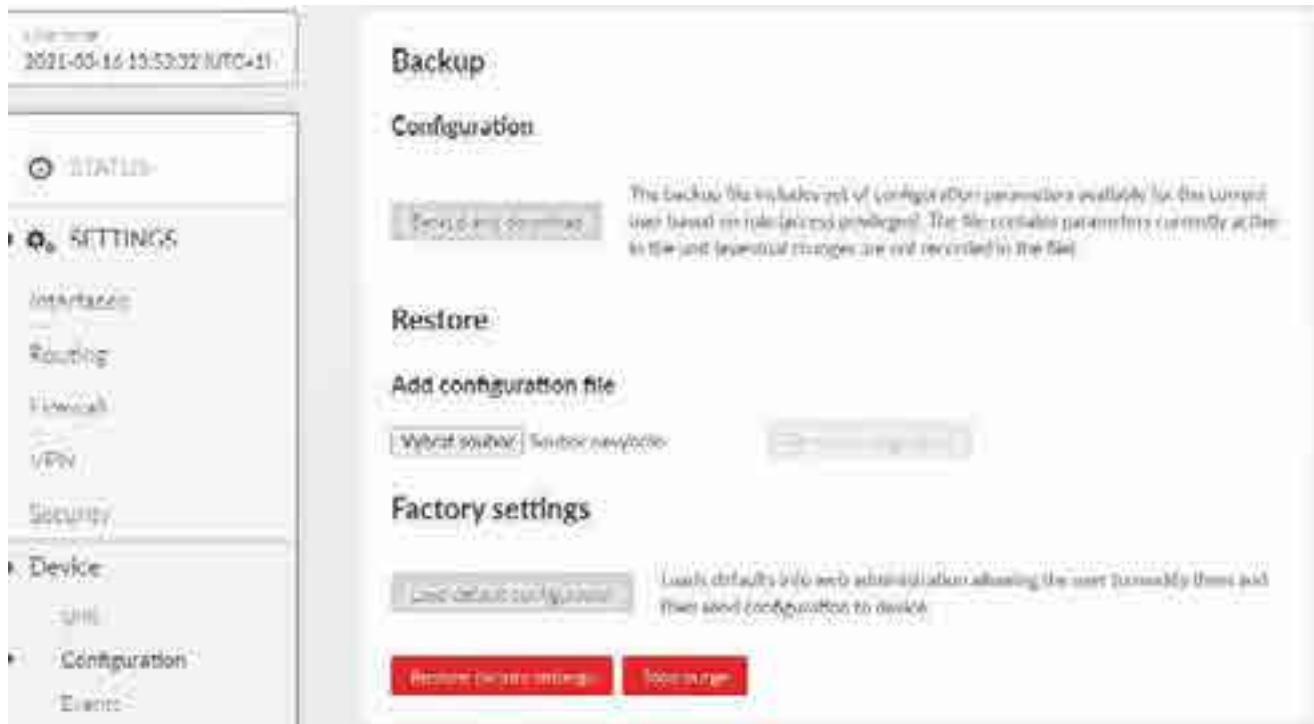


Note

Interconnected ETH interface IP addresses of both ETH addresses should be different as well as addresses of A and B units, yet in the same range as the virtual shared address (= together three different addresses in the same range).

7.6.2. Configuration

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



- **Restore factory settings**

Restores all configuration parameters to default setup (including monitoring settings)

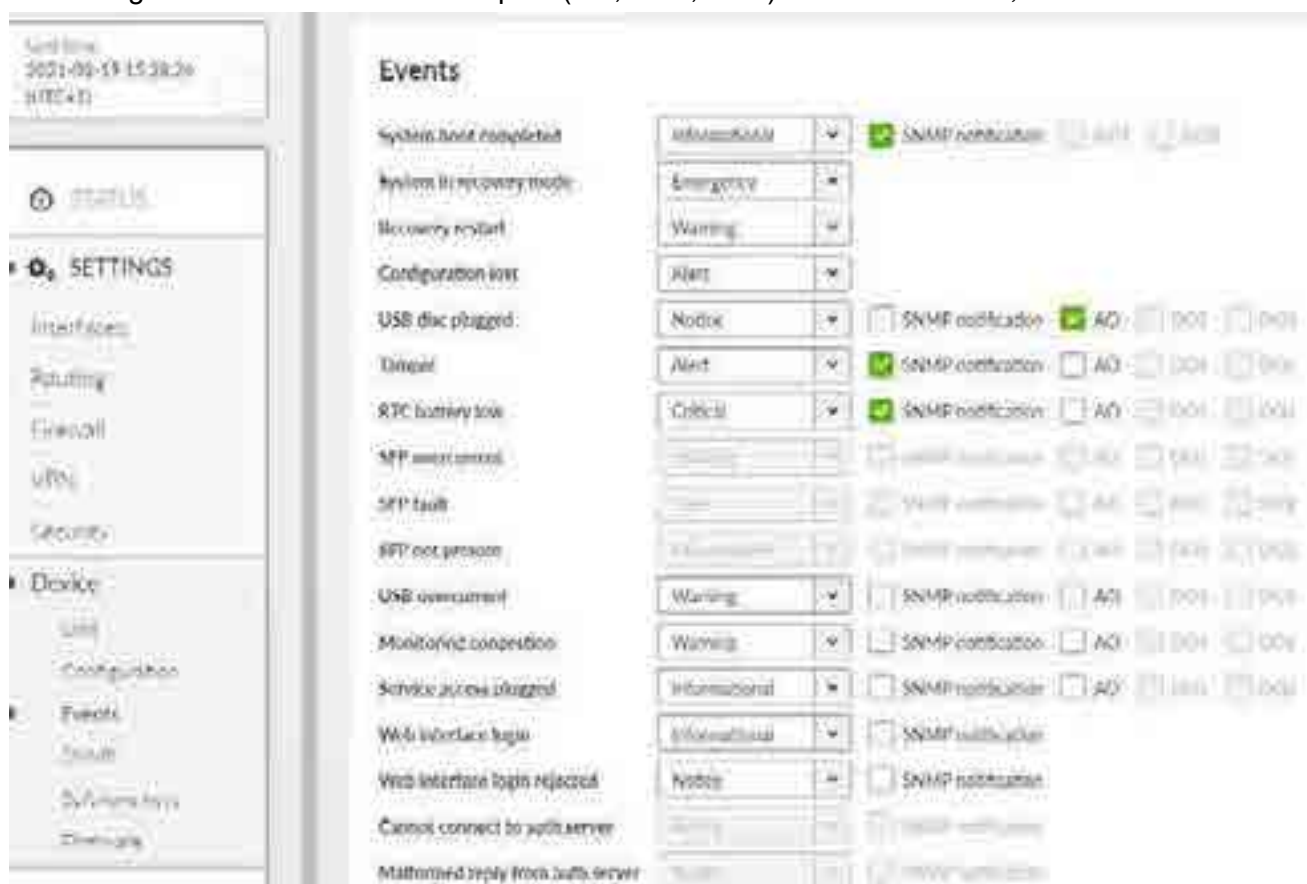
Deletes user database (only default user "admin" with default password will remain). Logout from station will apply.

- **Total purge**

Deletes completely all diagnostic

7.6.3. Events

Settings of the severities of the individual events. Some events can generate SNMP notification and can change level of the HW alarm outputs (AO, DO1, DO2) see *Section 2.2.2, “Power and Control”*.



7.6.4. SNMP

SNMP (Simple Network Management Protocol) implementation in RipEX provides three SNMP versions: v1, v2c and v3.

The screenshot shows the 'Settings' page of a device. The left sidebar contains a navigation menu with options like 'General', 'v1/v2c', 'v3', 'Notification', and 'Notification destinations'. The main content area is divided into several sections:

- General:** Includes a 'SNMP mode' dropdown menu set to 'v1_v2c_v3'.
- v1/v2c:** Includes a 'Community name' text input field with the value 'public'.
- v3:** Includes several fields for configuration: 'Security user name' (set to 'admin'), 'Security level' (set to 'AuthPriv'), 'Authentication algorithm' (set to 'SHA1'), 'Authentication password' (set to '123456'), 'Authentication password' (set to '123456'), 'Authentication password' (set to '123456'), 'Authentication password' (set to '123456'), and 'Authentication password' (set to '123456').
- Notification:** Includes fields for 'Authentication' (set to 'v3auth'), 'Authentication' (set to 'v3auth'), 'Authentication' (set to 'v3auth'), and 'Authentication' (set to 'v3auth').
- Notification destinations:** Includes a table with columns for 'Destination ID', 'Destination name', and 'Destination type'. The table is currently empty.



Note

Following characters are prohibited in SNMP communication:
 " (Double quote) ` (Grave accent) \ (Backslash) \$ (Dollar symbol) ; (Semicolon)

- **SNMP mode**
 List box {Off; v1_v2c_v3; v3}, default = "Off"
 Enables the SNMP and defines which protocol versions are available.
- **Community name**
 String {1..32 char}, default = <public>
 Community name used by v1 and v2c
 When mode v1_v2c_v3 is used, this parameter is mandatory.

Version 3 settings

- **Security user name**
 String {1..32 char}, default = <empty>
 User name for SNMPv3. When v3 protocol is selected, this parameter is mandatory.
- **Security level**
 List box {NoAuthNoPriv; AuthNoPriv; AuthPriv}, default = "NoAuthNoPriv"

The v3 protocol security level. Switches on/off Authentication (Auth) and the SNMP data encryption (Priv).

- **Authentication**

List box {MD5_legacy; SHA1_legacy; SHA224; SHA256; SHA384; SHA512}, default = "SHA256"
Authentication algorithm. Legacy algorithms are not recommended to use, they are available for compatibility reasons only.

- **Authentication passphrase**

String {8..128 char}, default = <empty>
Passphrase used for authentication with SNMP server.

- **Encryption**

List box {DES_legacy; AES128; AES192; AES256}, default = "AES128"
Encryption algorithm.

- **Encryption passphrase**

String {8..128 char}
Passphrase used for data encryption when communicating with SNMP server.

- **Engine ID mode**

List box {Default; User defined}, default = "Default"
Engine Id serves for unique identification of the SNMP instance (i.e. the RipEX unit) according to RFC3411. When the "Default" Engine ID mode is selected the MAC address of the Eth1 interface is used for the unique part of the Engine Id (the whole Engine ID example: 800083130302a92006ef).

- **Engine ID**

String {1..27 char}
When "User defined" Engine ID mode is selected the differentiated part of the Engine ID can be entered as ASCII characters or generated (e.g. U3qPrisWoDYbBVNsAWluZYG3M5). This string is converted into HEX number (i.e. 55 33 71 50 72 69 73 57 6f 44 59 62 42 56 4e 73 41 57 6c 75 5a 59 47 4c 33 4d 35). The whole Engine ID for mentioned example: 800083130455337150726973576f44596242564e7341576c755a59474c334d35.

Notification

Notification is used for asynchronous notification from a RipEX unit into the SNMP server.

- **Notification mode**

List box {Off; Trap; Inform}, default = "Off"
Mode of notification; Inform is not supported by SNMPv1

- **Notification version**

List box {v1; v2c; v3}, default = "v2c"
Notification packets version.

- **Inform repeats**

Number {0 – 10}, default = 3
Number of repeats used when Inform acknowledge was not received.

- **Inform timeout [s]**

Number {1 – 20}, default 10
Inform acknowledge timeout.

Notification destinations

- **Destination IP**

IP address {0.0.0.0}, default 0.0.0.0

IP address of SNMP server receiving notification packets.

- **Destination port**

Number {1 – 65535}, default = 162

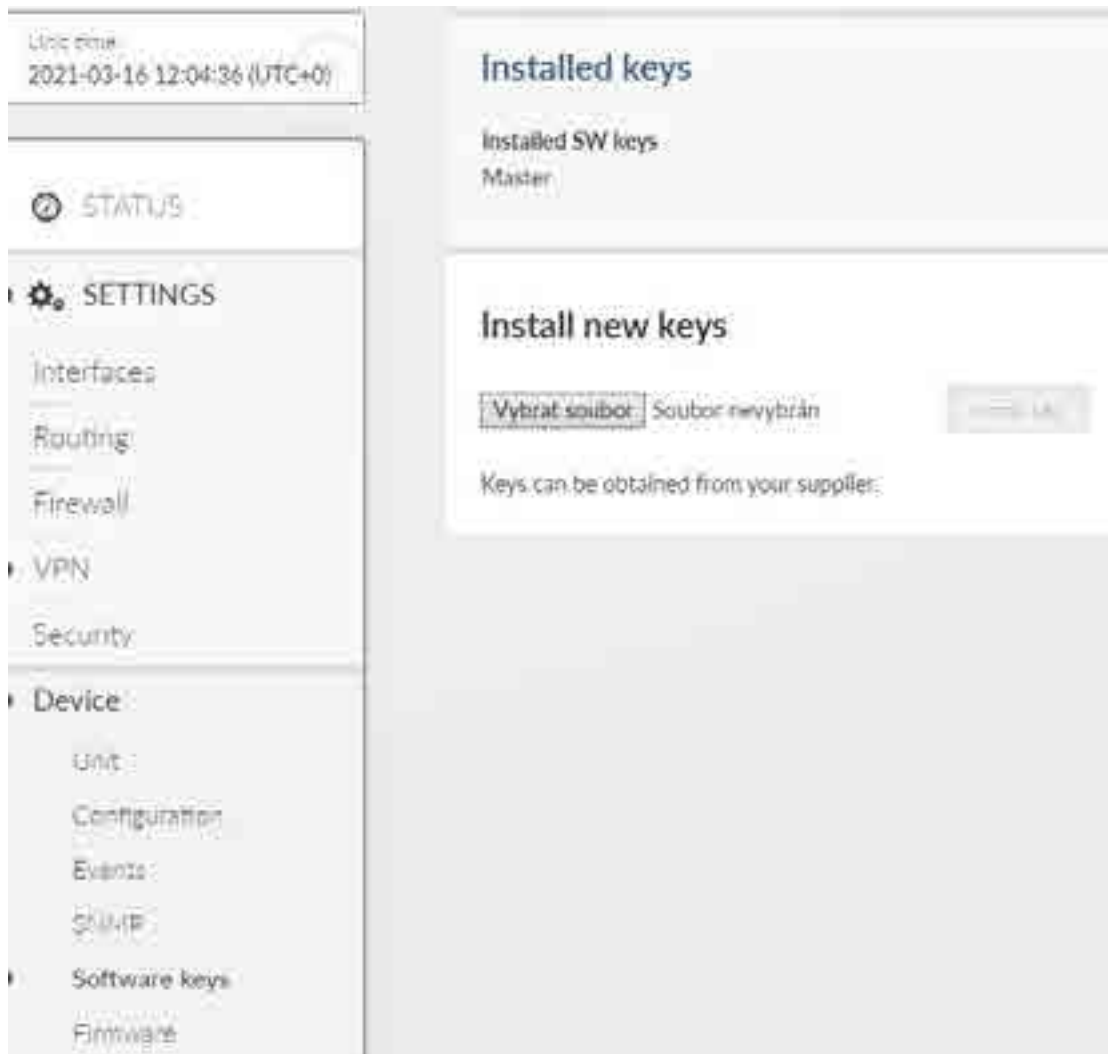
Notification packets destination port.

7.6.5. SW keys

Certain RipEX2 features need to be activated by a SW key to be available. When the respective SW key is not present, the feature can not be configured. If the feature is enabled in a configuration backup file and the file is loaded to a unit which is not equipped with the respective key, the configuration is refused (no changes are made in the unit).

Here is the list of available SW keys and their assignment to offered SW key packages.

SW key(s) can be obtained from your supplier. It is delivered as a text file containing the key(s). Every SW key is unique for the specific unit (specific serial number). Use Choose File dialog to select the file and Install key button to install the key(s) to unit.



Differences with the previous generation of RipEX:

- SW keys are always installed as a file (there is not a clipboard option)
- Single file can contain multiple SW keys
- SW keys are not time limited

7.6.6. Firmware

Unit firmware defines the unit functionality. There are several principles for managing the firmware in the running network:

- Maintain the same version of firmware all around the network – preferred scenario. RipEX units are able to cooperate even when running different version of firmware, but using the same firmware version in all units is the best way to keep the network maintenance easy and straightforward.
- The traditional good-practice says “do not touch the running system” – which means: do not upgrade the firmware if there is no reason to do so.
- The cyber security issues may force the firmware to be upgraded e.g. when some serious security vulnerability was fixed.

There are 2 stages of the firmware upgrade procedure:

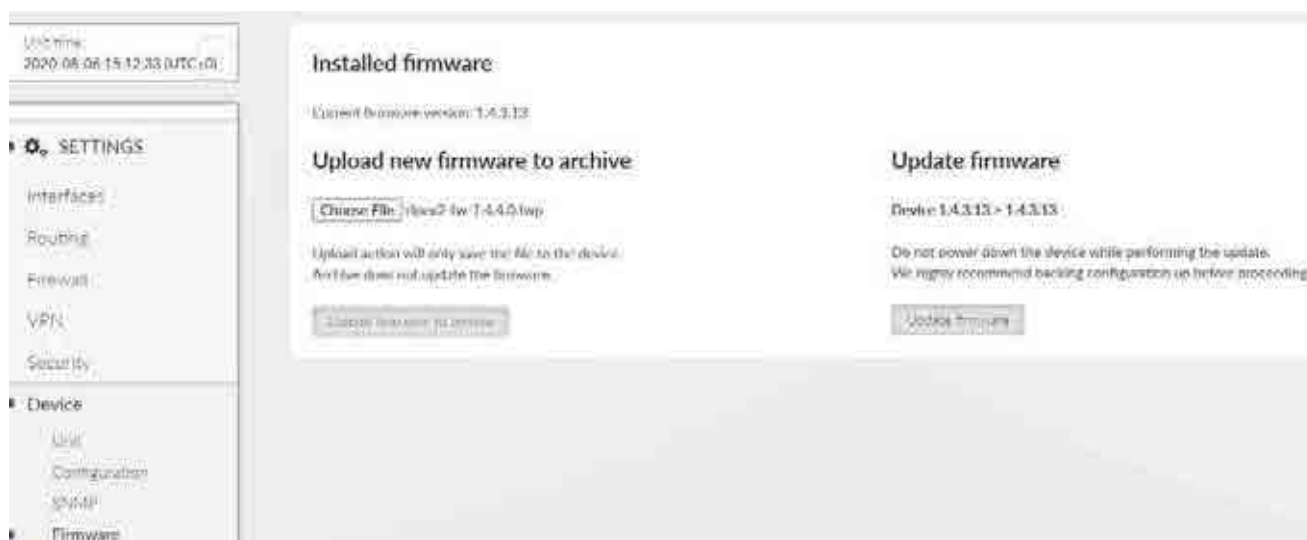
- Uploading new firmware into the unit internal archive
- Updating the unit firmware

Both operations can take several tens of seconds.)



Note

The uploading time of the new FW into the unit may last longer when slow connection to the file location is used.



Note

Unit configuration backup is highly recommended prior the firmware update.

To upgrade the firmware:

1. Optional (recommended): Backup the current unit configuration (menu Settings – Device – Configuration – Back up and download)
2. Download the required firmware from the *Racom web*¹: Products – RipEX – Download – Firmware RipEX2 – ripex2-fw-x.x.x.0.fwp
3. Click the **Choose File** button (the button label may differ based on your web browser localization) to select the firmware file
4. Click the **Upload firmware to archive** button to transfer the firmware file into the unit. The upload can take a long time – depending on the connection speed between the management PC and the RipEX2 unit. In case of slow connection and file transfer longer than 120 s, the web browser will shut down the connection and the action will not finish successfully. This action does not update the running unit firmware yet. There is no affection on the other communication running through this unit. Successful saving of the new firmware into the archive is announced in the Notifications and the available firmware version is printed Under the “Update firmware” heading (on the right side of the “>” mark).

Update firmware

Device 1.4.3.13 > 1.4.4.0

5. Click the **Update firmware** button to update (i.e. reinstall) the unit firmware. The update process takes approx. one minute. The user data communication running through this unit is interrupted for a while. All the processes are restarted in a certain moment (e.g. VPN tunnels need to be re-established).
6. It is possible not only to upgrade the firmware version, but even to downgrade it, although this operation is not recommended. Be aware of eventual security issues of firmware downgrade as eventually outdated security code can be part of an old firmware. Unit configuration may not be fully compatible. In such a case, parts of the unit configuration will be changed to the default values.



Warning

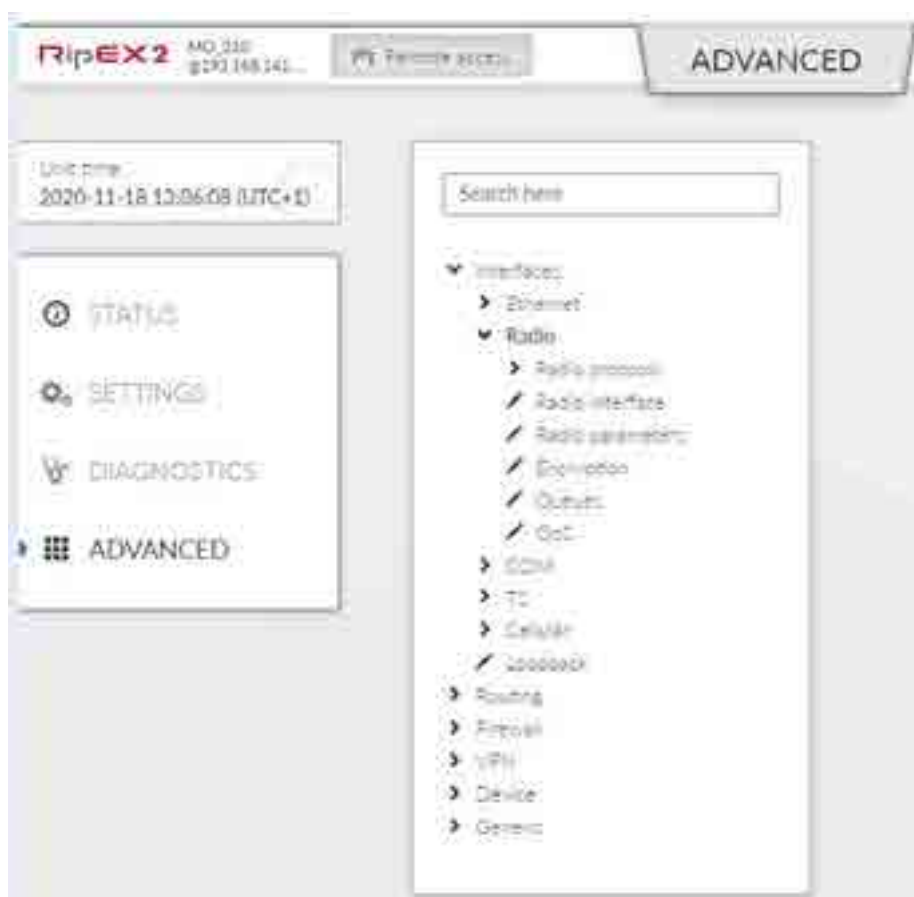
Do not shut down the unit during the firmware update process. It may permanently damage the unit.

7.7. Advanced

RipEX 2 introduces new concept for expert settings and rapid deployment of new features called “Advanced” section. Advanced section displays all configuration set points currently present in the device automatically, without need to design a special configuration page (like the ones in “Settings”). This allows us to deploy new features rapidly with each new firmware and also allows experienced users to fine-tune their RipEX 2.

Please note, that RipEX 2 is a very powerful device and it really shows all parameters in the Advanced section.

¹ <https://www.racom.eu/eng/products/radio-modem-ripex.html#download>



When you visit the page for the first time, you will see a search field and below a tree of configuration pages.

Search field looks through all labels and the tree itself and is capable of showing all relevant configuration pages. It features so called “fuzzy” search capable of returning right answers even when there is a typo in search query. Try searching for “Ethernet” or “BGP” to see the feature in action. To use the whole tree again, simply delete search query.

Configuration tree has two parts. For your convenience first few items (Interfaces, Routing, ...) use similar hierarchy to “Settings”, but include all advanced settings. The newest features then can be found in the last item called “General”, which contains all configuration tables there are in the unit.

By selecting a configuration page (marked with pencil icon) a window is shown on the right side of the screen containing selected configuration page set points. You can change settings and then send them to the device the same way you know from “Settings”.

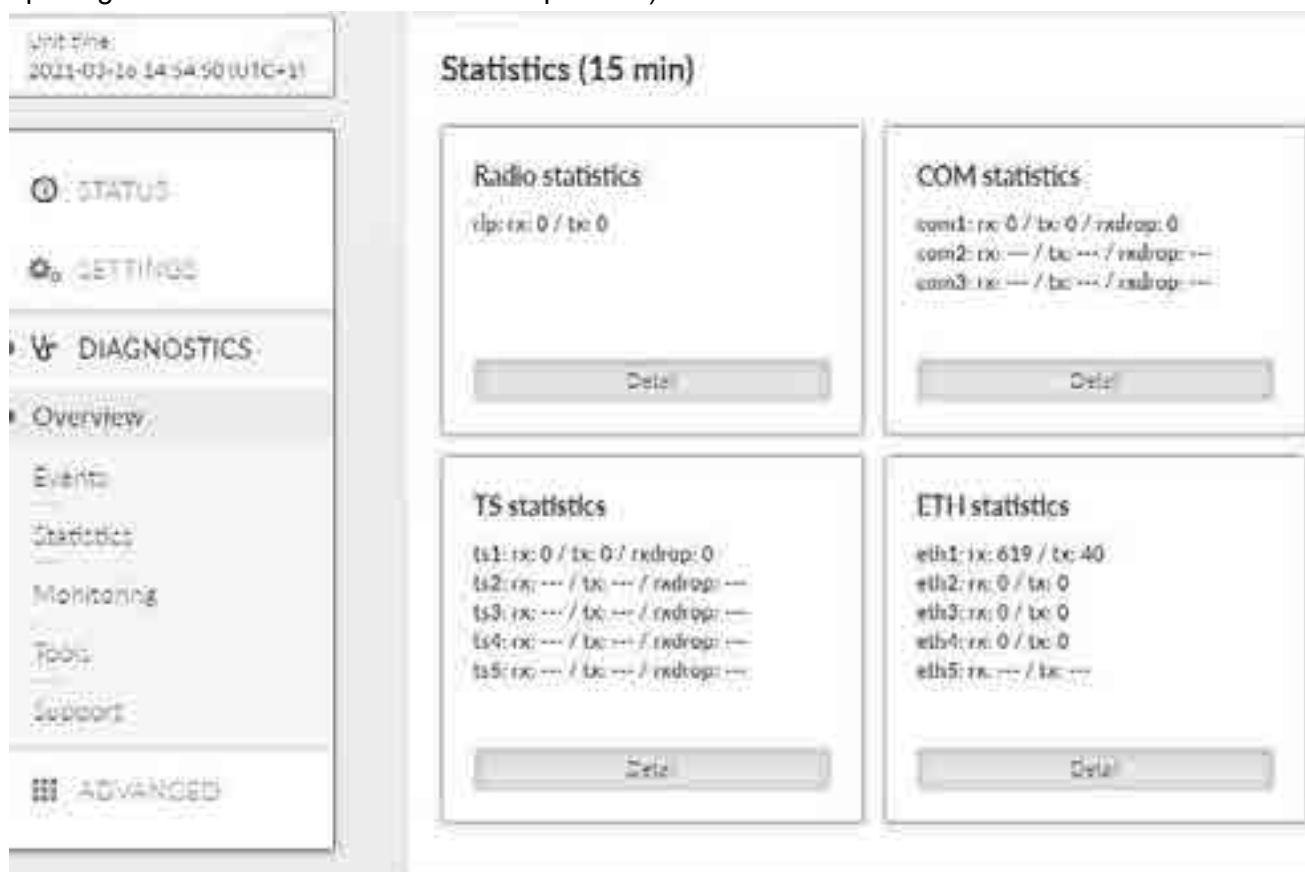


Please note, that RipEX 2 is a very powerful device and it really shows in the Advanced section. Be careful when adjusting settings in Advanced section and review the “Changes” page in detail before sending changes to the device.

8. Diagnostics

8.1. Overview

The Overview windows shows the short view of the statistic over last 15 minutes (from the time of opening of the window or Refresh button pressed).



8.2. Events

This menu shows all events which occurs within the unit history.

For filtering of the events you can use the filtering tool. When no filter rules are used, the last 30 events will be displayed after Display button click.

Older events should be displayed using Load more button click, the events which occurs during the viewing of this window can be load by using Load newer button.

Alarms are displayed in red color, warnings in orange, notices in black and debugs in gray.



It is possible to change severities of individual events in the menu SETTINGS/Device/Events.

8.3. Statistics

RipEX2 unit permanently monitors various system 'channels'. There are several types of those channels: Physical interfaces (Ethernet ports, serial ports, radio interface, additional module interface (e.g. LTE module) when installed), virtual interfaces (e.g. VLAN interfaces) and HW sensors (CPU temperature, supply voltage, ...). Monitored values are stored in the internal database.

Statistics page provides aggregated statistical data from this internal database. Data can be both displayed and downloaded in CSV format. This file format is suitable to be imported to any 3rd party spreadsheet program for further analysis.

There are two different options how to display statistics data:

- **Historical**

Statistics counters are aggregated over the defined time interval. The interval is defined by two time stamps "From" and "To".

- **Differential**

Statistics counters are aggregated between the counter reset and the current time (the moment when the Display button was pressed). Reset is triggered by a unit reboot or by the Reset statistics button.

Reset statistics button - initiates the Differential statistic counters reset. Such a reset does not affect normal statistic counters - i.e. the Historical statistics is not affected by such a Reset at all.

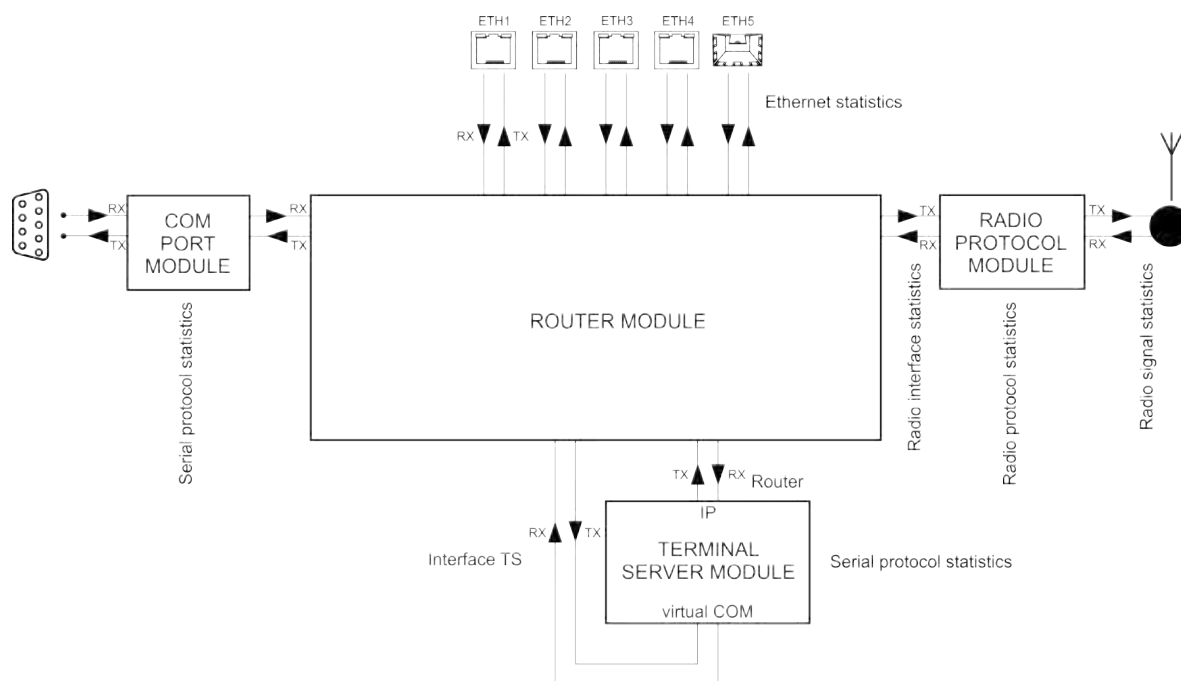


Fig. 8.1: Statistics data in the context of unit interfaces

8.3.1. Parameters

Statistics data are always retrieved as aggregated for a certain time Interval. This Interval can be set by putting specific date and time into "From" and "To" fields, or using buttons "Last day", "Last hour" or "More options" fast presets (from several minutes to several days). Button "Set Current Time" sets current time to both From and To fields to ease current unit status diagnostics.

There are following sets of statistical data available in the unit:

- Radio interface statistics
- Radio protocol statistics
- Radio protocol non-addressable statistics
- Radio signal statistics
- Radio signal non-addressable statistics
- Serial protocols statistics
- Ethernet statistics



“Display” button then shows chosen data below. “Download Selected Data” button generates CSV (UTF-8 encoded) file of all chosen systems’ data and downloads them as files without displaying them. Both “Display” and “Download ...” buttons send a request for the required set of statistics data to the unit. Retrieving and transferring of the data (over the radio channel) takes some time. Downloading the data is practical when the user needs to process them in a spreadsheet and wants to save some bandwidth. It is also recommended to use spreadsheet editor like Microsoft Excel or Apple Numbers to process statistics on mobile devices due to better user experience provided by the specialized apps.

8.3.2. Radio interface statistics

Radio interface statistics provides set of data monitoring the interface between the Router module (IP routing engine in the unit) and the Radio protocol module. It corresponds to monitoring Radio - Router.

Tx direction: from the Router module to the Radio protocol module. Rx direction: from the Radio protocol module to the Router module.

Radio interface statistics

Link address	IP address		UDP		TCP		ICMP		ARP		Other	
			count	[B]	count	[B]	count	[B]	count	[B]	count	[B]
TOTAL	0.0.0.0	Rx	71	0	130	29476	246	114532	1	42	0	0
		Tx	0	0	130	30504	246	145956	16	672	0	0
00:02:a9:20:07:43	10.10.10.11	Rx	0	0	130	29428	246	114532	1	42	0	0
		Tx	0	0	132	30504	248	145956	1	42	0	0
BROADCAST	255.255.255.255	Rx	0	0	0	0	0	0	0	0	0	0
		Tx	0	0	0	0	0	0	15	600	0	0

- MAC address** - MAC address of the IP packet. Source for Rx or destination for Tx packets.
- IP address** – translated MAC address when available. Address 0.0.0.0 is used as a placeholder if the translation is not available. If the Transparent protocol is used, the translation is not available at all.
- UDP, TCP, ICMP, ARP** - Packet count and amount of data in Bytes [B] for different protocol types. Amount of data is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).
- Other** – Packets not handled by the previous counters (e.g. VLAN, services, GRE, IPsec (ESP), ...)

8.3.3. Radio protocol statistics

Radio protocol statistics provides set of data monitoring the radio channel access protocol frames and events. It corresponds to monitoring Radio - Interface.

Frames which are not addressed to/from this unit are not handled (they do not affect any counter).

Rx direction: from the 'air' radio interface to the Radio protocol module. Tx direction: from the Radio protocol module to the radio interface.

Radio protocol statistics Download Data

Link address	IP address		Frame OK	Frame err	Frame dupl	Packet rej	Ctrl frames	Total count	[B]
			Frame OK	Frame lost	Frame rep				
TOTAL	0.0.0.0	Rx	377	0	0	0	4439037	4439414	26749120
		Tx	393	73	218	0	4432331	4433017	26866384
1	10.10.10.11	Rx	377	0	0	0	4439037	4439414	26749120
		Tx	378	73	218	0	754	1422	216544
UNICAST	255.255.255.255	Rx	0	0	0	0	0	0	0
		Tx	14	0	0	0	4441488	4441594	26849040

Link address – Link address of the frame. Source for Rx or destination for Tx frames. This is a Link address assigned at the origin (input) - when entering, or at the target (output) - when leaving the radio network.

In case of Base driven protocol or Transparent protocol, this address pair is not modified when re-translated. As a result of this fact, the whole traffic to a remote station behind the re-translation is counted together in a line assigned to the remote station.

For the Link address:

In case of Base driven protocol - the Protocol address is used

IP address – translated MAC address when available. Address 0.0.0.0 is used as a placeholder if the translation is not available. If the Transparent protocol is used, the translation is not available at all.

Frame OK (Rx) – Correctly received data frames count.

Frame OK (Tx) – Correctly send data frames count. Control frames are not included. When ACK is on, only acknowledged frames are included. Re-translated data frames are not included.

Frame err (Rx) – Received corrupted data frames count (CRC error)

Frame lost (Tx) – Transmitted unacknowledged frames count. It happens when ACK is on and acknowledging frame was not received even when full number of re-transmission attempts was reached.

Frame dupl (Rx) – Received, but dropped, duplicated data frames count. 'Duplicated' frames are repeatedly received acknowledged frames.

Frame rep (Tx) – Repeated frames count (they can appear when ACK is on). Re-translated frames are not included.

Frame rej (Tx) – Rejected frames count (rejected just before transmission) – reason: buffer timeout. In case of Transparent protocol (Bridge mode) it happens when there is a collision during re-translation.

Packet rej (Rx) – Correctly received but rejected packets count - reason: impossible to decrypt or decompress.

Packet rej (Tx) – Rejected packets count (rejected before handed over to the transmitter) – reason: buffer overflow, buffer timeout.

Ctrl frames (Rx, Tx) – Received / transmitted control frames count.

Total (Rx) – Received frames count and amount of data in Bytes. Amount of data - for both Rx and Tx - is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

Total (Tx) – Transmitted frames count and amount of data in Bytes. Re-translated frames are included.

8.3.4. Radio protocol non-addressable statistics

Radio protocol 'non-addressable' statistics provides set of data monitoring the radio channel access protocol frames and events which can not be linked with any address (e.g. broadcasts). It corresponds to monitoring Radio - Interface.



False Sync – False synchronization incidents count

Phy header err – Packet reception failure count - reason: sub header error

Phy err – Packet reception failure count - reason: physical layer analysis error

Header err - Packet reception failure count - reason: header content error or CRC error.

Incompatible – Received incompatible frames count - reason: different radio protocol

Strange – Received unexpected frames count - reason: wrong addresses, wrong sequence etc. Valid for Base Driven Protocol only.

Unroutable – Packets counter which were scheduled for transmission but impossible to be forwarded to the Radio protocol - multiple reasons: e.g. the destination IP address is not known

8.3.5. Radio signal statistics

Radio signal statistics provides set of data monitoring the radio interface quantities and events. It corresponds to monitoring Radio - Interface.

Statistic data are collected by the frame source address - Link address, which is an address of the originating radio transmitter (unlike "Radio protocol statistics" where the Link address is an address of the unit where the packet entered the RipEX network).

There is a special address 'RELAY' to indicate frames coming from the re-translation unit in case of Base Driven Protocol operation.

Link address	IP address	Header count	RSS [dBm]				Phy header MSE [dB]				Freq offset [Hz]	Ant [dBi]	Ant2 [dBi]			Data count	Data MSE [dB]			
			avg	dev	min	max	avg	dev	min	max			avg	min	max		avg	dev	min	max
BASE	10.10.10.12	4275832	-78	0	-81	-75	-34	1	-42	-20	-20	0	0	0	0	4275832	-34	3	-42	-17

Header count – Received headers count

RSS [dBm] – Radio Signal Strength - measured within the header reception

avg / dev / min / max – average / standard deviation / minimum / maximum

Phy header MSE [dB] – modulation Mean Squared Error - measured within the header reception

Freq offset [Hz] – Averaged frequency offset between the transmitter and the receiver station, measured by the receiver station.

Att1 [%] - First internal attenuator (15 dB) activated. Shown in percents of affected frames.

Att2 [dB] – Value of the 2nd internal attenuation applied.

Data count – Received complete frames (including data part) count. Frames with valid header CRC, but wrong data CRC are not counted

Data MSE [dB] - modulation Mean Squared Error - measured within the frame data part reception

8.3.6. Radio signal non-addressable statistics

Radio signal statistics provides set of data monitoring the radio interface quantities and events. This table contains measurements handled before the frame reception and measurements which can not be linked with any address (e.g. broadcasts). It corresponds to monitoring Radio - Interface.

Radio signal non-addressable statistics Download Data

Pre-frame										Others							
Count	RSS [dBm]				Att1 [%]	Att2 [dB]			Count	RSS [dBm]				Phy header MSE [dB]			
	avg	dev	min	max		avg	min	max		avg	dev	min	max	avg	dev	min	max
4261969	-119	2	-139	-95	0	0	0	0	1	-80	0	-80	-80	-34	0	-34	-34

Pre-frame – Values based on measurements handled before the frame reception

RSS [dBm] – Radio Signal Strength - measured short time just before the frame reception

Others – Values for frames which can not be linked with any address

8.3.7. Serial protocol statistics

Serial protocols statistics provides set of data monitoring the COM port(s) and Terminal server (s). Only enabled interfaces are displayed. The statistics counters are based on packets entering or leaving the COM port or Terminal server module. As a result of this the 'count' values correspond to the Protocol messages (the "Protocol" selected on the specific COM port or Terminal server). If the packet is 'glued' from the several frames, it is evaluated as a single packet. In case of COM port statistic, the summary of 'Correct' and 'Drop' Bytes provides the total amount of Bytes on the physical interface.

Rx direction: from the connected (at the COM or ETH port) external device to the RipEX unit (i.e. from the COM port module or Terminal server module to the Router module). Tx direction: from the RipEX unit to the external device.

Serial protocols statistics Download Data

Interface		Correct		Drop	
		count	[B]	count	[B]
com1	Rx	0	0	0	0
	Tx	0	0	0	0
eth	Rx	0	0	0	0
	Tx	0	0	0	0

Interface – Interface name

Correct (Rx, Tx) – Correctly received / transmitted packets count and amount of data in Bytes. Accepted by the COM port or Terminal server module - based on the selected Protocol processing. Amount of data - for both Correct and Drop counters - is affected by COM port data only (i.e. IP headers of the UDP frames created in the COM port module are NOT counted).

Drop (Rx, Tx) - Dropped received / transmitted packets - reason: corrupted frame, CRC error, wrong protocol message, unsupported protocol message.

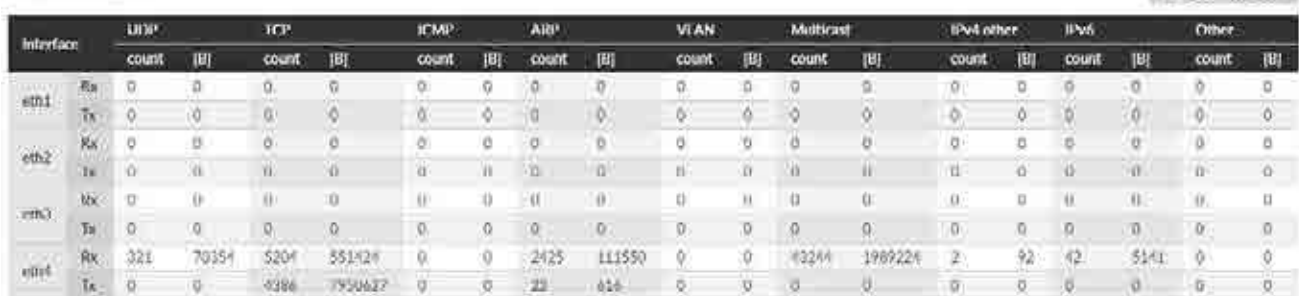
8.3.8. Ethernet statistics

Ethernet statistics provides set of data monitoring the physical Ethernet ports. Only enabled interfaces are displayed.

Only correctly received frames are handled. The counters correspond to the specific IP protocol types.

Rx direction: from the physical Ethernet port to the RipEX unit (i.e. to the Router module). Tx direction: from the RipEX unit to the physical Ethernet port.

Ethernet statistics



Interface		UDP		TCP		ICMP		ARP		VLAN		Multicast		IPv4 other		IPv6		Other	
		count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]	count	[B]
eth1	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	Rx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Tx	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth4	Rx	321	70354	5204	551424	0	0	2425	111550	0	0	40244	1989224	2	92	42	5141	0	0
	Tx	0	0	4386	7950622	0	0	23	616	0	0	0	0	0	0	0	0	0	0

Interface – Interface name.

UDP, TCP, ICMP, ARP, VLAN, Multicast - Packet count and amount of data in Bytes [B] for different protocol types - IPv4 traffic. Amount of data - for all counters - is summed over the whole Layer 2 Ethernet frame (i.e. all IP headers are counted).

IPv4 other - IPv4 traffic not handled by the previous counters

IPv6 - IPv6 traffic counter

Other - Counter summing up the frames which were not handled by the previous counters - for example MPLS and GOOSE protocols.

8.4. 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.

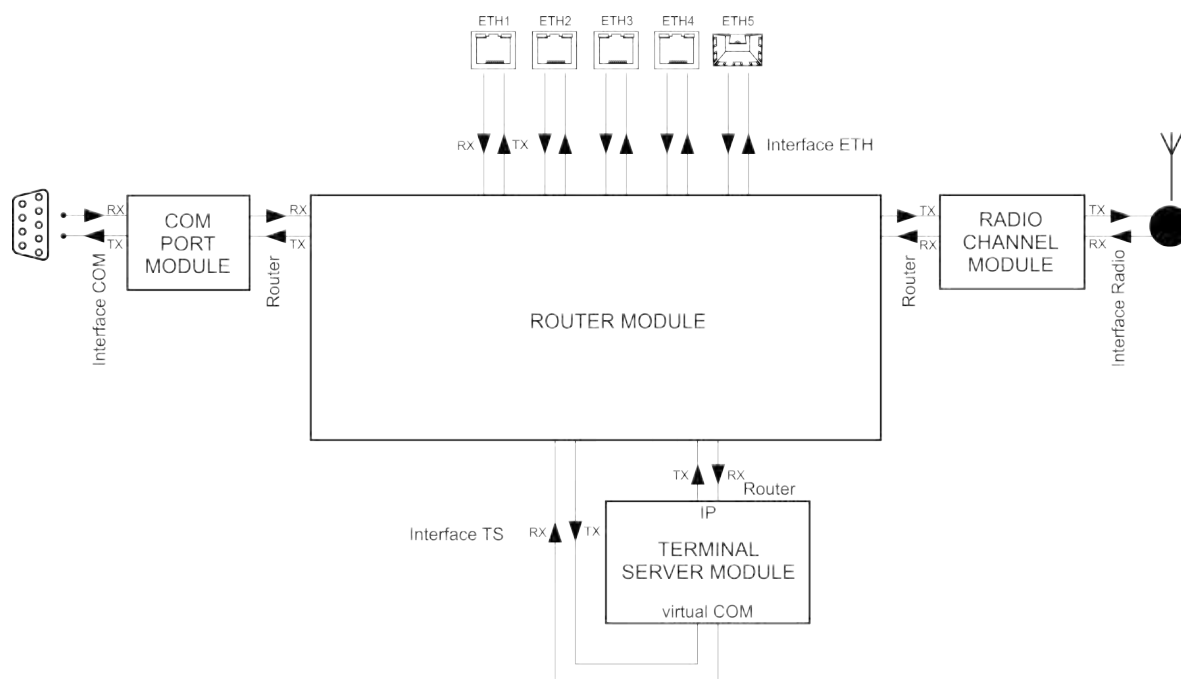
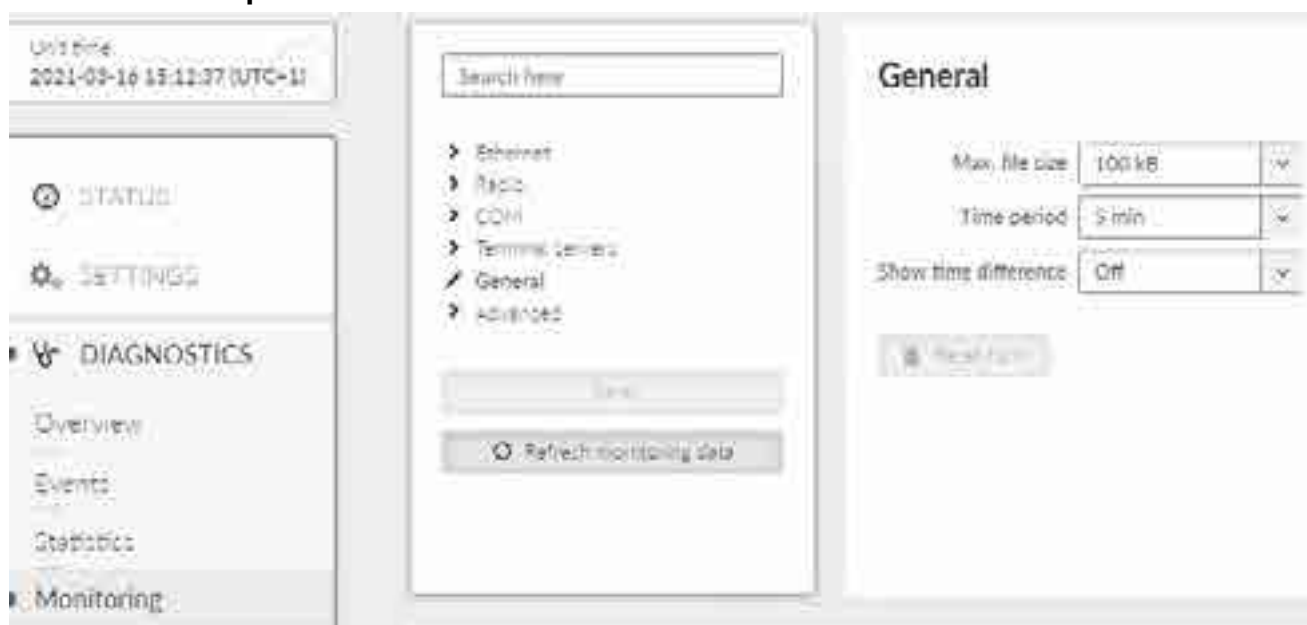


Fig. 8.2: Interfaces

8.4.1. 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**

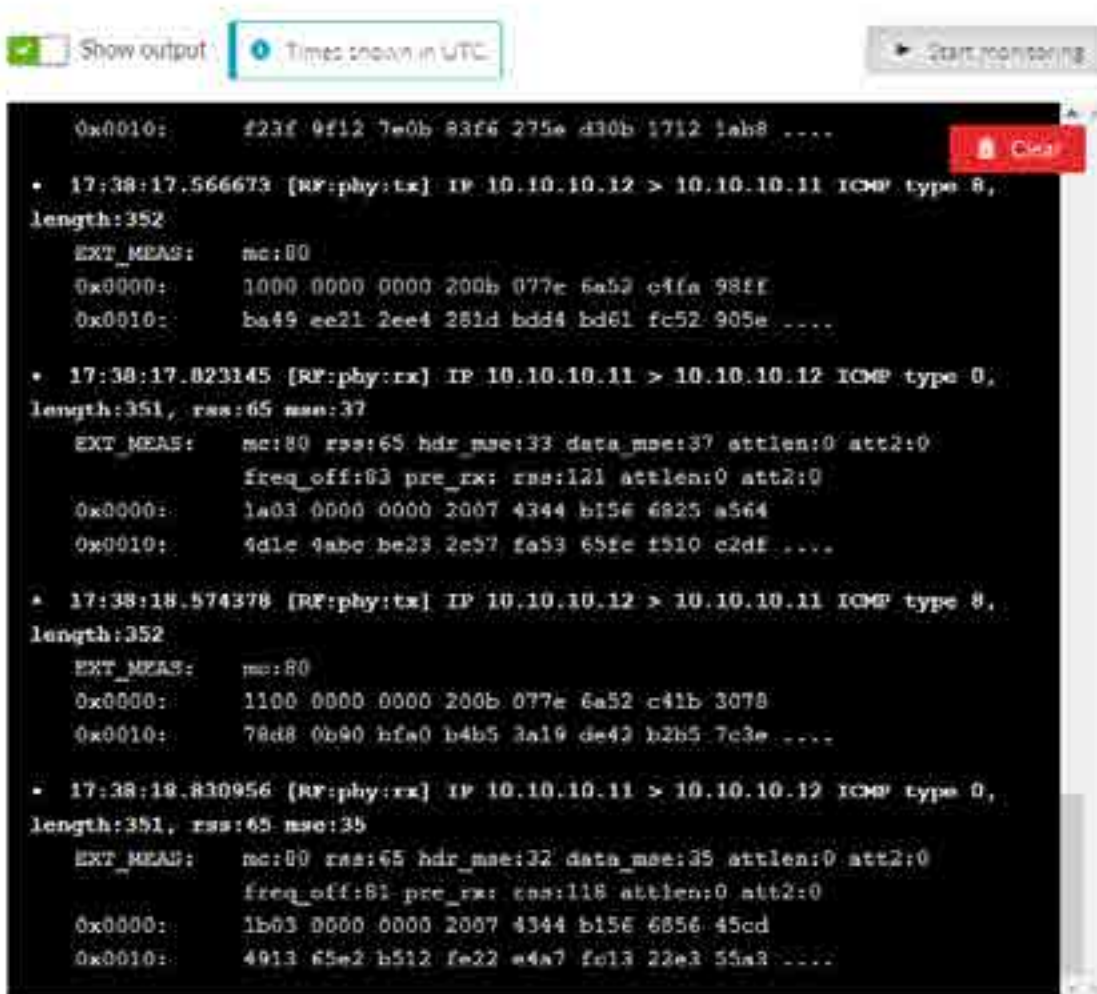
List box {On; Off}, default = "Off"

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

- **Display**

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

Output



- **Show output**

List box {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

8.4.2. Interfaces

Common parameters for several interfaces:

- **Rx enabled, Tx enabled**

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

A packet is considered a Tx one when it comes out from the respective software module (e.g. 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. 8.2, "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.

The screenshot shows the 'Router' configuration page. On the left, a sidebar contains 'SETTINGS', 'DIAGNOSTICS', 'Monitoring', 'Events', 'Statistics', 'Support', and 'ADVANCED'. The 'DIAGNOSTICS' menu is expanded, showing 'Overview', 'Monitoring' (selected), 'Events', 'Statistics', and 'Support'. The 'Monitoring' sub-menu is also expanded, showing 'General' and 'Advanced'. The 'Advanced' sub-menu is expanded, showing 'General' and 'Monitoring' (selected). The 'Router' configuration page has a search bar and a 'Refresh monitoring data' button. The configuration fields are: Enabled (Off), Rx enabled (On), Tx enabled (Off), Source mask (0), Destination mask (0), Include reverse (On), Offset (0), Length (0), Source IP (0.0.0.0), Destination IP (0.0.0.0), Source port (from) (0), Source port (to) (0), Destination port (from) (0), Destination port (to) (0), and Dropped frames (Router) (0).

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

The screenshot shows the 'Monitoring' configuration page. On the left, a sidebar contains 'SETTINGS', 'DIAGNOSTICS', 'Monitoring', 'Events', 'Statistics', 'Support', and 'ADVANCED'. The 'DIAGNOSTICS' menu is expanded, showing 'Overview', 'Monitoring' (selected), 'Events', 'Statistics', and 'Support'. The 'Monitoring' sub-menu is also expanded, showing 'General' and 'Advanced'. The 'Advanced' sub-menu is expanded, showing 'General' and 'Monitoring' (selected). The 'Monitoring' configuration page has a search bar and a 'Refresh monitoring data' button. The configuration fields are: Max. file size (100 kB), Time period (5 min), Show time difference (Off), Display (HEX), Enabled (Off), Rx enabled (On), Tx enabled (On), Dropped frames (On), and Bandwidth (NORMAL).

8.5. Tools



Available are all paremeters used by standard ICMP ping. Start / Stop button starts / stops pinging.

8.6. Support



Note

Testing is only allowed without standard radio protocol. Please set "Radio protocol" to "None" in Radio Settings before using this feature.

- **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**

List box {Random data; Carrier wave; Single tone}, default = "Random data"

Type of transmitted signal during the test. In case of Single tone a frequency with an offset from the central frequency is transmitted.

- **Period [s]**

Number {1 – 120 s}

Transmission test pre-set duration.

- **Start button**

Starts the transmission test

- **Stop button**

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

8.7. Syslog



- **SYSLOG server IP** – IP address of the remote Syslog server to which will be send logs with severity higher than severity set in the Max. severity
- **SYSTOG server Port** – port used by the Syslog server
- **Max. severity** – the events with set severity (and higher) will be send to the Syslog server
- **Login attempt** – un login

9. Technical parameters

Tab. 9.1: Technical parameters

hazardous-locations Radio parameters		
Frequency bands	135 – 175 MHz; 285 – 335 MHz; 335 – 400 MHz; 400 – 470 MHz; 450 – 520 MHz	
Channel spacing	6.25; 12.5; 25; 50; 100; 150; 200; 250; 300 kHz	
Frequency stability	±0.5 ppm ±0.01 ppm with internal GPS (optional) or external time synchronisation, <i>see details</i>	
Modulation	QAM: 256QAM; 64QAM; 16DEQAM; D8PSK; π /4DQPSK; DPSK FSK: 4CPFSK; 2CPFSK, <i>see details</i>	
FEC (Forward Error Correction)	2/3; 3/4; 5/6; Off Trellis code with Viterbi soft-decoder	
Gross data rate (data speed) ¹⁾	Channel spacing [kHz]	Gross data rate (modulation rate) [kb/s]
	6.25	42
	12.5	83
	25	167
	50	333
	100	555
	150	925
	200	1111
	250 ²⁾	1389
300 ²⁾	1736	
Transmitter		
RF Output power	QAM: 0.1 – 5.0 W (20 – 37 dBm) RMS in 1dB step ³⁾ FSK: 0.1 – 10 W (20 – 40 dBm) in 1dB step <i>see details</i>	
Duty cycle	Continuous	
Rx to Tx Time	< 2 ms @ 6.25 kHz channel < 1.0 ms @ 12.5 kHz channel < 0.7 ms @ 25 kHz channel	
Intermodulation Attenuation	> 40 dBm, > 70 dBm (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	-117 dBm (12.5 kHz; 2CPFSK; BER 10 ⁻⁶ ; 3/4 FEC) <i>see details</i>	

Anti-aliasing Selectivity	56 kHz @ -3 dB BW applicable for 6.25; 12.5; 25 kHz 500 kHz @ -3 dB BW applicable for 50; 100; 150; 200; 250; 300 kHz
Tx to Rx Time	< 2 ms @ 6.25 kHz channel < 1.0 ms @ 12.5 kHz channel < 0.7 ms @ 25 kHz channel
Maximum Receiver Input Power	20 dBm (100 mW)
Rx Spurious Emissions (Conducted)	< -57 dBm
Radiated Spurious Emissions	< -57 dBm
Blocking or desensitization	> -23 dBm @ 1 MHz > -19 dBm @ 2 MHz > -15 dBm @ 5 MHz > -13 dBm @ 10 MHz
Spurious response rejection	> 70 dB
Technical parameters are subject to change without prior notification. 1) Network throughput varies and depends heavily on the data structure, optimization effectivity, protocol on Radio channel, network topology, signal budgets and many other parameters of the network. Practical tests are recommended. 2) Available only in Bridge mode. 3) Max peak envelope power (PEP) 10 W (40 dBm) .	

Electrical		
Primary power	10 to 30 VDC, negative GND	
Rx	8 W / 13.8 V, <i>see details</i>	
Tx	12 – 55 W, <i>see details</i>	
Sleep mode	0.01 W	
Save mode	5 W	
Interfaces		
Ethernet	10/100/1000Base-T Auto MDI/MDIX	4× RJ45
SFP	10/100/1000Base-T or 1000Base-SX or 1000Base-LX user exchangeable SFP with max. power consumption 1.25 W	1× SFP
COM	RS232 / RS485 SW configurable	DB9F
	600 b/s – 1 Mb/s	
USB	USB 3.0	Host A
Antenna	50 Ω SW configurable 1× Tx / Rx or 1× Rx + 1× Tx	2× TNC female
Inputs/Outputs	1× HW alarm input 1× HW alarm output 1× Sleep input	Power connector
	2× DI, 2× DO, 1× difDI	RJ45

	not available when Expansion board 'C' (COM ports) is used
--	--

Optional interfaces	
Expansion board 'G' GPS (GNSS)	Active antenna 3.3 VDC SMA female (AUX on front panel)
	72-channel u-blox M8 engine GPS/QZSS L1 C/A, GLONASS L10F, BeiDou B1I, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN
Expansion board 'C' COM ports	COM2: RS232 - 5 pin (RxD, TxD, GND, RTS, CTS) 600 b/s to 2 Mb/s COM3: RS232 -3 pin (RxD, TxD, GND) 2.4 kb/s to 921.6 kb/s RJ45 (DI/DO on front panel)
Expansion board 'E', 'P', 'A' Cellular	<i>see details</i>

Indication LEDs	
LED panel	5× tri-color status LEDs (SYS, AUX, RX, TX, COM)
ETH	4× RJ45 (Link and Activity LEDs), 1× SFP (Status LED)
Environmental	
IP Code (Ingress Protection)	IP41, IP42, IP52 - <i>see details</i>
MTBF (Mean Time Between Failure)	> 900 000 hours (> 100 years)
Operating temperature	−40 to +70 °C (−40 to +158 °F) ⁴⁾
Operating humidity	5 to 95 % non-condensing
Storage	−40 to +85 °C (−40 to +185 °F) / 5 to 95 % non-condensing
Mechanical	
Casing	Rugged die-cast aluminium
Dimensions	H × W × D: 60 × 185 × 125 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 <i>see details</i> ¹
SW	
Operating modes	Bridge / Router
Radio channel protocols	Transparent @ Bridge Base driven, Flexible @ Router <i>see details</i> ²
User protocols on COM	DNP3, DF1, IEC101, Modbus RTU, PR2000, RDS, Siemens 3964R, Async Link
User protocols on Ethernet	Modbus TCP, IEC104, DNP3 TCP, Comli TCP, Terminal server...
Serial to IP converters	DNP3 / DNP3 TCP, Modbus RTU / Modbus TCP
Protocol on Radio channel	
Multi master applications	Yes
Report by exception	Yes
Collision Avoidance Capability	Yes
Remote to Remote communication	Yes
Addressed and acknowledged serial SCADA protocols	Yes
Data integrity control	CRC 32
Optimization	Intelligent payload data and header (Eth / IP / TCP / UDP) compression
Security	
Management	HTTPS (own certificate), SSH
Role-based access control (RBAC)	4 levels (Guest, Tech, SecTech, Admin)
WiFi management access (optional)	WPA2-PSK secured

¹ https://www.racom.eu/eng/products/radio-modem-ripex.html#accessories_mounting
² https://www.racom.eu/eng/products/radio-modem-ripex.html#radio_protocols

Encryption	AES256-CCM
VPN	IPsec, GRE
VLAN	IEEE 802.1Q (tagging), Q-in-Q for Transparent mode
AAA protocol	RADIUS
Firewall	Layer 2 - MAC, Layer 3 - IP, Layer 4 - TCP/UDP
FW	Digitally signed
HW tamper	Case opening evidence
⁴⁾ When full-duplex with full power (40 dBm PEP) and the surrounding temperature above + 60°C the external passive cooler should be used (e.g. <i>RipEX2-RS 19" Rack chassis</i>³).	

Diagnostic and Management	
Link testing	ICMP ping
Status informations	User interfaces
Statistics	Historical and differential statistics for Rx / Tx Packets on all user interfaces (ETH 1-5, COM 1-3, TS 1-5) and Radio interface - for individual connections. Radio protocol statistics (frame error, replied, duplicated, lost etc.) for individual radio links. Advanced statistics for Radio channel (RSS levels, MSE, Pre-frame RSS, Repeats, etc.)
Statistics history	Several weeks
Event log	Events filtered by time, severity, user, remote IP address and type of event
SNMP	SNMPv1, SNMPv2c, SNMPv3 Trap / Inform alarms generation as per settings
NTP	Client / Server
Monitoring	Real time analysis of all interfaces (RADIO, ETH 1-5 , COM 1-3, TS 1-5) and internal interfaces between software modules, <i>see details</i>

³ <https://www.racom.eu/eng/products/m/ripex2-hs/product.html#rip2rs>

Standards	
CE	RED, RoHS, WEEE
FCC, IC	FCC Part 90, IC RSS-119
Spectrum	ETSI EN 302 561 V2.1.1 ETSI EN 300 113 V2.2.1
EMC (electromagnetic compatibility)	ETSI EN 301 489-1 V2.2.3 ETSI EN 301 489-5 V3.2.1 EN 61850-3:2014
Product Safety	EN 62368-1:2014 + A11:2017
RF health safety	EN 62311:2008
Electric power substations environment	IEEE 1613:2009 IEEE 1613.1:2013 EN 61850-3:2014
Hazardous locations	EN 60079-0:2012 EN 60079-11:2012 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: Maximal power for individual modulations

RipEX2			
Modulation	PEP [dBm]	RMS [dBm]	RMS [W]
2CPFSK	20 – 40	20 – 40	0.1 – 10
4CPFSK	20 – 40	20 – 40	0.1 – 10
DPSK	20 – 40	20 – 37	0.1 – 5
$\pi/4$ -DQPSK	20 – 40	20 – 37	0.1 – 5
D8PSK	20 – 40	20 – 36	0.1 – 4
16DEQAM	20 – 40	20 – 35	0.1 – 3.2
64QAM	20 – 40	20 – 34	0.1 – 2.5
256QAM	20 – 40	20 – 33	0.1 – 2
SW configurable [PEP, dBm] FSK, QAM: 1 dB step			
PEP vs. RMS application note ⁴			

⁴ <https://www.racom.eu/eng/products/m/ripex/app/pep/pep.html>

Tab. 9.3: List of connected cables

Input / Output	Specified length	Shielded / Nonshielded	Recommended cable type
DC power supply 10 – 30 V	As needed	N	V03VH-H 2×0,5
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

Tab. 9.4: Power consumption for 24 Vdc

Tx Power consumption @24Vdc [W]	RipEX2-1			RipEX2-3, RipEX2-4		
	Min.	Typ.	Max.	Min.	Typ.	Max.
FSK 20 dBm RMS	12	14	15	12	14	15
FSK 40 dBm RMS	27	33	40	31	40	55
QAM 24 dBm PEP	12	13	14	12	13	14
QAM 40 dBm PEP	24	26	30	24	29	40

Rx Power consumption @24Vdc [W]	RipEX2
RipEX2	8.3 W
+Ethernet	+0.1 W @ 10BaseT +0.12 W @ 100BaseT +0.5 W @ 1000BaseT per Eth interface with connected equipment
+1st COM	+0.2 W
+GNSS	+0.15 W
+2nd COM	+0.1 W
+LTE	Rx +0.3, Tx +3 W
+SFP module typ.	+1 W

Tab. 9.5: Cellular interface (optional)

Cellular interface (optional)		
Frequency bands for expansion board 'E' Cellular	4G LTE Band 20 (800 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)	
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz	
	Ublox TOBY L-210	FCC ID XPYTOBYL210 TAC 35225506
Frequency bands for expansion board 'P' Cellular	4G LTE Band 28 (750 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 3 (1800 MHz), Band 1 (2100 MHz), Band 7 (2600 MHz)	
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz	
	Ublox TOBY L-280	FCC ID XPYTOBYL280 TAC 35850306
Frequency bands for expansion board 'A' Cellular	4G LTE Band 17 (700 MHz), Band 5 (850 MHz), Band 4 (1700 MHz), Band 2 (1900 MHz), Band 7 (2600 MHz)	
	3G UMTS/HSDPA/HSUPA Band 5 (850 MHz), Band 8 (900 MHz), Band 4 (AWS, i.e. 1700 MHz), Band 2 (1900 MHz), Band 1 (2100 MHz)	
	2G GSM/GPRS/EDGE GSM 850 MHz, E-GSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz	
	Ublox TOBY L-200	FCC ID XPYTOBYL200 TAC 35225406
Specification	ANT1, ANT2 - space diversity (on rear panel)	2× SMA Antenna
	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

Tab. 9.6: Sensitivity

Modulation	2CPFSK	4CPFSK	DPSK	$\pi/4$ DQPSK	D8PSK	16DEQAM	64QAM	256QAM
Channel spacing	Sensitivity [dbm] @ BER 10^{-6} , FEC 3/4 (2/3 QAM64 and QAM256)							
6.25	-119	-116	-116	-115	-111	-106	-104	-100
12.5	-117	-114	-114	-113	-108	-103	-101	-97
25	-115	-112	-112	-111	-106	-101	-99	-95
50	x	x	-109	-108	-103	-98	-96	-92
100	x	x	-106	-105	-100	-95	-93	-89
150	x	x	-104	-103	-98	-93	-91	-87
200	x	x	-103	-102	-97	-92	-90	-86
250	x	x	-102	-101	-96	-93	-89	-85
300	x	x	-100	-99	-94	-91	-87	-83
	Sensitivity [dbm] @ BER 10^{-2} (ETSI 80% PSR eqv.), FEC 3/4 (2/3 QAM64 and QAM256)							
6.25	-123	-121	-122	-121	-119	-116	-116	-109
12.5	-120	-119	-119	-118	-116	-112	-112	-106
25	-118	-117	-117	-116	-113	-110	-110	-104
50	x	x	-114	-113	-110	-107	-107	-101
100	x	x	-112	-111	-108	-104	-104	-99
150	x	x	-110	-109	-106	-102	-102	-97
200	x	x	-109	-108	-105	-101	-101	-96
250	x	x	-107	-106	-103	-100	-100	-94
300	x	x	-106	-105	-101	-98	-98	-93

9.1. Detailed radio channel parameters

Tab. 9.7: Channel spacing 6.25 kHz

Channel spacing [kHz]	6.25	
Occupied BW limit [kHz]	5	5
Modulation type	FSK	QAM
RipEX 1 "Mode"	FCC, CE	FCC
Baudrate [kBaud]	2.60	4.34
RipEX2 Compliance	FCC, ISSED	FCC, ISSED

6.25 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 2.60 kBaud				
2.60	2CPFSK	3K60F1DBN	3.60	5
5.21	4CPFSK	3K60F1DBN	3.60	5
Baudrate 4.34 kBaud				
4.34	DPSK	5K00G1DBN	5.00	5
8.68	$\pi/4$ -DQPSK	5K00G1DDN	5.00	5
13.02	D8PSK	5K00G1DEN	5.00	5
17.36	16DEQAM	5K00G1DEN	5.00	5
26.04	64QAM	5K00G1DEN	5.00	5
34.72	256QAM	5K00G1DEN	5.00	5

6.25 kHz						
Classification				Sensitivity [dBm]		
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10 ⁻²	BER 10 ⁻³	BER 10 ⁻⁶
RX sensitivity, Baudrate 2.60 kBaud						
2.60	1.95	3/4	2CPFSK	-122.5	-121.0	-119.0
2.60	2.60	Off	2CPFSK	-122.0	-120.0	-117.0
5.21	3.91	3/4	4CPFSK	-121.0	-119.0	-116.0
5.21	5.21	Off	4CPFSK	-120.0	-117.5	-114.0
RX sensitivity, Baudrate 4.34 kBaud						
4.34	3.26	3/4	DPSK	-122.0	-120.5	-116.0
4.34	4.34	Off	DPSK	-121.5	-119.5	-114.0
8.68	6.51	3/4	$\pi/4$ -DQPSK	-121.0	-119.5	-115.0
8.68	8.68	Off	$\pi/4$ -DQPSK	-120.0	-118.0	-112.0
13.02	9.77	3/4	D8PSK	-118.5	-116.0	-110.5
13.02	13.02	Off	D8PSK	-115.5	-112.0	-105.5
17.36	13.02	3/4	16DEQAM	-115.5	-112.0	-106.0
17.36	17.36	Off	16DEQAM	-112.5	-109.5	-102.5
26.04	17.36	2/3	64QAM	-115.5	-111.5	-103.5
26.04	19.53	3/4	64QAM	-112.5	-109.0	-102.0
26.04	21.70	5/6	64QAM	-111.5	-106.5	-99.5
26.04	26.04	Off	64QAM	-108.5	-104.0	-96.5
34.72	23.15	2/3	256QAM	-109.0	-106.0	-100.0
34.72	26.04	3/4	256QAM	-108.0	-104.5	-98.0
34.72	28.94	5/6	256QAM	-106.0	-103.0	-96.0
34.72	34.72	Off	256QAM	-104.0	-100.0	-94.5

Tab. 9.8: Channel spacing 12.5 kHz

Channel spacing [kHz]	12.5		
Occupied BW limit [kHz]	11	11	12.5
Modulation type	FSK	QAM	
RipEX 1 "Mode"	FCC, CE	FCC	CE
Baudrate [kBaud]	5.21	8.68	10.42
RipEX2 Compliance	RED FCC, ISED	RED FCC, ISED	RED

12.5 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 5.21 kBaud				
5.21	2CPFSK	7K50F1DBN	7.0	11.0
10.42	4CPFSK	7K50F1DDN	7.0	11.0
Baudrate 8.68 kBaud				
8.68	DPSK	10K0G1DBN	10.0	11.0
17.36	$\pi/4$ -DQPSK	10K0G1DDN	10.0	11.0
26.04	D8PSK	10K0G1DEN	10.0	11.0
34.72	16DEQAM	10K0G1DEN	10.0	11.0
52.08	64QAM	10K0G1DEN	10.0	11.0
69.44	256QAM	10K0G1DEN	10.0	11.0
Baudrate 10.42 kBaud				
10.42	DPSK	11K9G1DBN	11.9	12.5
20.83	$\pi/4$ -DQPSK	11K9G1DDN	11.9	12.5
31.25	D8PSK	11K9G1DEN	11.9	12.5
41.67	16DEQAM	11K9G1DEN	11.9	12.5
62.50	64QAM	11K9G1DEN	11.9	12.5
83.33	256QAM	11K9G1DEN	11.9	12.5

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

Tab. 9.9: Channel spacing 25 kHz

Channel spacing[kHz]	25				
Occupied BW limit[kHz]	14	16	16	20	25
Modulation type	FSK		QAM		
RipEX 1 "Mode"		CE	Narrow	FCC	CE
Baudrate [kBaud]	8.68	10.42	13.89	17.36	20.83
RipEX2 Compliance	RED FCC, ISSED	RED FCC, ISSED	RED FCC, ISSED	RED FCC, ISSED	RED

25 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 8.68 kBaud				
8.68	2CPFSK	13K5F1DBN	13.5	14
17.36	4CPFSK	12K2F1DDN	12.2	14
Baudrate 10.42 kBaud				
10.42	2CPFSK	15K5F1DBN	15.5	16
20.83	4CPFSK	15K5F1DDN	15.5	16
Baudrate 13.89 kBaud				
13.89	DPSK	15K9G1DBN	15.9	16
27.78	$\pi/4$ -DQPSK	15K9G1DDN	15.9	16
41.67	D8PSK	15K9G1DEN	15.9	16
55.56	16DEQAM	15K9G1DEN	15.9	16
83.33	64QAM	15K9G1DEN	15.9	16
111.11	256QAM	15K9G1DEN	15.9	16
Baudrate 17.36 kBaud				
17.36	DPSK	19K8G1DBN	19.8	20
34.72	$\pi/4$ -DQPSK	19K8G1DDN	19.8	20
52.08	D8PSK	19K8G1DEN	19.8	20
69.44	16DEQAM	19K8G1DEN	19.8	20
104.17	64QAM	19K8G1DEN	19.8	20
138.89	256QAM	19K8G1DEN	19.8	20
Baudrate 20.83 kBaud				
20.83	DPSK	24K0G1DBN	24.0	25
41.67	$\pi/4$ -DQPSK	24K0G1DDN	24.0	25
62.50	D8PSK	24K0G1DEN	24.0	25
83.33	16DEQAM	24K0G1DEN	24.0	25
125.00	64QAM	24K0G1DEN	24.0	25
166.67	256QAM	24K0G1DEN	24.0	25

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

Tab. 9.10: Channel spacing 50 kHz

Channel spacing [kHz]	50	
Occupied BW limit [kHz]	40	50
Modulation type	QAM	
RipEX 1 "Mode"	CE	Unlimited
Baudrate [kBaud]	34.72	41.67
RipEX2 Compliance	RED	RED

50 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 34.72 kBaud				
34.72	DPSK	40K0G1DBN	40.0	40
69.44	$\pi/4$ -DQPSK	40K0G1DDN	40.0	40
104.17	D8PSK	40K0G1DEN	40.0	40
138.89	16DEQAM	40K0G1DEN	40.0	40
208.33	64QAM	40K0G1DEN	40.0	40
277.78	256QAM	40K0G1DEN	40.0	40
Baudrate 41.67 kBaud				
41.67	DPSK	45K0G1DBN	45.0	50
83.33	$\pi/4$ -DQPSK	45K0G1DDN	45.0	50
125.00	D8PSK	45K0G1DEN	45.0	50
166.67	16DEQAM	45K0G1DEN	45.0	50
250.00	64QAM	45K0G1DEN	45.0	50
333.33	256QAM	45K0G1DEN	45.0	50

50 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10 ⁻²	BER 10 ⁻³	BER 10 ⁻⁶	[dB]
Baudrate 41.67 kBaud							
41.67	31.25	3/4	DPSK	-114	-113	-109	-7
41.67	41.67	Off	DPSK	-114	-112	-107	-7
83.33	62.50	3/4	$\pi/4$ -DQPSK	-113	-112	-108	-10
83.33	83.33	Off	$\pi/4$ -DQPSK	-112	-110	-105	-11
125.00	93.75	3/4	D8PSK	-110	-108	-103	-13
125.00	125.00	Off	D8PSK	-107	-104	-98	-15
166.67	125.00	3/4	16DEQAM	-107	-104	-98	-17
166.67	166.67	Off	16DEQAM	-105	-102	-95	-19
250.00	166.67	2/3	64QAM	-107	-103	-96	-17
250.00	187.50	3/4	64QAM	-105	-101	-94	-20
250.00	208.33	5/6	64QAM	-104	-99	-92	-21
250.00	250.00	Off	64QAM	-101	-96	-89	-23
333.33	222.22	2/3	256QAM	-101	-98	-92	-22
333.33	250.00	3/4	256QAM	-100	-97	-90	-23
333.33	277.78	5/6	256QAM	-98	-95	-88	-25
333.33	333.33	Off	256QAM	-95	-92	-85	-31

Tab. 9.11: Channel spacing 100 kHz

Channel spacing [kHz]	100	
Occupied BW limit [kHz]	80	100
Modulation type	QAM	
Baudrate [kBaud]	69.44	83.3
RipEX2 Compliance	RED	

100 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 69.44 kBaud				
69.44	DPSK	80K0G1DBN	80.0	80
138.89	$\pi/4$ -DQPSK	80K0G1DDN	80.0	80
208.33	D8PSK	80K0G1DEN	80.0	80
277.78	16DEQAM	80K0G1DEN	80.0	80
416.66	64QAM	80K0G1DEN	80.0	80
555.55	256QAM	80K0G1DEN	80.0	80

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

Tab. 9.12: Channel spacing 150 kHz

Channel spacing [kHz]	150	
Occupied BW limit [kHz]	125	150
Modulation type	QAM	
Baudrate [kBaud]	115.74	124.01
RipEX2 Compliance	RED	

150 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 115.74 kBaud				
115.74	DPSK	125KG1DBN	125.0	125
231.48	$\pi/4$ -DQPSK	125KG1DDN	125.0	125
347.22	D8PSK	125KG1DEN	125.0	125
462.96	16DEQAM	125KG1DEN	125.0	125
694.45	64QAM	125KG1DEN	125.0	125
925.93	256QAM	125KG1DEN	125.0	125

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

Tab. 9.13: Channel spacing 200 kHz

Channel spacing [kHz]	200
Occupied BW limit [kHz]	175
Modulation type	QAM
Baudrate [kBaud]	138.89
RipEX2 Compliance	RED

200 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 138.89 kBaud				
138.89	DPSK	150KG1DBN	150.0	175
277.78	$\pi/4$ -DQPSK	150KG1DDN	150.0	175
416.67	D8PSK	150KG1DEN	150.0	175
555.56	16DEQAM	150KG1DEN	150.0	175
833.33	64QAM	150KG1DEN	150.0	175
1111.11	256QAM	150KG1DEN	150.0	175

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

Tab. 9.14: Channel spacing 250 kHz

Channel spacing [kHz]	250
Occupied BW limit [kHz]	250
Modulation type	QAM
Baudrate [kBaud]	208.33

250 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 208.33 kBaud				
208.33	DPSK	225KG1DBN	225.0	250
416.67	$\pi/4$ -DQPSK	225KG1DDN	225.0	250
625.00	D8PSK	225KG1DEN	225.0	250
833.33	16DEQAM	225KG1DEN	225.0	250
1250.00	64QAM	225KG1DEN	225.0	250
1388.89	256QAM	225KG1DEN	225.0	250

250 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10⁻²	BER 10⁻³	BER 10⁻⁶	[dB]
Baudrate 208.33 kBaud							
208.33	156.25	3/4	DPSK	-107	-106	-102	-7
208.33	208.33	Off	DPSK	-107	-105	-100	-7
416.67	312.50	3/4	$\pi/4$ -DQPSK	-106	-105	-101	-10
416.67	416.67	Off	$\pi/4$ -DQPSK	-105	-103	-98	-11
625.00	468.75	3/4	D8PSK	-103	-101	-96	-13
625.00	625.00	Off	D8PSK	-100	-97	-91	-15
833.33	625.00	3/4	16DEQAM	-100	-97	-93	-17
833.33	833.33	Off	16DEQAM	-98	-95	-88	-19
1250.00	833.33	2/3	64QAM	-100	-96	-89	-17
1250.00	937.50	3/4	64QAM	-98	-94	-88	-20
1250.00	1041.67	5/6	64QAM	-97	-92	-86	-21
1250.00	1250.00	Off	64QAM	-96	-91	-84	-23
1388.89	1111.11	2/3	256QAM	-94	-91	-85	-22
1388.89	1250.00	3/4	256QAM	-93	-90	-83	-23
1388.89	1388.89	5/6	256QAM	-91	-88	-81	-25

Tab. 9.15: Channel spacing 300 kHz

Channel spacing [kHz]	300
Occupied BW limit [kHz]	300
Modulation type	QAM
Baudrate [kBaud]	260.42

300 kHz				
Modulation rate [kb/s]	Modulation	Emission code	OBW [kHz]	OBW limit [kHz]
Baudrate 260.42 kBaud				
260.42	DPSK	280KG1DBN	280.0	300
520.83	$\pi/4$ -DQPSK	280KG1DDN	280.0	300
781.25	D8PSK	280KG1DEN	280.0	300
1041.67	16DEQAM	280KG1DEN	280.0	300
1562.50	64QAM	280KG1DEN	280.0	300
1736.11	256QAM	280KG1DEN	280.0	300

300 kHz							
Classification				Sensitivity [dBm]			Co-Channel Rejection Ratio
Modulation rate [kb/s]	Bitrate [kb/s]	FEC	Modulation	BER 10⁻²	BER 10⁻³	BER 10⁻⁶	[dB]
Baudrate 260.42 kBaud							
260.42	195.31	3/4	DPSK	-106	-104	-100	-7
260.42	260.42	Off	DPSK	-105	-103	-98	-7
520.83	390.63	3/4	$\pi/4$ -DQPSK	-105	-103	-99	-10
520.83	520.83	Off	$\pi/4$ -DQPSK	-104	-102	-96	-11
781.25	585.94	3/4	D8PSK	-101	-99	-94	-13
781.25	781.25	Off	D8PSK	-99	-95	-89	-15
1041.67	781.25	3/4	16DEQAM	-98	-95	-91	-17
1041.67	1041.67	Off	16DEQAM	-96	-93	-86	-19
1562.50	1041.67	2/3	64QAM	-98	-94	-87	-17
1562.50	1171.88	3/4	64QAM	-96	-92	-86	-20
1562.50	1302.09	5/6	64QAM	-95	-90	-84	-21
1562.50	1562.50	Off	64QAM	-92	-87	-81	-23
1736.11	1388.89	2/3	256QAM	-93	-89	-83	-22
1736.11	1562.50	3/4	256QAM	-91	-88	-81	-23
1736.11	1736.11	5/6	256QAM	-90	-86	-79	-25

9.2. Recommended MSE thresholds

Tab. 9.16: 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
$\pi/4$ -DQPSK	3/4	-12
$\pi/4$ -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

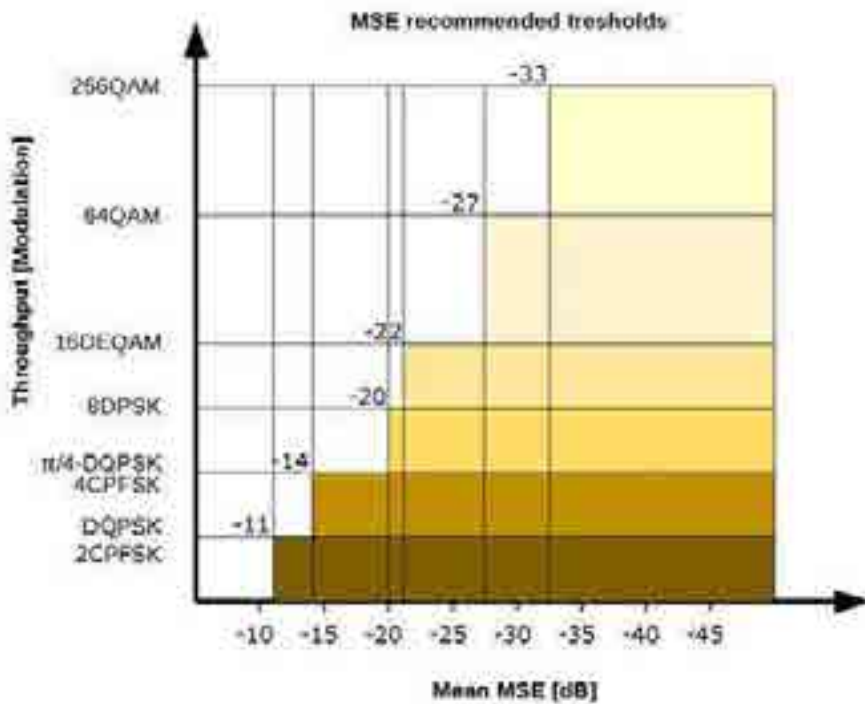


Fig. 9.1: MSE recommended thresholds

10. Safety, regulations, warranty

10.1. Frequency

The radio modem must be operated only in accordance with the valid frequency license issued by national frequency authority and all radio parameters have to be set exactly as listed.



Important

Use of frequencies between 406.0 and 406.1 MHz is worldwide-allocated only for International Satellite Search and Rescue System. These frequencies are used for distress beacons and are incessantly monitored by the ground and satellite Cospas-Sarsat system. Other use of these frequencies is forbidden.



Important

The radio operator is responsible for setting the radio parameters of the radio modem exactly in accordance with the valid frequency license issued by national frequency authority, and all radio parameters to be set exactly as listed.

10.2. Safety distance



Concentrated energy from a directional antenna may pose a health hazard to humans. Do not allow people to come closer to the antenna than the distances listed in the table below when the transmitter is operating. More information on RF exposure can be found online at the following website (OET Bulletin No. 65): <http://www.fcc.gov/oet/info/documents/bulletins>



Concentré d'énergie à partir d'une antenne directionnelle peut poser un risque pour 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 (OET Bulletin No. 65): www.fcc.gov/oet/info/documents/bulletins¹

The minimal safe distance is typically ensured by the antenna position on a mast. When special installation is required, the conditions of the standard EN 50385: 2002 have to be met. The distance between the persons and antenna shown in the table below comply with all applicable standards for human exposure of general public to RF electromagnetic fields.

Tab. 10.1: Minimum Safety Distance 300–470 MHz

300–470 MHz/70 cm band – 10 W RF power					
Antenna code	Antenna description	Gain G [dBi]	Gain G [–]	Dist. where the FCC limits are met for	
				General Population / Uncontrolled Exposure [cm]	General Population / Controlled Exposure [cm]
OV380.1	single dipole	4.6	2.9	130	60
OV380.2	stacked double dipole	7.6	5.8	180	80
SA380.3	3 element directional Yagi	7.6	5.8	180	80

¹ <http://www.fcc.gov/oet/info/documents/bulletins>

300–470 MHz/70 cm band – 10 W RF power					
SA380.5	5 element directional Yagi	8.7	7.4	200	90
SA380.9	9 element directional Yagi	12.5	17.8	310	140

Tab. 10.2: Minimum Safety Distance 135–175 MHz

135 - 175 MHz / 2 m band – 10 W RF power					
Antenna code	Antenna description	Gain G [dBi]	Gain G [–]	Dist. where the FCC limits are met for	
				General Population / Uncontrolled Exposure [cm]	General Population / Controlled Exposure [cm]
OV138.1	single dipole	4.6	2.9	155	55
OV138.2	stacked double dipole	7.6	5.8	215	75
SA138.3	3 element directional Yagi	8.0	6.3	225	80
SA138.5	5 element directional Yagi	10.0	10.0	285	100

Tab. 10.3: Minimum Safety Distance 135–175 MHz according to RSS-102

135 - 175 MHz / 2 m band – 10 W RF power					
Antenna code	Antenna description	Gain G [dBi]	Gain G [–]	Dist. where the limits are met for	
				General Population / Uncontrolled Exposure [cm]	General Population / Controlled Exposure [cm]
OV138.1	single dipole	4.6	2.9	170	70
OV138.2	stacked double dipole	7.6	5.8	240	95
SA138.3	3 element directional Yagi	8.0	6.3	250	100
SA138.5	5 element directional Yagi	10.0	10.0	315	125

10.3. High temperature



If the RipEX2 is operated in an environment where the ambient temperature exceeds 55 °C, the RipEX2 must be installed within a restricted access location to prevent human contact with the enclosure heatsink.

10.4. Battery disposal

Battery Disposal - This product may contain a battery (e.g. CRC1225, 3V, 48 mAh). Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste. Batteries are marked with a symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point.

10.5. 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. SW license

Conditions of use of this product software abide by the license mentioned below. The program spread by this license has been freed with the purpose to be useful, but without any specific guarantee. The author or another company or person is not responsible for secondary, accidental or related damages resulting from application of this product under any circumstances.

RACOM Open Software License

Version 1.0, November 2009

Copyright (c) 2001, RACOM s.r.o., Mírová 1283, Nové Město na Moravě, 592 31

Everyone can copy and spread word-for-word copies of this license, but any change is not permitted.

The program (binary version) is available for free on the contacts listed on <https://www.racom.eu>. This product contains open source or another software originating from third parties subject to GNU General Public License (GPL), GNU Library / Lesser General Public License (LGPL) and / or further author licenses, declarations of responsibility exclusion and notifications. Exact terms of GPL, LGPL and some further licenses is mentioned in source code packets (typically the files COPYING or LICENSE). You can obtain applicable machine-readable copies of source code of this software under GPL or LGPL licenses on contacts listed on <https://www.racom.eu>. This product also includes software developed by the University of California, Berkeley and its contributors.

Waste Framework Directive Statement

According to the Directive 2008/98/EC on waste amended by Directive (EU) 2015/1127 and Directive (EU) 2018/851 (Waste Framework Directive) we hereby state that our products doesn't contain substances of very high concern (SVHC) listed on European chemical agency (ECHA) SCIP database candidate list in concentrations above 0.1 % w/w.

10.7.2. EU restrictions or requirements notice

Radio equipment used within the EU countries listed below:

- there are restrictions on putting into service or
- any requirements for authorisation of use.



BE	BG	CZ	DK	DE	EE	IE
EL	ES	FR	HR	IT	CY	LV
LT	LU	HU	MT	NL	AT	PL
PT	RO	SI	SK	FI	SE	UK

Fig. 10.2: EU restrictions or requirements

The RipEX2 radio modem predominantly operates within frequency bands that require a site license be issued by the radio regulatory authority with jurisdiction over the territory in which the equipment is being operated.

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/EE.

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.

10.8. 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. 10.4: 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	RSS-102	24993-RIPEX24A

Possible values for channels, channel spacing and occupied bandwidth fulfilling FCC rules are shown in *Chapter 9, Technical parameters*.



Important

The radio operator is responsible for setting the radio parameters of the radio modem exactly in accordance with the valid frequency license issued by national frequency authority, and all radio parameters to be set exactly as listed.

TCB**GRANT OF EQUIPMENT
AUTHORIZATION****TCB**

Certification
Issued Under the Authority of the
Federal Communications Commission
By:

TUV SUD America Inc.
 10 Centennial Drive
 Peabody, MA 01960

Date of Grant: 01/23/2020

Application Dated: 01/22/2020

Racom
 Mirova cp. 1283
 Nove Mesto na Morave, 592 31
 Czech Republic

Attention: Jiri Hruska , Programme Manager

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE,
 and is VALID ONLY for the equipment identified hereon for use under the
 Commission's Rules and Regulations listed below.

FCC IDENTIFIER: SQT-RIPEX2-4A

Name of Grantee: Racom

Equipment Class: Licensed Non-Broadcast Station Transmitter

Notes: Radio modem and router

<u>Grant Notes</u>	<u>FCC Rule Parts</u>	<u>Frequency Range (MHz)</u>	<u>Output Watts</u>	<u>Frequency Tolerance</u>	<u>Emission Designator</u>
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	19K8G1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	15K5F1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	10K0G1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	7K50F1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	5K0G1D
EF ES	90	406.1 - 450.0	10.0	102.0 Hz	3K60F1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	19K8G1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	15K5F1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	10K0G1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	7K50F1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	5K0G1D
EF ES	90	450.0 - 454.0	10.0	102.0 Hz	3K60F1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	19K8G1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	15K5F1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	10K0G1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	7K50F1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	5K0G1D
EF ES	90	456.0 - 462.5375	10.0	102.0 Hz	3K60F1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	19K8G1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	15K5F1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	10K0G1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	7K50F1D

Fig. 10.4: TCB authorization

EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	5K0G1D
EF ES	90	462.7375 - 467.5375	10.0	102.0 Hz	3K60F1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	19K8G1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	15K5F1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	10K0G1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	7K50F1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	5K0G1D
EF ES	90	467.7375 - 470.0	10.0	102.0 Hz	3K60F1D

Output power listed is rated conducted power. The device is designed for professional installation, users and installers must be provided with appropriate antenna installation instructions and transmitter operating conditions, including antenna co-location requirements of § 1.1307(b)(3), for satisfying RF exposure compliance. The antennas used for this transmitter shall be installed to provide a separation distance from all persons during normal operation as documented in this filing. RF exposure compliance may need to be addressed at the time of licensing.

EF: This device may contain functions that are not operational in U.S Territories except as noted in the filing. This grant has extended frequencies as noted in the filing and Section 2.927(b) applies to this authorization.

ES: This equipment is capable of supporting a minimum data rate of 4800 bits per second per 6.25 kHz of channel bandwidth.

Fig. 10.5: TCB authorization



FCB Technical Acceptance Certificate

CB Number: US0156

ISSUED TO	➤ RACOM s.r.o. RACOM, Mirova 1283 Nove Mesto na Morave 592 31 Czech Republic
CERTIFICATION No.	➤ 24993-RIPEX24A
DESCRIPTION	➤ Wireless modem router
TYPE OF EQUIPMENT	➤ Land-Mobile Transmitter and Receiver (27.41–960 MHz)
HVIN(s)	➤ RipEX2-4
PMN(s)	➤ RipEX2-4
FVIN(s)	➤ N/A
TYPE OF LISTING:	➤ New Single Certification
ANTENNA INFORMATION	➤ External Antenna, 12.5 dBi Max
RF EVALUATION TYPE	➤ RF Evaluation
MANUFACTURING No.	➤ 24993
REPRESENTATIVE No.	➤ 10842A
TEST LAB No.	➤ 3036B
TESTING LABORATORY	➤ Professional Testing (EMI) Inc. 11400 Burnet Road, Austin, Texas, 78758, United States Tel: 512-244-3371; Fax: 512-244-1846 Contact: Larry Finn; E-mail: lfinn@ptitest.com

Authorised by: 

Title of Signatory: **Wireless Certification Manager**
On Behalf of TÜV SÜD America

I hereby attest that the subject equipment was tested and found in compliance with the above-noted specification.

Certification of equipment means only that the equipment has met the requirements of the above-noted specification. Licence applications, where applicable to use certified equipment, are acted on accordingly by the ISDE issuing office and will depend on the existing radio environment, service and location of operation. This certificate is issued on condition that the holder complies and will continue to comply with the requirements and procedures issued by ISDE. The equipment for which this certificate is issued shall not be manufactured, imported, distributed, leased, offered for sale or sold unless the equipment complies with the applicable technical specifications and procedures issued by ISDE.;

Certified Equipment shall not be distributed, leased, sold or offered for sale in Canada before the details of the certification have been added to the REL. This certificate has been issued in accordance with the Testing and Certification Regulations of TÜV SÜD America. For further details related to this certification please contact Certification@tuvam.com

Issue Date: 12th March 2020

Number: CB-19-0187 Issue: 1

J'atteste, par la présente, que le matériel a fait l'objet d'essai et a été jugé conforme à la spécification ci-dessus.

La certification du matériel signifie seulement que le matériel a satisfait aux exigences de la norme indiquée ci-dessus. Les demandes de licences nécessaires pour l'utilisation du matériel certifié sont traitées en conséquence par le bureau de délivrance d'ISDE et dépendent des conditions radio ambiantes, du service et de l'emplacement d'exploitation. Le présent certificat est délivré à la condition que le titulaire satisfasse et continue de satisfaire aux exigences et aux procédures d'ISDE. Le matériel à l'égard duquel le présent certificat est délivré ne doit pas être fabriqué, importé, distribué, loué, mis en vente ou vendu à moins d'être conforme aux procédures et aux spécifications techniques applicables publiées par ISDE.

UCB_F_10.09 Rev 1 TÜV SÜD America, Inc. 10 Centennial Drive, Peabody, MA 01960, USA Page 1 of 2

Fig. 10.6: FCB certificate



Radio Details

Number: CB-19-0187 Issue 1

Frequency Min (MHz)	Frequency Max (MHz)	RF Power (W)		Emission Designator	Specification Issue
Min	Max	Min	Max		
406.1	430.0	11.8	11.8	19K8G1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	15K5F1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	10K0G1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	7K50F1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	5K00G1D	RSS-119 Issue 12
406.1	430.0	11.8	11.8	3K60F1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	19K8G1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	15K5F1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	10K0G1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	7K50F1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	5K00G1D	RSS-119 Issue 12
450.0	470.0	11.8	11.8	3K60F1D	RSS-119 Issue 12

Fig. 10.7: FCB certificate

10.9. Compliance ANATEL Brasil

RipEX2-4A : RipEX2-4A : This equipment is approved by ANATEL under number 16763-20-08917.

10.10. 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.

10.11. RipEX2 Availability and service life time

Annual availability is $\geq 99.99\%$ (for MTTR = 8 hours and P-t-P scenario)

The Availability depends on specific network design and Service availability. Availability can be increased by decreasing MTTR. Availability calculation needs to be done for each network element separately.

RipEX 2 redundant solution within Field Replaceable Units fully achieving the level availability and reliability for the Core elements.



Note

Core networks elements(repeaters/bases) are typically designed for high availability i.e. needs to be 99.999% available with any single component (radio node) fails.

Service life of system ≥ 15 years

10.12. RipEX2 maintenance

Action	Period	Note
Visual check – Antenna:	Quarterly	

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

Abbreviations

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

A

- accessories, 27
- addressing
 - bridge, 39
- antenna, 15
 - mounting, 33
- AUX, 20

B

- base driven protocol, 40

C

- connectors, 15
- Copyright, 7

D

- default
 - parameters, 8
 - setting, 22
- dimensions, 12

E

- environment, 177

F

- flexible protocol, 40

G

- grounding, 34

I

- installation, 28
- IP/serial, 47

L

- LED, 22

M

- mode
 - router, 40
 - base driven, 40
- model offerings, 24
- mounting
 - bracket, 30
 - DIN rail, 29
 - IP52, 32

P

- product
 - conformity
 - EU, 182

Q

- quick guide, 8

R

- radio
 - parameters, 160
- reset, 22
- RoHS and WEEE, 180
- router, 40

S

- safety, 177
 - distance, 177

T

- technical parameters, 151

W

- warranty, 177

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 First issue	2018-11-11
Revision 1.0 Chapter Technical parameters updated.	2019-07-30
Revision 1.1 Minor improvements	2019-09-10
Revision 1.2 Added chapter 6 (<i>Web interface</i>) and 7 (<i>Settings</i>).	2019-10-04
Revision 1.3 Chapter 7 (<i>Settings</i>) improved.	2019-11-14
Revision 1.4 Bridge mode and Transparent radio protocol added.	2019-11-20
Revision 1.5 Minor modification of chapters 5-7, TBC grant added	2020-01-24
Revision 1.6 Screenshots updated according to version 1.3.6.0 Chapter Technical parameters updated.	2020-02-28
Revision 1.7 Added new features of 1.4.3.0 fw	2020-06-25
Revision 1.8 Added new features of 1.4.5.0 fw	2020-08-28
Revision 1.9 Minor modification of chapter 7	2020-10-23
Revision 1.10 Chapter 3 and 9 rework	2021-02-11
Revision 1.11 FW 2.0.0.0 features	2021-04-19