4.4. Technical specification

Tab. 4.6: Technical parameters

Radio parameters			
Frequency bands		135–175*; 300–330*; 330–350; 350–370*; 368–470; 928–960* MHz	
Channel spacing		6.25 / 12.5 / 25 kHz	
Frequency stability		±1.0 ppm	
Modulation		16DEQAM, D8PSK, π/4DQPSK, DPSKΩ 4CPFSK, 2CPFSK	Detail
RF Data rate Detail	25 kHz	83.33 – 62.50 – 41.67 kbps 20.83 – 10.42 kbps	max. 2 W max. 10 W
	12.5 kHz	41.67 – 31.25 – 20.83 kbps 10.42 – 5.21 kbps	max. 2 W max. 10 W
	6.25 kHz	20.83 – 15.63 – 10.42 kbps 5.21 – 2.60 kbps	max. 2 W max. 10 W
FEC (Forward Error Correction)		On/Off, ¾ Trellis code with Viterbi soft-decoder	
Transmitter			
Carrier Output power	supply	output power [W]	modulation
	10–30 VDC	0.1 - 0.2 - 0.5 - 1.0 - 2.0 - 3.0 - 4.0 - 5.0 - 10 **	CPFSK
		0.5 - 1.0 - 2.0	others
Duty cycle		Continuous	
Rx to Tx Time		< 1.5 ms	
Intermodulation Attenuation		> 40 dB	
Spurious Emissions (Conducted)		< −36 dBm	
Radiated Spurious Emissions		< −36 dBm	
Adjacent channel power		< −60 dBc	
Transient adjacent channel power		< −60 dBc	
Receiver			
Sensitivity			Detail
Anti-aliasing Selectivity		50 kHz @ −3 dB BW	
Tx to Rx Time		< 1.5 ms	
Maximum Receiver Input Power		20 dBm (100 mW)	
Rx Spurious Emissions (Conducted)		< −57 dBm	
Radiated Spurious Emissions		< −57 dBm	
Blocking or desensitization			Detail
Spurious response rejection		> 70 dB	
* not available yet ** For output power 10 W it is recommended to use input power above 11 VDC			

Electrical			
Primary power		10 to 30 VDC, negative GND	
Rx		5 W (360 mA/13.8 V; 200 mA/24 V)	
Tx 4CPFSK, 2CPFSK	0.1 W	1.0 A/13.8 V; 0.55 A/24V; 14 W	
	1 W	1.1 A/13.8 V; 0.6 A/24 V; 15 W	
	5 W	2.4 A/13.8 V; 1.3 A/24 V; 33 W	
	10 W	3.0 A/13.8 V; 1.6 A/24 V; 42 W	
Tx 16DEQAM, D8PSK, π/4DQPSK	0.1 W	2.2 A/13.8 V; 1.25 A/24 V; 30 W	
	1 W	2.2 A/13.8 V; 1.25 A/24 V; 30 W	
	2 W	2.2 A/13.8 V; 1.25 A/24 V; 30 W	
Sleep mode		7 mA/13.8 V, 0.1 W; 6 mA/24 V; 0.15 W	
Save mode		170 mA/13.8 V; 95 mA/24 V; 2.3 W	
Interfaces			
Ethernet		10/100 Base-T Auto MDI/MDIX	RJ45
COM 1		RS232	DB9F
		300–115 200 bps	
COM 2		RS232/RS485 SW configurable	DB9F
		300–115 200 bps	
USB		USB 1.1	Host A
Antenna		50 Ω	TNC female
LED panel			
7× tri-color status LEDs		Power, ETH, COM1, COM2, Rx, Tx, Status	
Enviromental			
Operating temperature		−40 to +70 °C (−40 to +158 °F)	
Humidity		5 to 95 % non-condensing	
Storage temperature		−40 to +85 °C (−40 to +185 °F)	
Mechanical			
Casing		Rugged die-cast aluminium	
Dimensions		50 H × 150 W × 118 mm D (1.97× 5.9 × 4.65 in)	
Weight		1.1 kg (2.4 lbs)	
Mounting		DIN rail, L-bracket, Flat-bracket, 19" Rack shelf	
SW			
Operating modes		Bridge / Router	
User protocols on COM		Modbus, IEC101, DNP3, UNI, Comli, DF1, Profibus…	
User protocols on Ethernet		Modbus TCP, IEC104, DNP3 TCP, Comli TCP Terminal server…	
Serial to IP convertors		Modbus RTU / Modbus TCP, DNP3 / DNP3 TCP	
Protocol on Radio channel			
Multi master applications		Yes	
Report by exception		Yes	

Collision Avoidance Capability	Yes
Remote to Remote communication	Yes
Addressed & acknowledged serial SCADA protocols	Yes
Data integrity control	CRC 32
Encryption	AES256
Optimization	up to 3× higher throughput
Diagnostic and Management	
Radio link testing	Yes (ping with RSS, Data Quality, Homogenity)
Watched values in each radiomodem (broadcast to other radiomodems)	Rx/Tx packets for ETH, COM1, COM2 Rx/Tx packets on User interfaces and for User data
Statistics	Rx/Tx Packets on User interfaces and for User data and Radio protocol (Repeates, Lost, ACK etc.) on Radio channel
Graphs	For Watched values and Statistics
History	20 periods (configurable, e.g. days)
SNMP	SNMPv1, SNMPv2 Trap alarms generation for Watched values
Standards	
CE, FCC, RoHS	
Radio	ETSI EN 300 113-2
	ETSI EN 302 561
	ETSI EN 301 166-2
	FCC Part 90
EMC (electromagnetic compatibility)	ETSI EN 301 489-1
	ETSI EN 301 489-5
Electrical Safety	EN 60950-1

4.4.1. Emission code

Tab. 4.7: Channel spacing 25 kHz, exponential modulation, CE

Channel spacing 25 kHz Exponential modulation | Symbol rate 10,42 kBaud || CE									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
2CPFSK	0,75	7,81	13K8F1DCN	-118	-115	-111	-8	-6	-5
2CPFSK	1,00	10,42	13K8F1DBN	-117	-114	-110	-10	-8	-7
4CPFSK	0,75	15,63	14K2F1DDN	-115	-112	-107	-9	-9	-7
4CPFSK	1,00	20,83	14K2F1DDN	-113	-110	-104	-11	-11	-9

Tab. 4.8: Channel spacing 25 kHz, linear modulation, CE

Channel spacing 25 kHz Linear modulation | Symbol rate 20,83 kBaud || CE									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
DPSK	0,75	15,62	24K0G1DCN	-114	-112	-107	-6	-6	-5
DPSK	1,00	20,83	24K0G1DBN	-113	-111	-106	-8	-8	-7
π/4-DQPSK	0,75	31,25	24K0G1DDN	-113	-110	-106	-4	-4	-3
π/4-DQPSK	1,00	41,66	24K0G1DDN	-111	-108	-104	-6	-6	-5
D8PSK	0,75	46,87	24K0G1DEN	-106	-103	-98	-8	-8	-8
D8PSK	1,00	62,49	24K0G1DEN	-104	-101	-95	-10	-10	-9,5
16DEQAM	0,75	62,49	24K0D1DEN	-104	-101	-95	-6	-6	-5
16DEQAM	1,00	83,32	24K0D1DEN	-102	-99	-93	-8	-8	-7

All values are guarenteed for temperatures from -25 to +60 °C (-13 to +140 °F) and for all frequency channels

Note: How to understand basic radio parameters of a radio modem.

The very first parameter which is often required to be taken into consideration is the receiver sensitivity. Each of those interested in the wireless data transmission probably knows what this parameter means, but we should see it simultaneously in its relation to other receiver parameters, especially the blocking and desensitization. Today's wireless communication arena tends to be overcrowded and a modern radio modem, which is demanded to compete, should have good dynamic range that is defined by the parameters listed above. The receiver of a radio modem, which is designed purely for optimum sensitivity, will not be able to give proper performance. However, the main receiver parameters determining

its dynamic range go against each other and a clear trade-off between the sensitivity and the blocking is therefore an essential assumption. Then, from the viewpoint of a logical comparison, the consequence of better receiver sensitivity can be easily seen – a lower power level of the blocking and degradation parameters generally.

Blocking or desensitization values were determined according to the standards ETSI 300 113-1 V1.7.1 (channels 25 and 12.5 kHz) and ETSI 301 166-1 V1.3.2 (channel 6.25 kHz) respectively.

Tab. 4.9: Channel spacing 12,5 kHz, exponential modulation, CE

Channel spacing 12,5 kHz Exponential modulation | Symbol rate 5,21 kBaud || CE									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
2CPFSK	0,75	3,91	7K00F1DCN	-120	-117	-113	-6	-4	-3
2CPFSK	1,00	5,21	7K00F1DBN	-119	-116	-112	-8	-6	-5
4CPFSK	0,75	7,81	7K00F1DDN	-117	-114	-108	-6	-6	-5
4CPFSK	1,00	10,42	7K00F1DDN	-115	-112	-105	-8	-8	-7

Tab. 4.10: Channel spacing 12,5 kHz, linear modulation, CE

Channel spacing 12,5 kHz Linear modulation | Symbol rate 10,42 kBaud || CE									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
DPSK	0,75	7,81	11K9G1DCN	-116	-114	-110	-4	-4	-3
DPSK	1,00	10,42	11K9G1DBN	-115	-113	-109	-6	-6	-5
π/4-DQPSK	0,75	15,62	11K9G1DDN	-115	-113	-109	-3,5	-3	-2
π/4-DQPSK	1,00	20,83	11K9G1DDN	-114	-111	-106	-4	-4	-3
D8PSK	0,75	23,44	11K9G1DEN	-109	-106	-101	-6	-6	-5
D8PSK	1,00	31,25	11K9G1DEN	-107	-104	-98	-8	-8	-7
16DEQAM	0,75	31,25	11K9D1DEN	-107	-104	-99	-3	-3	-2
16DEQAM	1,00	41,67	11K9D1DEN	-105	-102	-96	-5	-5	-4

Tab. 4.11: Channel spacing 25 kHz, exponential modulation, FCC

Channel spacing 25 kHz Exponential modulation | Symbol rate 10,42 kBaud || FCC									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
4CPFSK	0,75	15,63	18K6F1DDN	-116	-113	-108	-8	-8	-6
4CPFSK	1,00	20,83	18K6F1DDN	-114	-111	-105	-10	-10	-8

Tab. 4.12: Channel spacing 25 kHz, linear modulation, FCC

Channel spacing 25 kHz Linear modulation | Symbol rate 17,36 kBaud || FCC									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
π/4-DQPSK	0,75	26,04	19K8G1DDN	-113	-110	-106	-3	-3	-2
π/4-DQPSK	1,00	34,72	19K8G1DDN	-111	-108	-104	-5	-5	-4
D8PSK	0,75	39,06	19K8G1DEN	-106	-103	-98	-8	-7	-7
D8PSK	1,00	52,08	19K8G1DEN	-104	-101	-95	-10	-9	-9
16DEQAM	0,75	52,08	19K8D1DEN	-104	-101	-95	-4	-4	-3
16DEQAM	1,00	69,44	19K8D1DEN	-102	-99	-93	-6	-6	-5

Tab. 4.13: Channel spacing 12,5 kHz, exponential modulation, FCC

Channel spacing 12,5 kHz Exponential modulation | Symbol rate 5,21 kBaud || FCC									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
4CPFSK	0,75	7,81	8K90F1DDN	-117	-114	-108	-5	-5	-4
4CPFSK	1,00	10,42	8K90F1DDN	-115	-112	-105	-7	-7	-6

Tab. 4.14: Channel spacing 12,5 kHz, linear modulation, FCC

Channel spacing 12,5 kHz Linear modulation | Symbol rate 10,42 kBaud || FCC									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
π/4-DQPSK	0,75	13,02	10K0G1DDN	-115	-113	-109	-2	-2	-2
π/4-DQPSK	1,00	17,36	10K0G1DDN	-114	-111	-106	-4	-4	-3
D8PSK	0,75	19,53	10K0G1DEN	-109	-106	-101	-6	-6	-5
D8PSK	1,00	26,04	10K0G1DEN	-107	-104	-98	-8	-8	-7
16DEQAM	0,75	26,04	10K0D1DEN	-107	-104	-99	-3	-3	-2
16DEQAM	1,00	34,72	10K0D1DEN	-105	-102	-96	-5	-5	-4

Tab. 4.15: Channel spacing 6,25 kHz, exponential modulation, FCC

Channel spacing 6,25 kHz Exponential modulation | Symbol rate 2,60 kBaud || FCC									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
4CPFSK	0,75	3,91	4K35F1DDN	-120	-117	-112	-2	-2	-2
4CPFSK	1,00	5,21	4K35F1DDN	-118	-115	-109	-4	-4	-3

Tab. 4.16: Channel spacing 6,25 kHz, linear modulation, FCC

Channel spacing 6,25 kHz Linear modulation | Symbol rate 4,34 kBaud || FCC									
Classification				Sensitivity			Blocking or desensitization		
Modulation	FEC Code Rate	Raw Bit Rate	Emission dsg.	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	±1 MHz	±5 MHz	±10 MHz
[–]	[–]	[kbit/s]	[–]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
π/4-DQPSK	0,75	6,51	5K0G1DDN	-118	-116	-113	-3	-3	-2
π/4-DQPSK	1,00	8,68	5K0G1DDN	-117	-114	-111	-5	-5	-4
D8PSK	0,75	9,77	5K0G1DEN	-112	-110	-105	-2	-2	-2
D8PSK	1,00	13,02	5K0G1DEN	-110	-107	-102	-4	-4	-3
16DEQAM	0,75	13,02	5K0D1DEN	-110	-107	-103	-3	-3	-2
16DEQAM	1,00	17,36	5K0D1DEN	-108	-105	-100	-5	-5	-4

4.5. Model offerings

Software feature keys

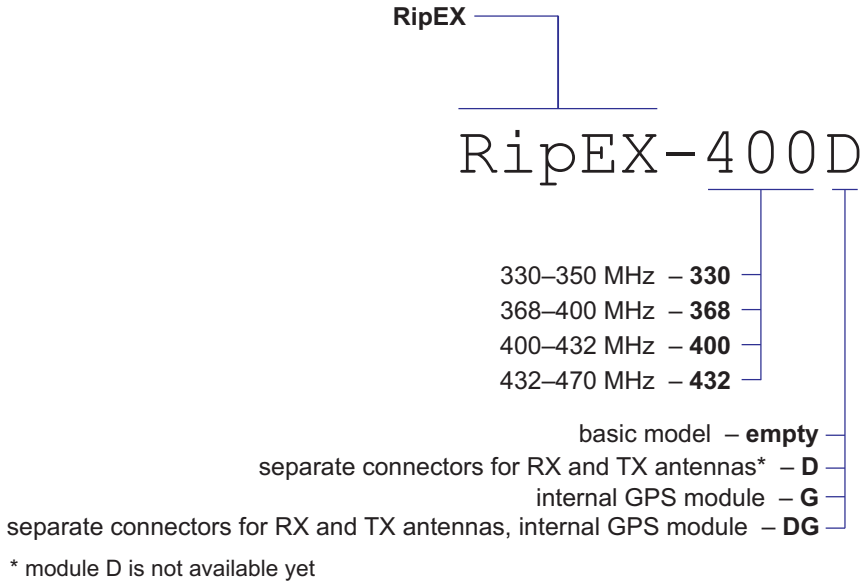
Certain advanced RipEX features are activated with software keys. Among such code protected features are the Router mode, High speed (83 kbps), COM2, 10 W and others. A Master key, which activates all coded features, is also available. Feature keys enable the users to initially purchase only the functionality they require and buy additional functions as the requirements and expectations grow. Similarly, when some features (e.g. COM2) are required on certain sites, the respective key can be activated only where needed.

- Keys protect the investment into the hardware. Thanks to SDR-based hardware design of RipEX no physical replacement is necessary – the user simply buys a key and activates the feature.
- For evaluation and testing, Time-limited keys can be supplied. These keys activate the coded feature for a limited operational (power on) time only.
- Software keys are always tied to a specific RipEX production code. When purchasing a software key, this production code must be given.

Model offerings

RipEX radio modem has been designed to have minimum possible number of hardware variants. Upgrade of functionality does not result in on-site hardware changes – it is done by activating software keys (see chapter *RipEX in detail* and *Adv. Config., Maintenance*).

Part Number – RipEX



Examples:

RipEX–368 = RipEX for frequencies from 368 to 400 MHz
RipEX–400G = RipEX for frequencies from 400 to 432 MHz, with GPS module
RipEX–432DG = RipEX for frequencies from 432 to 470 MHz, with two antenna connectors, with GPS module

Fig. 4.14: Part Number

4.6. Accessories

1. **RipEX Fan kit**

   External Fan kit for additional cooling in extreme temperatures. For connection see chapter *Connectors*.

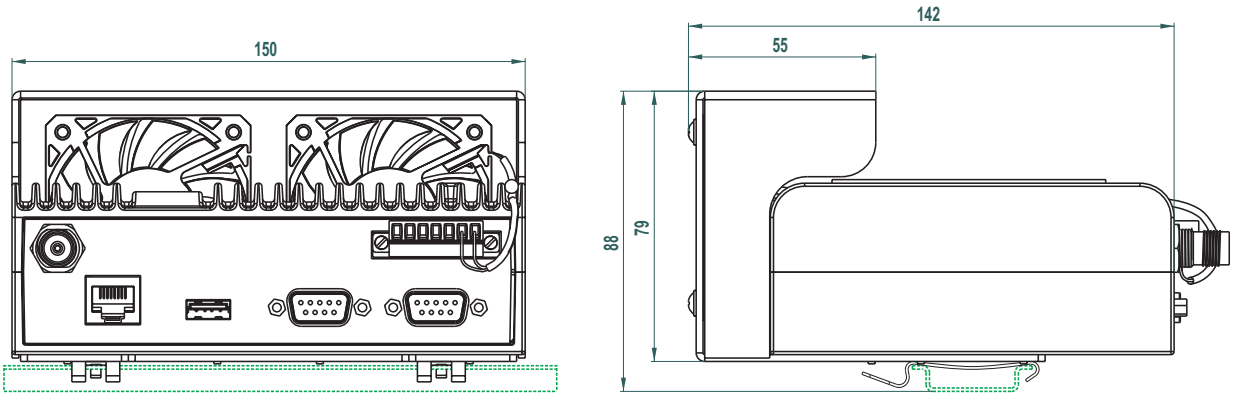


Fig. 4.15: Assembly dimensions with fan

2. **RipEX – Dummy load antenna**

   Dummy load antenna for RipEX is used to test the configuration on a desk. It is unsuitable for higher output – use transmitting output of 0.1 W only.

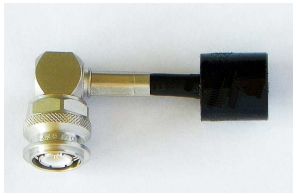


Fig. 4.16: Dummy load

3. **RipEX – L-bracket**

   Installation L bracket for vertical mounting. For details on use see chapter Mounting and chapter Dimensions.

Fig. 4.17: L-bracket

4. **RipEX – Flat-bracket**

   Installation bracket for flat mounting. For details on use see chapter Mounting and chapter Dimensions.

Fig. 4.18: Flat bracket

5. **RipEX – 19" rack shelf – single**

   For installation of a single RipEX into the standard 19” rack.

6. **RipEX – 19" rack shelf – double**

   For installation of 2 RipEX’s into the standard 19” rack.

Fig. 4.19: 19" Rack shelf

7. **X5 – ETH/USB adapter**

   ETH/USB adapter for service access to the web interface via USB connector. Includes a built-in DHCP server. To access the RipEX always use the fixed IP 10.9.8.7. For details on use see Section 5.3, “Connecting RipEX to a programming PC”.

Fig. 4.20: X5 adapter ETH/USB

8. **RipEX – Demo and field test kit**

   A rugged plastic case for carrying up to 3 RipEX's and accessories needed to perform an on-site signal measurement, complete application bench-test or a functional demostration of radiomodems.

Contains a MS2000/24 power supply connected via a switch to the 230 VAC socket. Three RipEX's connected to 24 VDC power supply and complete with dummy loads are ready for testing. ETH/USB adapter can be used for service access. During a field test, RipEX's can be powered from the backup battery and external antenna can be connected to one of them through a connector on the case.

Fig. 4.21: Demo case

Contents:
- Brackets for installation of three RipEX's (radiomodems are not part of the delivery)
- MS2000/24 power supply for 3 RipEX's
- 1× Backup battery
- 3× Dummy load antenna
- 1× Pig-tail for connecting an external antenna
- 1× L-bracket, 1× Flat-bracket
- 1× Fan kit
- 1× X5 – ETH/USB adapter
- Network cable
- Printed user manual
- Outside dimension: 455 × 365 × 185 mm
- Weight ca. 4 kg (excluding the RipEx's)

5. Bench test

5.1. Connecting the hardware

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

If you use your own installation for lab tests, don't forget:

- A dummy load or an actual antenna with 50 ohm impedance should be connected to the RipEX
- The minimum RF output must be set to avoid overloading the dummy antenna and to keep the received signal at reasonable level, between -40 and -80 dBm.
- The power supplies must meet the requirements given in the specifications, Table 4.6, "Technical parameters". 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 RipEX switches from reception to transmission and back.

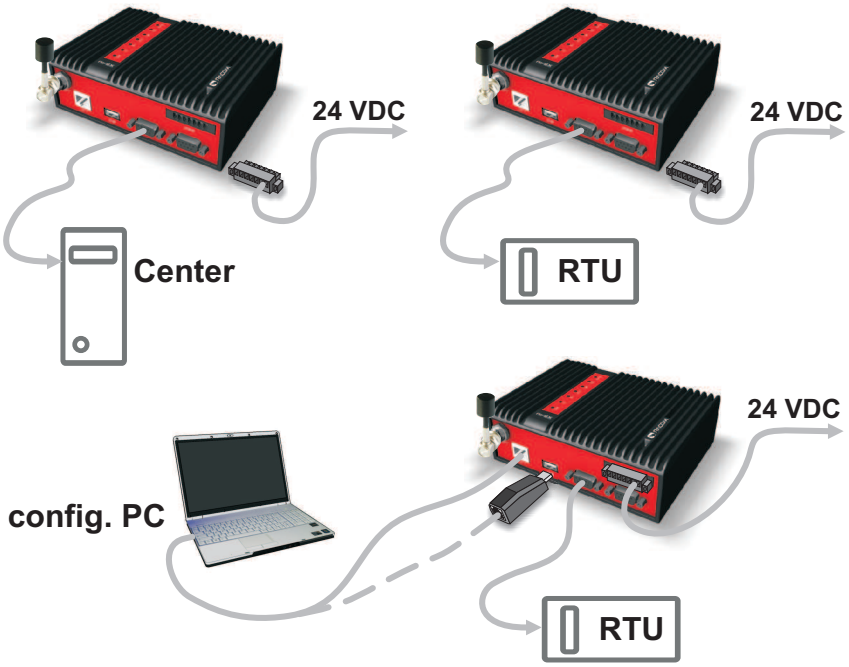


Fig. 5.1: Bench test

5.2. Powering up your RipEX

Switch on your power supply. LED PWR flashes quickly and after 8 seconds it switches to a green light. After approximately 30 seconds your RipEX will have booted and will be ready; the STATUS LED shines. You'll find the description of the individual LED states in Section 4.3, "Indication LEDs".

5.3. Connecting RipEX to a programming PC

To configure a RipEX you can connect it to your PC in two ways:

1. Using the "X5" - external ETH/USB adapter

2. Directly over the ethernet interface

Fig. 5.2: Connecting to a PC over ETH and over ETH/USB adapter

1. **PC connected via ETH/USB adapter**

   We recommend using the "X5" - external ETH/USB adapter (an optional accessory of the RipEX). The ETH/USB contains a built-in DHCP server, so if you have a DHCP client in your PC as most users, you don't need to set anything up. The RipEX's IP address for access over the ETH/USB adapter is fixed: 10.9.8.7.

   Go to 3. Login to RipEX

2. **PC connected directly to ETH port**

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

   Start > Settings > Network Connections > Local Area Connections
   Right Click > Properties > General
   select Internet Protocol (TCP/IP) > Properties > General
   IP address 192.168.169.250 - for RipEX in the default state
   Subnet mask 255.255.255.0
   Default gateway leave empty
   OK (Internet Protocol Properties window)
   OK (Local Area Properties window)
   Some Operating systems may require you to reboot your PC.

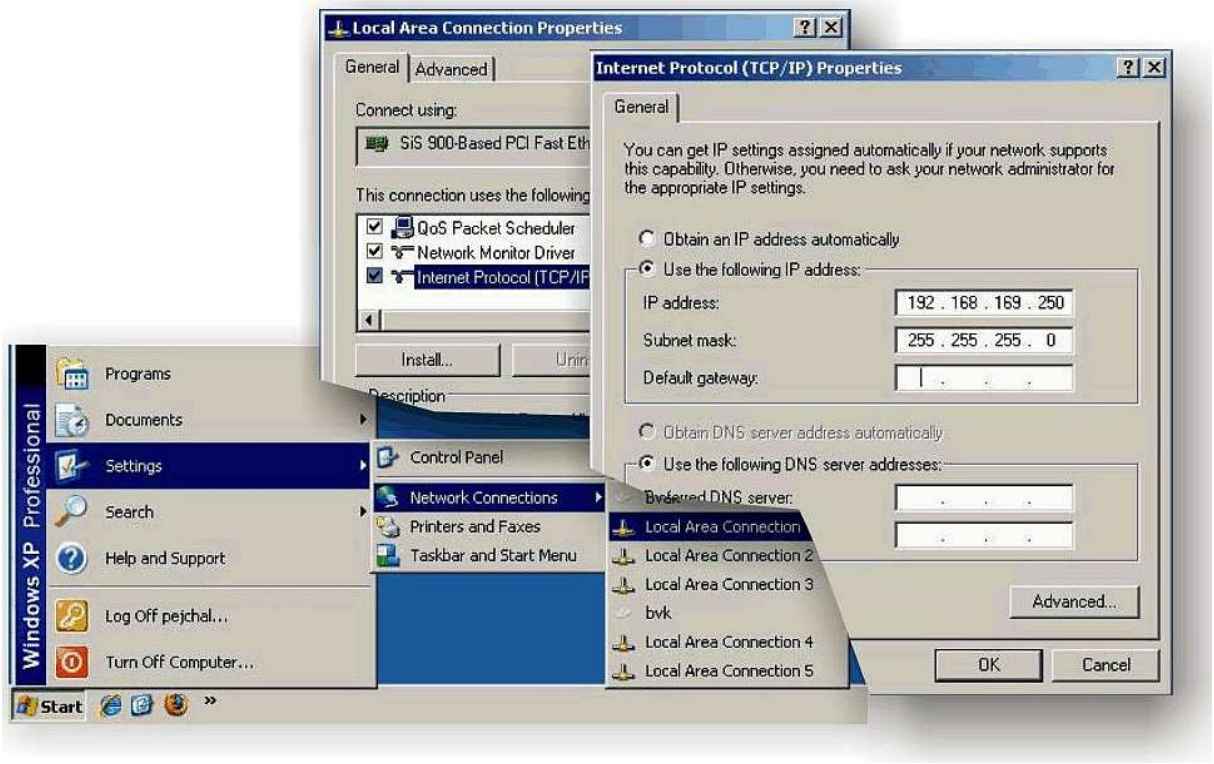


Fig. 5.3: PC address setting

Note: When you change the RipEX ETH address from the default value later on and the new IP network does not include the default one, you will have to change your PC's static IP again to be able to continue configuring the RipEX.

3. **Login to RipEX**

Start a web browser (Mozilla Firefox, Internet Explorer - JavaScript enabled) on your PC and type the RipEX's default IP in the address line default IP of RipEXfield:

- **10.9.8.7** – when connected via "X5" - external ETH/USB adapter to USB. IP address 10.9.8.7 is fixed and cannot be changed; it is independent of the IP address of the RipEX's ethernet interface.)
- **192.168.169.169** – when connected directly to ETH

Note

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

The login screen appears:

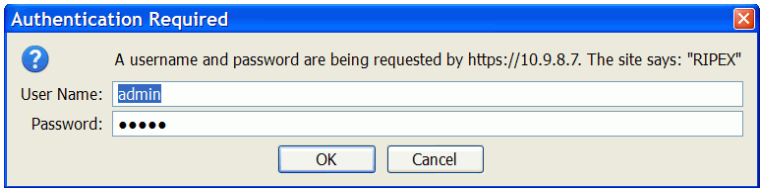


Fig. 5.4: Authentication

The default entries for a new RipEX are:

User name: admin
Password: admin
Click OK.

Initial screen should appear then:

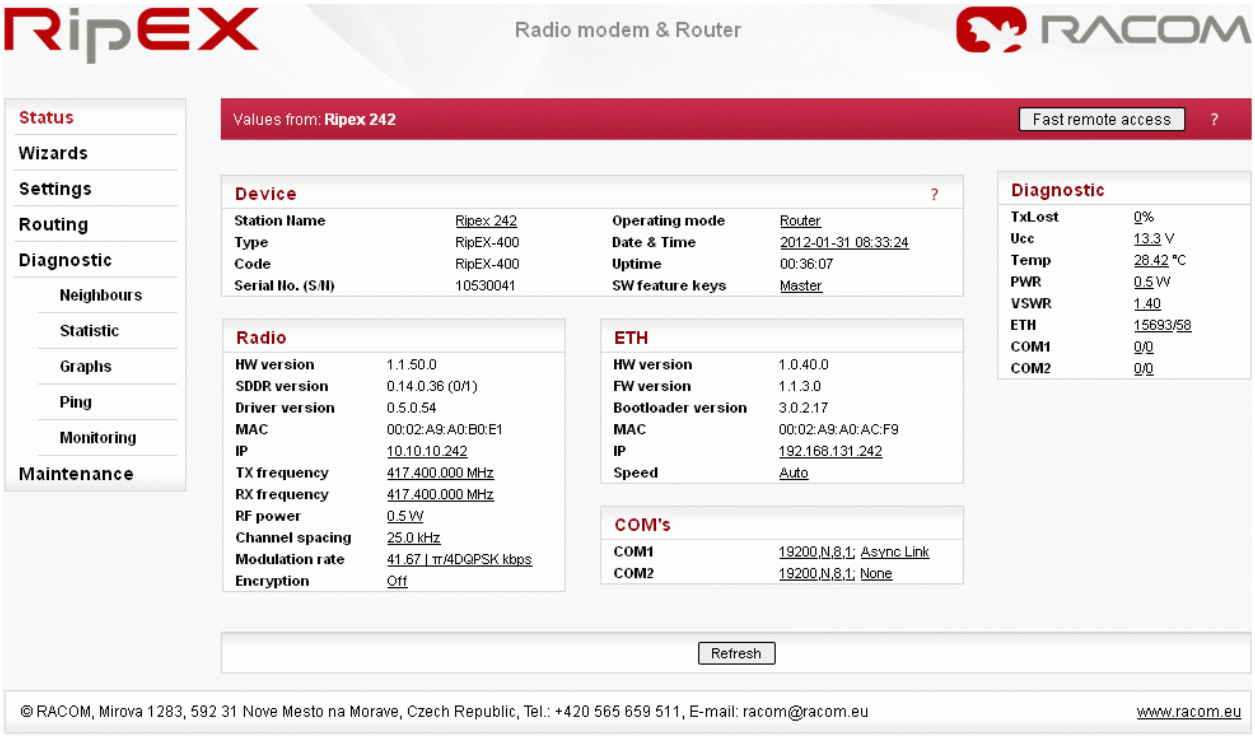


Fig. 5.5: Status Menu

Warning: Before you start any configuration, make sure only one unit is powered ON. Otherwise, a different radio modem could reply to your requests! (All units share the same IP address and are in Bridge mode when in factory settings.)

4. **IP address unknown**

If you don't have the adapter or you have forgotten the password, you can reset the access parameters to defaults, see Section 4.2.6, "Reset button".

5.4. Basic setup

For the first functionality test we recommend that you use the setup wizard. The wizard will guide you through basic functionality setup. Simply select Wizard in the web interface and proceed according to the information on the screen. Repeat for all RipEX's in the test network.

If you want to test applications which require a more complex setup, see Chapter 7, *Advanced Configuration*. To setup the IP addresses you can use the examples in Section 2.3.3, "Configuration examples" as your models, or the RipEX-App. notes, Address planing[1].

5.5. Functional test

To test radio communication between the RipEX's you can use the Ping test, under Diagnostic/Ping menu. Setting up and the output of this test are described in chapter *Adv. Conf., Tools*.

If the radio communication between RipEX's is functional, you can proceed with a test of communication between the connected devices.

You can monitor the status of configuration using the diodes on the LED panel, see Section 4.3, "Indication LEDs".

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

6. Installation

Step-by-step checklist

1. Mount RipEX into cabinet (Section 6.1, “Mounting”).
2. Install antenna (Section 6.2, “Antenna mounting”).
3. Install feed line (Section 6.3, “Antenna feed line”).
4. Ensure proper grounding (Section 6.4, “Grounding”).
5. Run cables and plug-in all connectors except from the SCADA equipment (Section 4.2, “Connectors”).
6. Apply power supply to RipEX
7. Connect configuration PC (Section 5.3, “Connecting RipEX to a programming PC”).
8. Configure RipEX (Chapter 7, *Advanced Configuration*).
9. Test radio link quality (Section 5.5, “Functional test”).
10. Check routing by the ping tool (the section called “Ping”) to verify accessibility of all IP addresses with which the unit will communicate.
11. Connect the SCADA equipment.
12. Test your application.

6.1. Mounting

6.1.1. DIN rail mounting

Radio modem RipEX is directly mounted using clips to the DIN rail. The mounting can be done lengthwise (recommended) or widthwise, in both cases with the RipEX lying flat. The choice is made by mounting the clips, one M4 screw per each. RipEX is delivered with two clips, two screws and four threaded holes.

Fig. 6.1: Flat lengthwise mounting to DIN rail – recommended

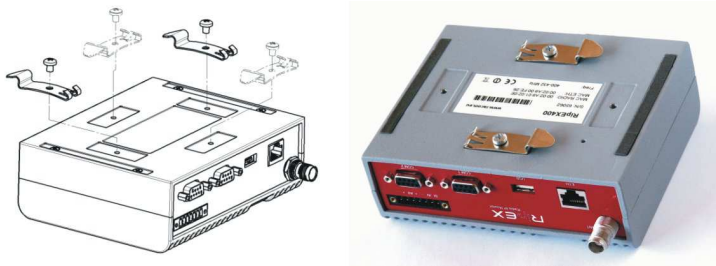


Fig. 6.2: Flat widthwise mounting to DIN rail

For vertical mounting to DIN rail, L-bracket (optional accessory) is used.

Fig. 6.3: Vertical widthwise mounting to DIN rail

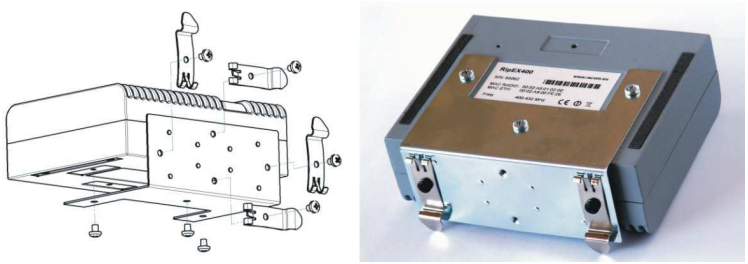


Fig. 6.4: Vertical lengthwise mounting to DIN rail

6.1.2. Flat mounting

For flat mounting directly to the support you must use the Flat bracket (an optional accessory).

Fig. 6.5: Flat mounting using Flat bracket

6.1.3. 19" rack mounting

For installation into the 19" rack you can use the 19" rack shelf – single or 19" rack shelf- double for one or two RipEXes. 19" rack shelf is an optional accessory delivered with/without a power supply.

Fig. 6.6: Rack shelf

6.1.4. Fan kit

In extreme temperatures you can install an external fan kit for additional cooling. The fan kit installs using three screws driven into the openings on the bottom side of the RipEX. Use M4×8 screws.

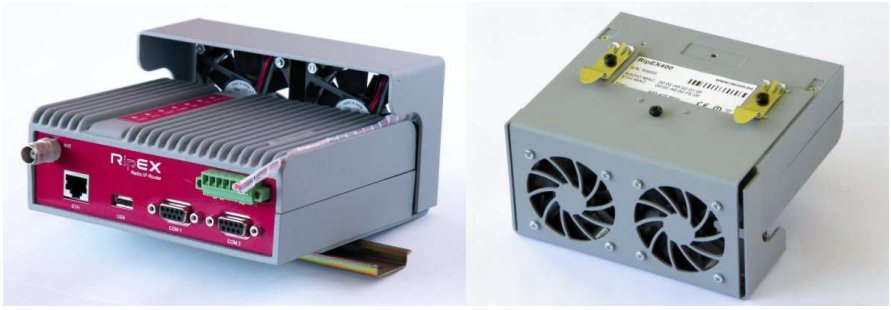


Fig. 6.7: Fan kit mounting

The fan kit may be controlled using the Alarm Output (Control and Power connector, Section 4.2.2, “Power and Control”), which is triggered when the temperature inside RipEX exceeds a set temperature (recommended) or it can run permanently (it should be connected in parallel to the RipEX’s power supply). Configuration of the Alarm Output is described in chapter *Advanced Configuration, Device*.

Dimensions are given in the Product chapter.

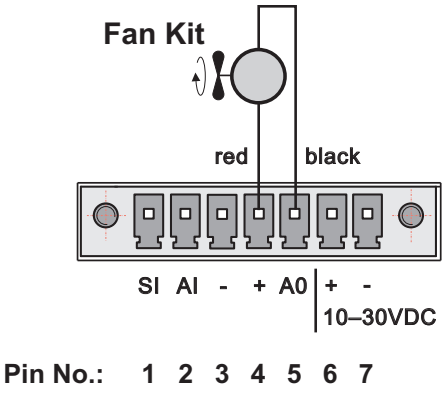


Fig. 6.8: Fan kit using Alarm Output, recommended

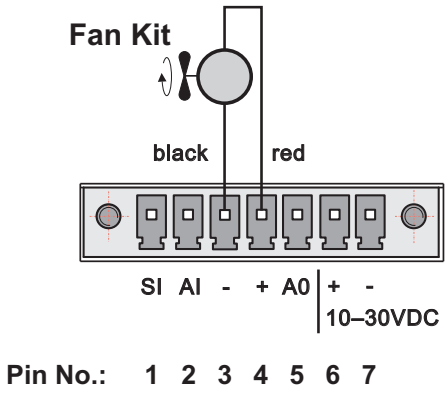


Fig. 6.9: Fan kit, always on

6.2. Antenna mounting

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 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 RipEX, including all power supplies.

Additional safety recommendations

Only qualified personnel with authorisation 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.

6.3. 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, see Chapter 3, *Network planning*. Use 50 Ω impedance cables only.

The shorter the feed line, the better. RipEX can be installed right next to the antenna and an ethernet cable can be used to connect it to the rest of the installation and to power the RipEX . An ethernet cable can also be used for other protocols utilising the serial port, see *Advanced Configuration, Terminal server*. 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.

6.4. Grounding

To minimise 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 RipEX 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.

6.5. Connectors

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

You will find the connectors' pin-outs in chapter Section 4.2, "Connectors".

6.6. Power supply

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

RipEX 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. Maximal supply cable length is 3 m.

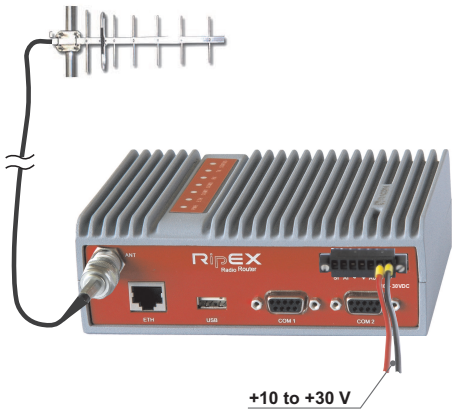


Fig. 6.10: 10–30 VDC Supplying

7. Advanced Configuration

This chapter is identical with the content of **Helps** for individual menu.

7.1. Menu header

7.1.1. Generally

RipEX can be easily managed from your computer using any web browser (Mozilla Firefox, Microsoft Internet Explorer, etc.). If there is an IP connection between the computer and the respective RipEX, you can simply enter the IP address of any RipEX in the network directly in the browser address line and log in. However it is not recommended to manage an over-the-air connected RipEX 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 RipEX, log-in to a RipEX, which your computer is connected to using either a cable (via LAN) or a high speed WAN (e.g. Internet). The RipEX which you are logged-in to in this way is called Local. Then you can manage any remote RipEX 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 RipEX and only information specific to the remote unit is transferred over the Radio channel. RipEX connected in this 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 remote management. IP routing between source (IP of ETH interface in Local RipEX) and destination IP (either Radio or ETH interface in Remote RipEX) has to exist.

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

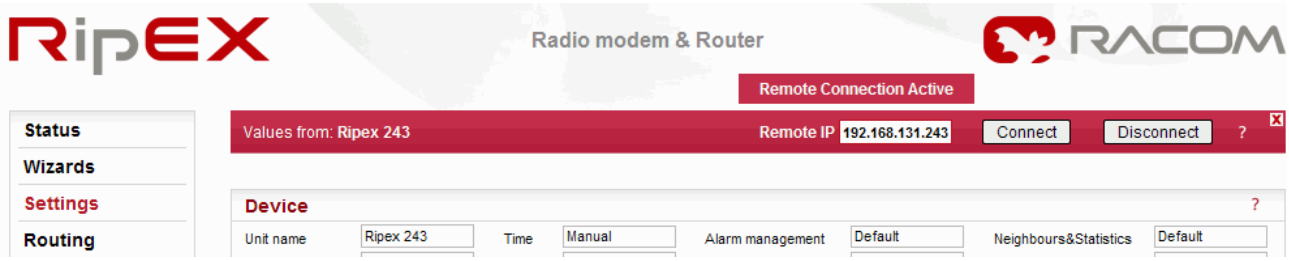


Fig. 7.1: Menu Header

Values from

The Unit name (Settings/Device/Unit name) of the RipEX from which data is currently displayed and which is currently managed.

Remote

IP address of the remotely connected RipEX. After filling-in the Connect button shall be pressed.

Connect

Action button to connect to the remote RipEX, which is specified by the IP address in the Remote box. The Unit name in "Values from" box is changed accordingly afterwards.

Disconnect

When a Remote RipEX is sucessfully connected, the Disconnect button shows up. When the Disconnect process is executed, the Local RipEX (IP address in the Local box) can be managed and the Unit name in the "Values from" box changes accordingly.

7.2. Status

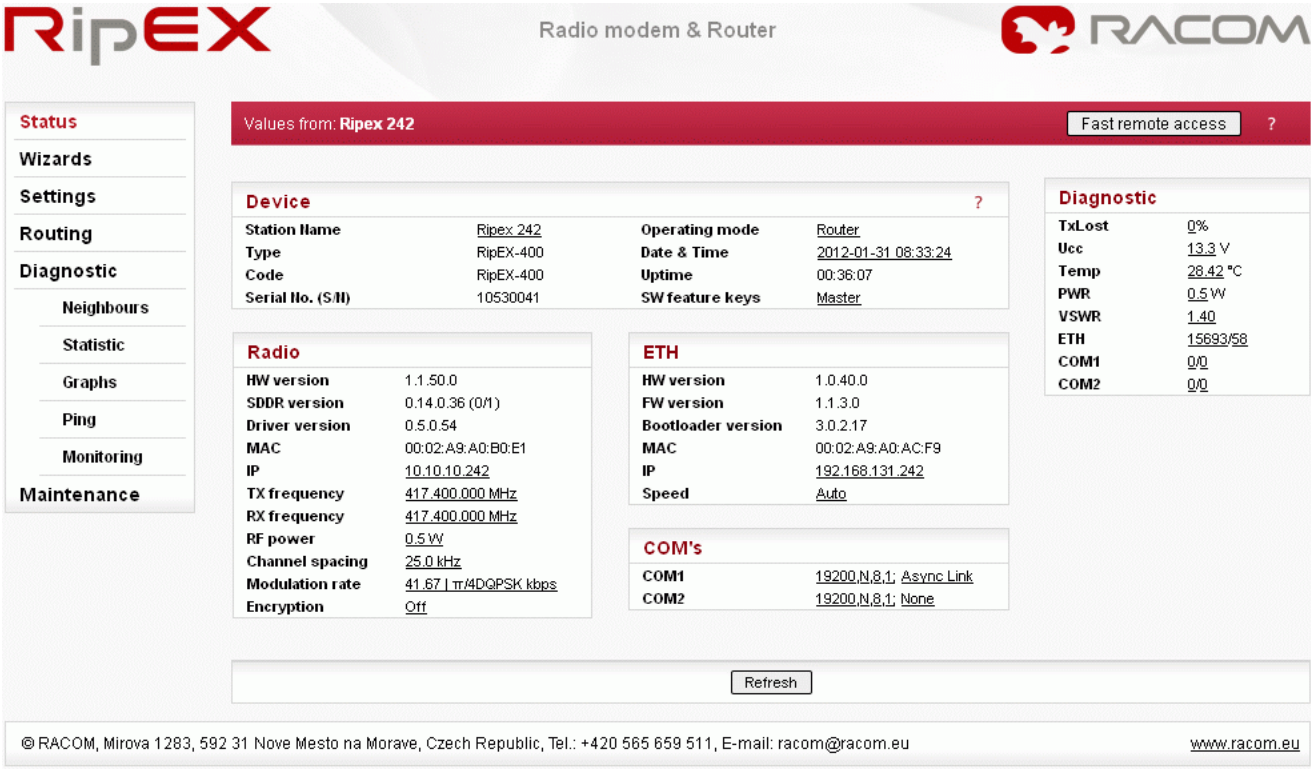


Fig. 7.2: Menu Status

7.2.1. Device, Radio, ETH&COM's

This part of Status page displays basic information about the RipEX (e.g. Serial No., MAC addreses, HW versions etc.) and overview of its most important settings. Configurable items are underlined and one click can take you to the respective Settings menu.

7.2.2. Diagnostic

The current state of Watched values is displayed in the Diagnostic part of the Status page. Watched values are values of parameters, which are continuously monitored by RipEX itself.

On-line help for each individual item is provided by balloon tips (when cursor is placed over an item name). When an item goes red, it means that the item is monitored for alarm and its value is in the alarm range (see Settings/Device/Alarm management)

Refresh - complete refresh of displayed values is performed.

7.3. Settings

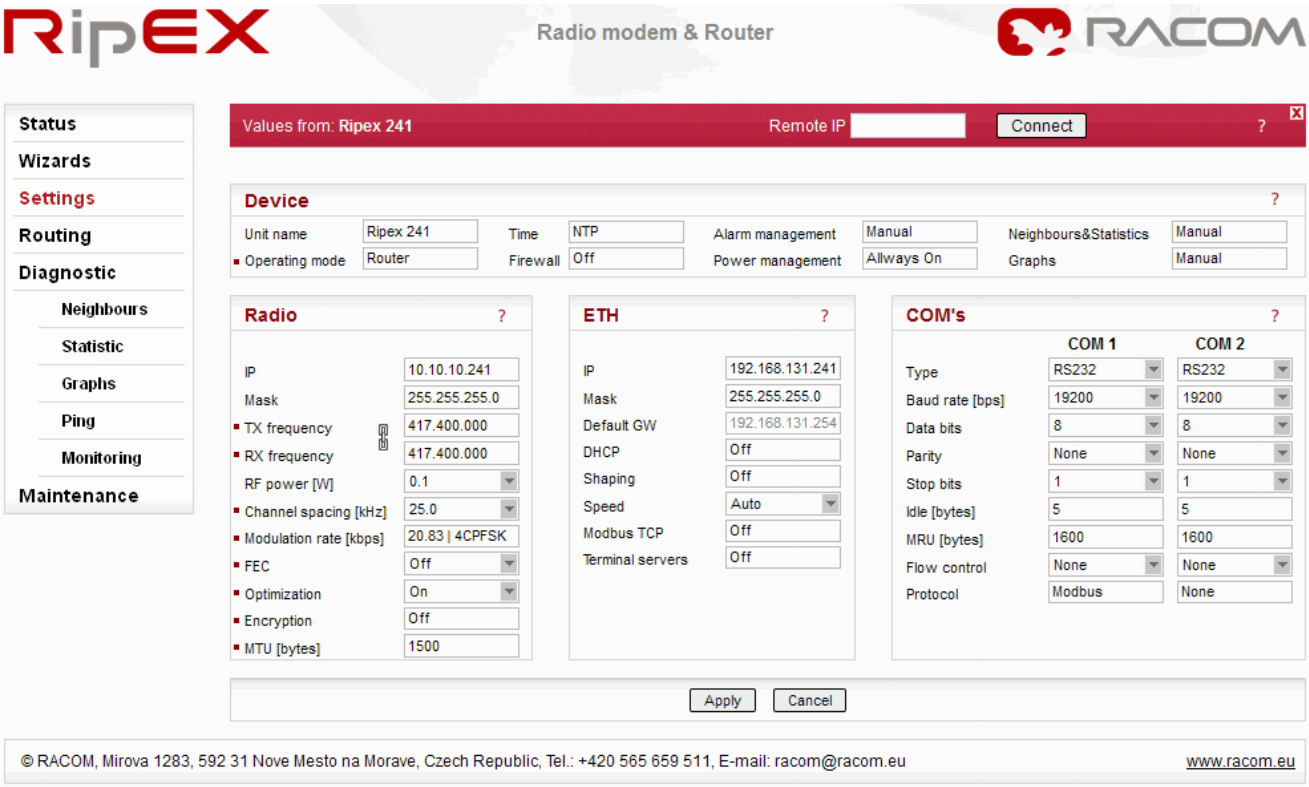


Fig. 7.3: Menu Settings

7.3.1. Device

Unit name

Default = NoName
Each Unit may have its unique name - string up to 16 characters.

Note: The Unit name is just for your convenience, there no DNS (Domain Name Server) is used in RipEX network.

Operating Mode

List box: Bridge, Router
Default = Bridge

Bridge

Bridge mode is suitable for Point-to-Multipoint networks, where Master-Slave application with polling-type communication protocol is used. RipEX in Bridge mode is as easy to use as a simple transparent device, while allowing for a reasonable level of communication reliability and spectrum efficiency in small to medium size networks.po

In Bridge mode, the protocol on Radio channel does not have the collision avoidance capability. There is CRC check of data integrity, i.e. once a message is delivered, it is 100% error free.

All the messages received from user interfaces (ETH&COM's) are immediately transmitted to Radio channel, without any checking or processing.

ETH: The whole network of RipEX units behaves like a standard Ethernet network bridge, so the Ethernet interface IP address itself is not significant. Each ETH interface automatically learns which devices (MAC addresses) lie in the local LAN and which devices are accessible via the Radio channel. Consequently only the Ethernet frames addressed to remote devices are physically transmitted on the Radio channel. This arrangement saves the precious RF spectrum from extra load which would otherwise be generated by local traffic in the LAN (the LAN to which the respective ETH interface is connected).

COM1,COM2: all frames received from COM1(2) are broadcast over Radio channel and transmitted to all COM's (COM1 as well as COM2) on all units within the network, the other COM on the source RipEX excluding.

- **Frame closing (COM1,2)**
  List box: Idle, Stream
  Default = Idle
- **Idle**
  Received frames on COM1 (COM2) are closed when gap between bytes is longer than the Idle value set in COM1,2 settings and transmitted to Radio channel afterwards.
  - **Repeater**
    List box: Off, On.
    Default = Off
    Each RipEX may work simultaneously as a Repeater (Relay) in addition to the standard Bridge operation mode..
    If "**On**", every frame received from the Radio channel is transmitted to the respective user interface (ETH,COM1,2) 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.
  - **Number of repeaters** [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 RipEX) is blocked for a period calculated to prevent collision with a frame transmitted by a Repeater. Furthemore, 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 [ms]** [0-5000]
    Default = 0
    It delays forwarding of all frames from user interfaces (ETH&COM's) to the Radio channel for the set time. The set value should be equal to the transmitting time of the longest message.

    This should be used when e.g. all sub-stations (RTU's) reply to a broadcast query from the master station. In such a case a massive collisions would take place, because all sub-stations (RTU's) would reply more or less in the same instant. In order to prevent such a collision, TX

delay should be set individually in each slave RipEX. The length of responding frame, the length of Radio protocol overhead, Modulation rate have to be taken into account.

- **Stream**

  In this mode, the incoming bytes from a COM are immediately broadcast over the Radio channel. COM port driver does not wait for the end of a frame. When the first byte is coming from a COM, the transmission in the Radio channel starts with the necessary frame header. If the next byte arrives before the end of transmission of the previous one, it is glued to it and the transmission on the Radio channel continues. If there is a gap between incoming bytes, the byte after the gap is treated as the first byte and the process starts again from the beginning. Padding is never transmitted between blocks of bytes.

  The receiving RipEX transmits incoming bytes (block of bytes) from the Radio channel to both COM ports immediately as they come.

  When the ETH interface is used simultaneously (e.g. for remote configuration), it works as the standard bridge described above. ETH frames have higher priority, i.e. the stream from COM is interrupted by a frame from Ethernet.

  Stream mode is recommended to be used for time-critical application only, when the first byte has to be delivered as soon as possible. However there is not any data integrity control. If the Baud rate of COM is significantly lower than the Modulation rate on the Radio channel, frames are transmitted byte by byte. If it is higher, blocks of bytes are transmitted as frames over the Radio channel.

  Note: Stream mode can not be used when there is a Repeater in the network.

Router

Router mode is suitable for Multipoint networks, where Multi-master applications with any combination of polling and/or spontaneous data protocols can be used. The proprietary link-layer protocol on the Radio channel is very sophisticated, it can transmit both unicast and broadcast frames, it has collision avoidance capability, it uses frame acknowledgement and retransmissions and a CRC check to guarantee data delivery and integrity even under harsh interference conditions on the Radio channel.

RipEX works as a standard IP router with 2 independent interfaces: Radio and ETH. Each interface has got its own MAC address, IP address and Mask.

IP packets are processed according the Routing table. There is also possibility to set a router Default gateway (apply to both interfaces) in the Routing table.

The COM ports are treated in the standard way as router devices, messages can be delivered to them as UDP datagrams to selected port numbers. Destination IP address of COM port is either the IP of ETH or the IP of Radio interfaces. The source IP address of outgoing packets from COM ports is always the IP of ETH interface.

- **ACK**
  List box: Off, On.
  Default = On
  - **On**
    Each frame transmitted on Radio channel from this RipEX has to be acknowledged by the receiving RipEX, using the very short service packet (ACK), in order to indicate that it has received the packet successfully. If ACK is not received, RipEX will retransmit the packet according its setting of Retries.

Note: The acknowledgement/retransmission scheme is an embedded part of the Radio protocol and works independently of any retries at higher protocol levels (e.g. TCP or user application protocol)

- **Off**
  There is no requirement to receive ACK from the receiving RipEX. i.e. the packet is transmitted only once and it is not repeated.

- **Retries [No]** [0-15]
  Default = 3
  When an acknowledge from the receiving RipEX is not received, the frame is retransmitted. The number of possible retries is specified.
- **RSS threshold [-dBm]** [50-150]
  Default = 120
  RSS (Received Signal Strength) limit for access to Radio channel. RipEX does not start transmitting when a frame is being received and the RSS is better than the set limit or when the destination MAC address of the frame is its own.
- **Repeat COM Broadcast**
  List box: On, Off
  Default = Off
  If On, a broadcast originated on COM port (Protocol/Broadcast = On) in any remote unit and received by this unit on Radio channel is repeated to Radio channel.

Time

List box: Manual, NTP
Default = Manual
Internal calendar time of RipEX can be set manually or synchronized via NTP (Network Time Protocol).

- **Manual**

  RipEX internally uses the Unix epoch time (or Unix time or POSIX time) - the number of seconds that have elapsed since January 1, 1970. When RipEX calendar time is set, the Unix epoch time is calculated based on filled in values (Date, Time) and the time zone, which is set in operating system (computer), where the browser runs.
  - **Current Date&Time**
    Information about the actual date and time in the RipEX
  - **Date [YYYY-MM-DD]**
    Fill in Local Date in required format
  - **Time [HH:MM:SS]**
    Fill in Local Time in required format
  - **RipEX Time zone**
    Select RIPEX Time zone from list box.
    Default = (GMT +1:00) Central Europe
    This time zone is used for conversion of internal Unix epoch time to "human readable date&time" in RipEX logs.
  - **Daylight saving**
    List box: On, Off
    Default = On
    If **On**, Daylight saving is activated according the respective rules for selected RipEX Time zone.
- **NTP**

  Internal calendar time in RipEX is synchronized via NTP and RipEX becomes a standard NTP server simultaneously.
  - **Current Date&Time**

Information about the actual date and time in the RipEX

- **Time source**
  List box: NTP server, Internal GPS
  Default = NTP server
  - **NTP server** – The source of time is a standard NTP server. This server has to be connected via the Ethernet interface.
  - **Internal GPS** – The source of time is the internal GPS. In this case only RipEX Time zone and Daylight saving parameters below are active.
- **Source IP**
  Default = empty
  IP address of the NTP server, which provides Time source. Date and Time will be requested by RipEX from there. More NTP servers can be configured, the more servers, the better time accuracy. If the Time source is a RipEX over Radio channel, only one source server is recommended, since the Radio channel could be overloaded.
- **Minimum polling interval**
  List box: 1min to 2h 17min
  RipEX polls the source server in order to synchronize itself in the set period or later.
- **RipEX Time zone**
  Select RipEX Time zone from list box.
  Default = (GMT +1:00) Central Europe
  This time zone is used for conversion of internal Unix epoch time to "human readable date&time" in RipEX logs..
- **Daylight saving**
  List box: On, Off
  Default = On
  If **On**, Daylight saving is activated according the respective rules for selected RipEX Time zone.

- **RipEX NTP server**

  Information about the status of internal NTP server in the RipEX
  - **State**
    - not synced - not synchronized
    - synced to GPS - synchronized to internal GPS
    - synced to NTP - synchronized to NTP server
  - **Stratum**
    1 to 16 (1=the best, 16=the worst, 8=when internal time in RipEX is set manually)
    The stratum represents the quality and accuracy of time, which the NTP server provides.
  - **Delay [ms]** This is the delay of packet (1/2 round trip time), which RipEX received from the NTP server while asked for synchronization. This delay is compensated in the RipEX NTP server.
  - **Jitter [ms]**
    The Jitter of received times when RipEX asked for time synchronization from NTP server(s).

Firewall

List box: Off, On
Default = Off

There is a standard Linux firewall implemente.

- **Port** – interval of ports can be filled in. E.g. 2000-2120.
- **Connection state** – state-firewall active only for TCP protocol.
- **New** – relates to the first packet when a TCP connection starts (Request from TCP client to TCP server for opening of a new TCP connection). Used e.g. for allowing to open TCP only from the RipEX network to the outside.

- **Established** – relates to already existing TCP connection. Used e.g. for allowing to get replies for TCP connections created from RipEX network to the outside.
- **Related** – a connection related to the “Established” one. E.g. FTP typically uses 2 TCP connections – control and data – where the data connection is created automatically using dynamic ports.

Note: Port 44 is used for the service access. Be careful when making rules which may affect datagrams to/from this port in Firewall settings. You may lose the connection between your PC and RipEX. When it happens, use the Reset button on the bottom side of RipEX (press it for 15 sec.) in order to set Default access, which restores the default IP, default password and clears the Firewall.

Alarm management

The average values of parameters listed in the table (Watched values) are continuously monitored. When any of them exceeds the respective threshold, the selected action(s) is(are) invoked.

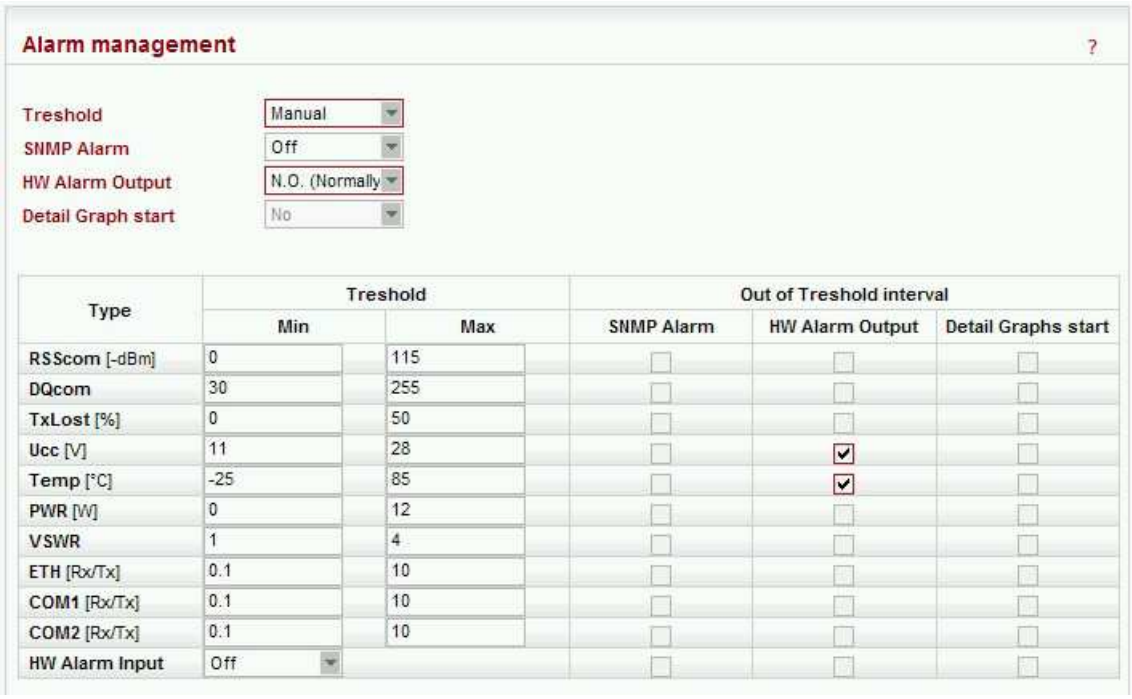


Fig. 7.4: Menu Alarm management

Note: At least 10 values have to be included in average value before it is checked for the possible alarm.

- **Threshold**
  List box: Default, Manual,
  Default = Default
  Default – Default (recommended) values are set and can not be edited.
  Manual – Thresholds can be set manually.
- **SNMP Alarm**
  List box: Off, On.
  Default = Off
  If "**On**", SNMP Alarm trap is activated. The SNMP trap message is sent both when a parameter value exceeds the alarm threshold and when it returns back into its “normal” range. Remember to set the IP destination address for SNMP trap messages.
- **HW Alarm Output**

List box: Off, N.O. (Normally Open), N.C. (Normally Closed)
Default = Off
If "**N.O.**" or "**N.C.**", the HW Alarm Output is active and its normal status (no alarm) is open or closed, respectively.

The HW Alarm Output is a pin (open n-p-n collector) on the screw terminal at the Power and Control connector on the front panel.

- **Detail Graph start**
  Just for information. It can be set in Settings/Graph/Detail Graph start, not here.
  Alarm starts Detail Graph only when this value is set to "Alarm"
- **HW Alarm Input**
  List box: Off, N.O. (Normally Open), N.C. (Normally Closed)
  Default = Off
  If "N.O." or "N.C.", the HW Alarm Input is active and its normal status (no alarm) is open or closed, respectively.

  The Alarm event is triggered when the HW Alarm Input changes its status from "Normal" to "Alarm". Note that to "Close" the HW Alarm Input means connecting the respective screw terminal at the Power and Control connector on the front panel to the Ground terminal at the same connector.

Power management

- **Power supply mode**
  List box: Always On, Save Mode, Sleep Mode
  Default = Always On
- **Always On**
  RipEX is always on, no special power saving modes are active.
- **Save Mode**
  RipEX is listening on Radio channel in the Save mode while consuming 2.3 W.

  Router mode: When the RipEX receives a packet for its IP address, it wakes up. However data from this first received packet is lost.

  Bridge mode: Any packet received on Radio channel wakes the unit up.
  - Timeout
    List box: On, Off
    Default = On
    When On, RipEX remains on for the set seconds from the moment of its wake-up.
  - Timeout from wake-up [sec.]
    Default = 300 [240 - 64 800]
    RipEX stays on for the set time from the moment of its wake-up.
  - Reset timeout on received packets
    List box: On, Off
    Default = Off
    If On, the Timeout from wake-up is reset with each packet received
- **Sleep Mode**
  Sleep Mode is controlled via the digital input on Power and Control connector. When the respective pin is grounded, RipEX goes to sleep and consumes only 0.1 W at 13.8 V (see Section 4.4, “Technical specification”). The time needed for complete wake-up is approx. 25 seconds (booting time).
  - **Timeout from sleep request [sec.]**
    Default = 300 [0 - 64 800]
    RipEX remains on for the set time from the moment when the sleep input pin has been grounded.

Neighbours&Statistics

- **Parameters**

  List box: Default, Manual,
  Default = Default
  Default – Default (recommended) values are set and can not be edited.
  Manual – Values can be set manually.
  There are 2 tables with diagnostic information in the main menu - Diagnostic/Neighbours, Diagnostic/Statistic. The Neighbours table displays Watched values from RipEX and from all its neighbours. (Neighbour = RipEX, which can be accessed directly over the radio channel, i.e. without a repeater). There is statistic information about the traffic volume in the Statistic table.
  - **Watched values broadcasting period [min]**
    Default = 10 min, [0 = Off]
    RipEX periodically broadcasts its Watched values to neighbouring units. The Watched values can be displayed in Graphs and Neighbours menu.
    Note: When Bridge mode is used, watched values broadcasting creates collisions for user traffic. Be careful in using this feature.
  - **Neighbours&Statistic log save period [min]**
    Default = 1440 min (1 day) [10 - 7200 min]
    This is the period, in which Neighbours and Statistics logs are saved in the archive and cleared and new logs start from the beginning.
    Note: The history files are organized in a ring buffer. Whenever a new file is opened, the numbers of files are shifted, i.e. 0->1, 1->2, etc. There is a history of 20 log files available

Graphs

- **Parameters**
  List box: Default, Manual,
  Default = Default
  Default – Default (recommended) values are set and can't be edited.
  Manual – Values can be set manually.
  Graphs displays history of Watched values and history of some of the items from the Statistic table. Displayed values are stored in each RipEX including data from selected five neighbouring units. Neighbour = RipEX, which can be accessed directly over the Radio channel (not over Ethernet), i.e. without a repeater. The graph data is stored in files, each file contains 60 samples of all values. The sampling period can be configured. There are two types of graphs- Overview and Detail. Overview graphs cover a continuous time interval back from the present, they use relatively long sampling period. Detail graph is supposed to be used in case of a special event, e.g. an alarm, and the sampling period is much shorter.
  - **Logged Neighbour IP's**
    Default = 0.0.0.0
    Up to 5 IP addresses of neighbouring units can be set. (Neighbour = RipEX, which can be accessed directly over the radio channel, i.e. without a repeater). Watched values from these units are stored in the graph files and can be displayed afterwards.
  - **Overview graph sampling period**
    List box: 1, 2, 4, 12 hours
    Default = 12 hours
    The 60 samples per graph file result in (depending on the sampling period) 60, 120, 240 or 720 hours in each file. There are 6 files available, so total history of saved values is 15, 30, 60 or 180 days. The Overwiev graph files are organized in a ring buffer. Whenever a new file is opened, the oldest one is replaced.
  - **Detail Graph sampling period**

List box: 1, 5, 10, 20 mins
Default = 1 min
The 60 samples per graph file result in 60, 300, 600, 1200 minutes in each file. There are 20 files available. They are organized in a ring buffer. When a new file is opened, the one with oldest data is replaced. The Detail graph files may not cover a continuous segment of history. See Detail graph start for details.

- **Detail Graph start**
  List box: No, Alarm, Single, Continual
  Default = No
  Detail graph data sampling is started based on selected event from list box:
  No – Detail graph does not start.
  Alarm – if a tickbox in Detail graph column (Settings/Alarm management) is checked, then the Detail graph file is stored in case of that alarm. Twenty samples prior the alarm event and 40 samples after the alarm event are recorded. When another alarm occurs while a Detail graph file is opened, the sampling continues normally and no other file is opened.
  Single – a single Detail graph file is manually started immediatelly after the Apply button is clicked.
  Continual – Detail graph files are periodically saved in the same way as Overview graph files are.

7.3.2. Radio

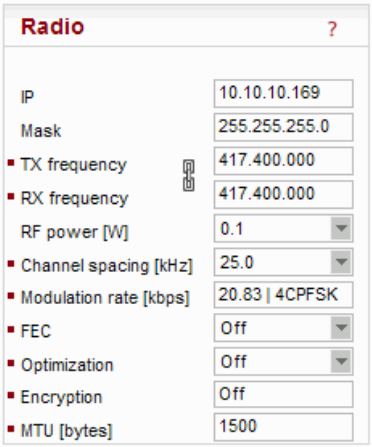


Fig. 7.5: Menu Radio

* Active only when in Router mode
** These items have to be set in accordance with the license issued by the respective radio regulatory authority

IP*

Default = 10.10.10.169
IP address of Radio interface

Mask*

Default = 255.255.255.0
Network Mask of Radio interface

TX frequency**

Transmitting frequency. Format MHz.kHz.Hz. Step 5 or 6.25 kHz.
The value entered must be within the frequency tuning range of the product as follows:
RIPEX-330: 330–350 MHz
RIPEX-368: 368–400 MHz
RIPEX-400: 400–432 MHz
RIPEX-432: 432–470 MHz

RX frequency**

Receiving frequency, the same format and rules apply.
Note: By default, the TX and RX frequencies are locked together and change in one field is mirrored in the other. If clicked, the lock is removed and different TX and RX frequencies can be entered.

RF power [W]**

List box: possible values
Default = 5 W
The range of values in the list box is limited to 2 W for high Modulation rates. 10 W is available only for lower Modulation rates and only when the respective SW feature key is active.

Channel spacing [kHz]**

List box: possible values
Default = 25 kHz

The wider the channel the higher the posible Modulation rate.

Modulation rate [kbps]

- **Approval**
  List box: possible values
  - **CE**
    Radio parameters meet ETSI EN 300 113-2 and ETSI EN 302 561
  - **FCC**
    Radio parameters meet FCC part 90 CPFSK modulations have use approx. 20% higher frequency deviation compared to CE, so the receiver sensitivity is approx. 1-2 dB better.
- **Modulation rate [kbps]**
  List box: possible values
  Default = 16DEQAM

  Possible values in list box are dependent on the Approval set. The two highest rates are available only when the respective SW feature key is active.
  Higher Modulation rate provides higher data speed but they also result in lower receiver sensitivity, i.e. lower coverage range. The reliability of communication over a radio channel is always higher when using lower Modulation rate.

FEC

List box: possible values
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 (to some extent). The improvement comes at the expense of the user data rate. The lower the FEC ratio, the better the capability of error correction and the lower the user data rate. The User data rate = Modulation rate x FEC ratio.

Optimization*

List box: On, Off
Default = Off

Optimization is applicable in Router mode for packets directed to Radio channel. It watches packets on individual radio links and optimizes both the traffic to the counterpart of a link and the sharing of the Radio channel capacity among the links.
On an individual link the optimizer supervises the traffic and it tries to join short packets when opportunity comes. However in case of heavy load on one link (e.g. FTP download) it splits the continuous stream of packets and creates a window for the other links. To minimize the actual load, Zlib compression (with LZ77 decimation and Huffman coding) and other sophisticated methods are used.
In addition a special TCP optimiser is used for TCP/IP connections. It supervises every TCP session and eliminates redundant packets. It also compresses TCP headers in a very efficient way. The overall effect of the Optimization depends on many factors (data content, packet lengths, network layout etc.), the total increase of network throughput can be anything from 0 to 200%, or even more in special cases.
Note: Apart from this Optimization, there is an independent compression on the Radio channel, which works in both Operating modes, Bridge and Router. This compression is always On.

Encryption

AES 256 (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.
List box: Off, AES 256
Default = Off

When AES 256

Key mode
List box: Pass Phrase, Manual
Default = Pass Phrase

- **Pass phrase**
  It is not necessary to fill in 32 Bytes of hexa chars in order to set the encryption key. The key can be automatically generated based on a Pass phrase. Fill in your Pass phrase (any printable ASCII character, min. 1 char., max. 128 char.). The same Pass phrase must be set in all units within the network
- **Manual**
  The key can be configured manually (fill in 32 Bytes of 64 hexa chars) or it can be randomly generated using Generate button. The same key must be in all units within the network, i.e. it has to be generated only in one unit and copied to the others.

MTU [bytes]*

Default = 1500 Bytes [70 - 1500] (max. packet size)

When a packet to be transmitted from the Radio interface is longer than the MTU (Maximum Transmission Unit) set, the RipEX router performs standard IP fragmentation. A packet longer than the configured size is split into the needed number of fragments, which are then independently transmitted - the first packet(s) is (are) transmitted fragment-size long, the last packet contains the remaining bytes. The reassembly of the fragments into the original packet normally takes place in the unit at the end of the path.
Reducing the maximum length of a frame on a Radio link may improve its performance under unfavourable conditions (interference, multi-path propagation effects). However the recommended place to determine the packet size is the actual user interface, e.g. a COM port. Note that the IP fragmenting is possible in the Router mode only.

7.3.3. ETH

* Active only when Router mode

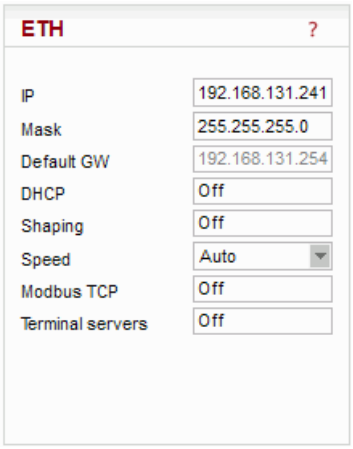


Fig. 7.6: Menu Ethernet

IP

Default = 192.168.169.169
IP address of ETH interface

Mask

Default = 255.255.255.0
Mask of ETH interface

Default GW

Default = 0.0.0.0
The default gateway (applies to whole RipEX). It can be set only in the Routing menu while Router mode.

DHCP*

List box: Off, Server
Default = Off

Server

DHCP (Dynamic Host Configuration Protocol) Server in RipEX sets network configuration (IP address, Mask, Gateway) in connected DHCP clients. They have to be connected to the same LAN as the ETH interface of RipEX. The Mask set is the same as on RipEX ETH, the Gateway is the IP address of ETH interface of RipEX. Typical DHCP client is e.g. a PC used for configuration of RipEX.
Important! Never activate the DHCP Server when ETH interface of RipEX is connected to LAN, where another DHCP server is operating.

- **Start IP**
  Default = IP address of ETH interface + 1
  DHCP Server assigns addresses to connected clients starting from this address.
- **End IP**
  DHCP server assigns IP addresses to clients from the range defined by Start IP and End IP (inclusive).
- **No of leases**
  Default = 5 [1 - 255]
  Maximum number of DHCP client(s) which can RipEX simultaneously serve. It can not be more than the number of addresses available in the Start IP - End IP range.
- **Lease timeout [DD:HH:MM:SS]**
  Default = 1 day (max. 10 days)
  A DHCP Client has to ask DHCP Server for refresh of the received configuration within this timeout, otherwise the Lease expires and the same settings can be assigned to another device (MAC).
- **Assigned IP's**
  Table shows MAC addresses of Clients and IP addresses assigned to them by the Server. Expiration is the remaining time till the respective Lease expires. If the assigned IP addresses are required to be deleted, set DHCP Server to Off, then action Apply and set DHCP server to On (+Apply) again.
- **Preferred IP's**
  It is possible to define which IP should be assigned by the Server to a specific MAC. The requested IP has to be within the Start IP – End IP range.

Shaping*

List box: On, Off
Default = Off
Ethernet interface could easily overload the Radio channel. Because of that, it is possible to shape traffic received from the ETH interface.
If On, specified volume of Data [Bytes] in specified Period [sec] is allowed to enter the RipEX from ETH interface. The first packet which exceeds the limit is stored in the buffer and transmitted when new Period starts. Further over-limit packets are discarded.

Speed

List box: Auto, 100baseTX/Full, 100baseTX/Half, 10baseT/Full, 10baseT/Half
Default = Auto
Communication speed on the Ethernet interface.

Modbus TCP*

Use this setttings only for **Modbus TCP Master** when it communicates with both types of Modbus slaves using either Modbus RTU or Modbus TCP protocols. Or when TCP/IP communication should

run locally between Modbus Master and RipEX in Modbus TCP network. Read Help and Application note Modbus in RipEX.

For more information refer to the manual Application note / Modbus TCP[1].

** - denotes items to be used only when either all or some RTUs (Remote Telemetry Unit) on remote sites are connected via RS232 or RS485 interface to RipEX, using the Modus RTU protocol. Then automatic conversion between Modbus TCP and Modbus RTU protocols takes place for such units.

List box: On, Off
Default = Off

- **My TCP port**
  Default = 502 [1 - 65 535]
  TCP port used for Modbus TCP in RipEX.
- **TCP Keepalive [sec.]**
  Default = 120 [0 - 16 380]
  TCP socket in RipEX is kept active after the receipt of data for the set number of seconds.
- **Broadcast****
  List box: On, Off
  Default = Off
  Some Master SCADA units send broadcast messages to all Slave units. SCADA application typically uses a specific address for such messages. RipEX (Protocol utility) converts such message to an IP broadcast and broadcasts it to all RipEX units resp. to all SCADA units within the network.
  If On, the address for broadcast packets in SCADA protocol has to be defined:
- **Broadcast address format** - List box Hex, Dec - format in which broadcast address is defined.
- **Broadcast address** - address in the defined format (Hex, Dec)
- **Address translation**
  List box: Table, Mask
  Default = Mask
  In a SCADA protocol, each SCADA unit has a unique address, a "Protocol address". In RipEX Radio network, each SCADA unit is represented by an IP address (typically that of ETH interface) and a UDP port (that of the protocol daemon or the COM port server to which the SCADA device is connected via serial interface).

  A translation between "Protocol address" and the IP address & UDP port pair has to be done. It can be done either via Table or via Mask.

  Each SCADA message received from serial interface is encapsulated into a UDP/IP datagram, where destination IP address and destination UDP port are defined according the settings of Address translation.
  - **Mask**
    Translation using Mask is simpler to set, however it has some limitations:
    − all IP addresses used have to be within the same network, which is defined by this Mask
    − the same UDP port is used for all the SCADA units, which results in the following limitations:
    − SCADA devices on all sites have to be connected to the same interface (COM1 or COM2)
    − only one SCADA device to one COM port can be connected, even if the RS485 interface is used
    - **Base IP**
      Default = IP address of ETH interface

[1] http://www.racom.eu/eng/products/m/ripex/app/modbus.html

When the IP destination address of the UDP datagram, in which serial SCADA message received from COM1(2) is encapsulated, is created, this Base IP is taken as the basis and only the part defined by Mask is replaced by 'Protocol address'.

- **Mask**
  Default = 255.255.255.0
  A part of Base IP address defined by this Mask is replaced by 'Protocol address'. The SCADA protocol address is typically 1 Byte, so Mask 255.255.255.0 is most frequently used.
- **UDP port (Interface)**
  List box: COM1, COM2, TS1-TS5, TCPM1, Manual.
  Default = COM1
  This UDP port is used as the destination UDP port in the UDP datagram in which serial SCADA packet received from COM1(2) is encapsulated. Default UDP ports for COM1, COM2 or Terminal servers 1-5 (TS1-TS5) or Modbus TCP (TCPM1) can be used or UDP port can be set manually. If the destination IP address belongs to a RipEX and the UDP port is not assigned to COM1(2) or to a Terminal server or to any special daemon running in the destination RipEX, the packet is discarded.

- **Table**
  The Address translation is defined in a table. There are no limitations like when the Mask translation is used. If there are more SCADA units on RS485 interface, their “Protocol addresses” translate to the same IP address and UDP port pair. . There are 3 possibilities how to fill in aline in the table:
  − One "Protocol address" to one "IP address" (e.g.: 56 −−> 192.168.20.20)
  − Interval of "Protocol addresses" to one "IP address" (e.g.: 56-62 −−> 192.168.20.20)
  − Interval of "Protocol addresses" to interval of "IP addresses" (e.g.: 56-62 −−> 192.168.20.20-26). It is possible to write only the start IP and dash, the system will add the end address itself.
  - **Protocol address**
    This is the address which is used by SCADA protocol. It may be set either in Hexadecimal or Decimal format according to the respective List box value.
    Protocol address length can be maximum 1 Byte.
  - **IP**
    IP address to which Protocol address will be translated. This IP address is used as destination IP address in UDP datagram in which serial SCADA packet received from COM1(2) is encapsulated.
  - **UDP port (Interface)**
    This is the UDP port number which is used as destination UDP port in UDP datagram in which the serial SCADA message, received from COM1(2), is encapsulated.
  - **Note**
    You may add a note to each address up to 16 characters long for your convenience. (E.g. “Remote unit #1" etc.).
  - **Active**
    You may tick/untick each translation line in order to make it active/not active.
  - **Modify**
    Edit Delete Add buttons allow to edit or to add or to delete a line. The lines can be sorted using up and down arrows.

Terminal servers

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

Examples of the use:

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

- there is not any physical serial interface on the computer
- the serial cable between the RipEX and computer would be too long (e.g. the RipEX is installed very close to the antenna to improve radio coverage).
- the LAN between the computer and the place of RipEX installation already exists
- Modbus TCP is used with local TCP sessions on slave sites or when combination of Modbus RTU and Modbus TCP is used. For more information refer to Application note Modbus TCP/RTU[2] This applies also to other SCADA protocol TCP versions, e.g. DNP3 TCP.

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

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

- **Terminal server**
  List box: On, Off
  Default = Off

  If **On**, up to 5 independent Terminal servers can be set up. Each one can be either of TCP or UDP **Type, Keepalive** is the timeout in sec. for which the TCP socket in RipEX is kept active after the last dataa receiption or transmissiontof data, **My IP** address of a Terminal server has to be always the same as the IP address of the RipEX ETH interface, **My Port** can be set as required. **Destination IP** and **Destination port** values belong to the locally connected application (e.g. a virtual serial interface). The Aapplications in some cases dynamically change IP port with each datagram. In such a case set Destination port=0. RipEX will then send replies to the port from which the last response has been received. This feature allows tocan extend the number of simultaneously opened TCP connections between a RipEX and locally connected application up to 10. **Protocol** follows the same principles as a protocol on COM interface. You may tick/untick each individual Terminal server in order to make it **active**/not active.

7.3.4. COM's

* Active only when Router mode

The COM ports in RipEX are served by special daemons, which are connected to the IP network through a standard Linux socket. Consequently a COM port can be accessed using any of the two IP addresses (either ETH or Radio interface) used in a RipEX and the respective UDP port number. The source IP address of outgoing packets from COM ports is equal to IP address of the interface (either Radio or Ethernet) through which the packet has been sent. Outgoing interface is determined in Routing table according to the destination IP. The default UDP port numbers are COM1 = 8881, COM2 = 8882. If necessary they may be changed using CLI, nevertheless it is recommended to stick to the default values because of dependencies between different settings (e.g. Protocols) in the network.

[2] http://www.racom.eu/eng/products/m/ripex/app/modbus.html

Note: UDP port settings is valid only in Router mode. In Bridge mode all packets received by COM port are broadcasted to all COM ports on all RipEXes within the network.

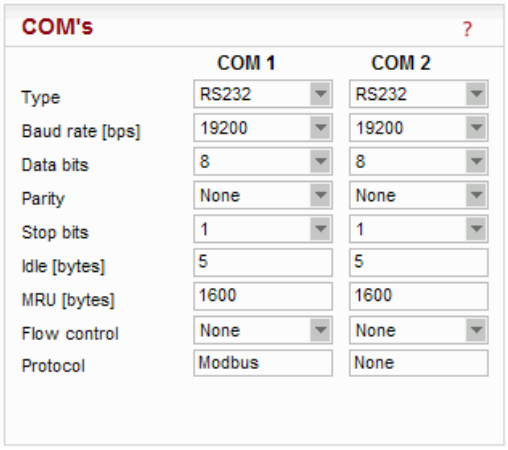


Fig. 7.7: Menu COM

Type

List box: possible values
Default = RS232
COM1 is always RS232, COM2 can be configured to either RS232 or RS485.
Note: The settings of Data rate, Data bits, Parity and Stop bits of COM port and connected device must match.

Baud rate [bps]

List box: standard series of rates from 300 to 115200 bps
Default = 19200
Select Baud rate from the list box: 300 to 115200 bps 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 1s, 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 sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronise with the character stream.

Idle [bytes]

Default = 5 [0 - 2000]
This parameter defines the maximum gap (in bytes) in the received data stream. If the gap exceeds the value set, the link is considered idle, the received frame is closed and forwarded to the network.

MRU [bytes]

Default = 1600 [1 - 1600]
MRU (Maximum Reception Unit) — an incoming frame is closed at this size even if the stream of bytes continues. Consequently, a permanent data stream coming to a COM results in a sequence of MRU-sized frames sent over the network.
Note 1: very long frames (>800 bytes) 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 RipEX (DCE - Data Communications Equipment) can be enabled in order to pause and resume the transmission of data. If RX buffer of RipEX is full, the CTS goes down.
Note: RTS/CTS Flow control requires a 5-wire connection to the COM port.

Protocol*

List box: possible values
Default = None
Each SCADA protocol used on serial interface is more or less unique. The COM port daemon performs conversion to standard UDP datagrams used in RipEX Radio network. Each protocol has its individual configuration parameters, which are described in separate Help page (accessible from configuration light box Protocol - click on Protocol, then on Help). Protocol “None” simply discards any data received by the COM port or from the network, which means that the respective COM port is virtually disconnected from the RipEX.

7.3.5. Protocols

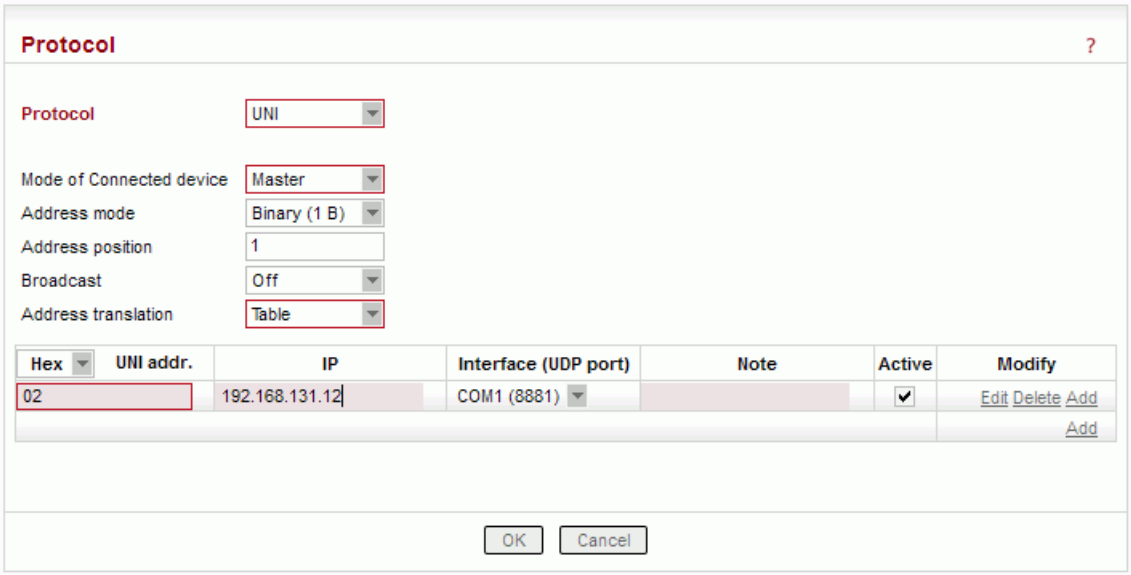


Fig. 7.8: Menu Protocols COM

Generally

Each SCADA protocol like Modbus, DNP3, IEC101, DF1 etc. has its unique message format, most importantly its unique way of addresing of remote units. The basic task for protocol utility is to check whether received frame is within protocol format and it is not corrupted. Most of the SCADA protocols are using some type of Error Detection Codes (Checksum, CRC, LRC, BCC, etc.) for data integrity control, so RipEX calculates this code and check it with the received one.

RipEX radio network works in IP enviroment, so the basic task for Protocol interface utility is to convert SCADA serial packets to UDP datagrams. The Address translation settings are used to define the destination IP address and UDP port. Then these UDP datagrams are sent to RipEX router, processed there and they are typically forwarded as unicasts to Radio channel to their destination. When the gateway defined in the Routing table belongs to the Ethernet LAN, UDP datagrams are rather forwarded to the Ethernet interface. After reaching the gateway (typically a RipEX router again), the datagram is forwarded according to the Routing table.

Note: Even if UDP datagrams, they can be acknowledged on the Radio channel (ACK parameter of Router mode), however they are not acknowledged on Ethernet.

When the UDP datagram reaches its final IP destination, it should be in a RipEX router again (either its ETH or Radio interface). It is processed further according its UDP port. It can be delivered to COM1(2) port daemon, where the datagram is decapsulated and the data received on the serial interface of the source unit are forwarded to COM1(2). The UDP port can also be that of a Terminal server or any other special protocol daemon on Ethernet like Modbus TCP etc. The datagram is then processed accordingly to the respective settings.

RipEX uses a unique, sophisticated protocol on Radio channel. This protocol ensures high probability of data delivery. It also guarantees data integrity even under heavy interference or weak signal conditions due to the 32 bit CRC used, minimises the probability of collision and retransmits frame when a collision happens, etc., etc. These features allow for the most efficient SCADA application arrangements to be

used, e.g. multi-master polling and/or spontaneous communication from remote units and/or parallel communication between remote units etc.

Note: These Radio protocol features are available only in the Router mode. The Bridge mode is suitable for simple Master-Slave arrangement with a polling-type application protocol.

Common parameters

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

Mode of Connected device
List box: Master, Slave
Default = Master
Typical 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 RipEX.
Note: For SCADA Master set Master, for SCADA Slave set Slave.

- **Master**
  SCADA Master always sends addressed messages to Slaves. The way of addressing is different from SCADA protocol to SCADA protocol, so this is one of the main reasons why an individual Protocol utility in RipEX for each SCADA protocol has to be used.
  - **Broadcast**
    List box: On, Off
    Default = Off
    Some Master SCADA units sends broadcast messages to all Slave units. SCADA application typically uses a specific address for such messages. RipEX (Protocol utility) converts such message to an IP broadcast and broadcasts it to all RipEX units resp. to all SCADA units within the network.
    If **On**, the address for broadcast packets in SCADA protocol has to be defined:
    - **Broadcast address format** - List box Hex, Dec - format in which broadcast address is defined.
    - **Broadcast address** - address in the defined format (Hex, Dec)
  - **Address translation**
    List box: Table, Mask
    Default = Mask
    In a SCADA protocol, each SCADA unit has a unique address, a "Protocol address". In RipEX Radio network, each SCADA unit is represented by an IP address (typically that of ETH interface) and a UDP port (that of the protocol daemon or the COM port server to which the SCADA device is connected via serial interface).
    A translation between "Protocol address" and the IP address & UDP port pair has to be done. It can be done either via Table or via Mask.
    So SCADA message received from serial interface is encapsulated into a UDP/IP datagram, where destination IP address and destination UDP port are defined according the settings of Address translation.
    - **Mask**

      Translation using Mask is simpler to set, however it has some limitations:
      − all IP addresses used have to be within the same network, which is defined by this Mask
      − the same UDP port is used for all the SCADA units, which results in the following limitations:
        − SCADA devices on all sites have to be connected to the same interface (COM1 or COM2)

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

- **Base IP**
  Default = IP address of ETH interface
  When the IP destination address of UDP datagram, in which serial SCADA message received from COM1(2) is encapsulated, is created, this Base IP is taken as the basis and only the part defined by Mask is replaced by 'Protocol address'.
- **Mask**
  Default = 255.255.255.0
  A part of Base IP address defined by this Mask is replaced by 'Protocol address'. The SCADA protocol address is typically 1 Byte, so Mask 255.255.255.0 is most frequently used.
- **UDP port (Interface)**
  List box: COM1,COM2, TS1-TS5, TCPM1, Manual.
  This UDP port is used as the destination UDP port in UDP datagram in which serial SCADA packet received from COM1(2) is encapsulated. Default UDP ports for COM1, COM2 or Terminal servers 1-5 (TS1-TS5) or Modbus TCP (TCPM1) can be used or UDP port can be set manually. If the destination IP address belongs to a RipEX and the UDP port is not assigned to COM1(2) or to a Terminal server or to any special daemon running in the destination RipEX, 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 on RS485 interface, their “Protocol addresses” should be translated to the same IP address and UDP port pair, where the multiple SCADA units are connected. There are 3 possibilities how to fill in the line in the table:
− One "Protocol address" to one "IP address" (e.g.: 56 −−> 192.168.20.20)
− Interval of "Protocol addresses" to one "IP address" (e.g.: 56-62 −−> 192.168.20.20)
− Interval of "Protocol addresses" to interval of "IP addresses" (e.g.: 56-62 −−> 192.168.20.20-26). It is possible to write only the start IP and dash, the system will add the end address itself.

- **Protocol address**
  This is the address which is used by SCADA protocol. It may be set either in Hexadecimal or Decimal format according the List box value.
  Protocol address length can be only 1 Byte.
- **IP**
  IP address to which Protocol address will be translated. This IP address is used as destination IP address in UDP datagram in which serial SCADA packet received from COM1(2) is encapsulated.
- **UDP port (Interface)**
  This is UDP port number which is used as destination UDP port in UDP datagram in which the serial SCADA message, received from COM1(2), is encapsulated.
- **Note**
  You may add a note to each address up to 16 characters long for your convenience. (E.g. “Remote unit #1 etc.).
- **Active**
  You may tick/un-tick each translation line in order to make it active/not active.
- **Modify**
  Edit Delete Add buttons allow to edit or to add or to delete a line. The lines can be sorted using up and down arrows.

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

Messages from serial interface are processed in similar way as at Master site, i.e. they are encapsulated in UDP datagrams, processed by router inside the RipEX and forwarded to the respective interface, typically to Radio channel.

- **Broadcast accept**
  List box: On, Off
  Default = On
  If **On**, broadcast messages from the Master SCADA device to all Slave units are accepted and sent to connected Slave SCADA unit.

Protocols implemented:

None

All received frames from COM port are discarded.

Async link

Async link creates asynchronous link between two COM ports on different RipEX units. Received frames from COM1(2) are sent without any processing transparently to Radio channel to set IP destination and UDP port. Received frames from Radio channel are sent to COM1 or COM2 according UDP port settings.

- **Parameters**
  - **Destination IP**
    This is IP address of destination RipEX, either ETH or Radio interface.
  - **UDP port (Interface)**
    This is UDP port number which is used as destination UDP port in UDP datagram in which packet received from COM1(2) is encapsulated.

Modbus

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.
Modbus protocol configuration uses all parameters described in *Common parameters*.

Mode of Connected device

Master

Broadcast

Address translation

Table

Mask

Slave

Broadcast accept

IEC 870-5-101

IEC 870-5-101 is a serial polling-type communication protocol used by Master-Slave application.
When RipEX radio network run in Router mode, more IEC 870-5-101 Masters can be used within one Radio network and one Slave can be polled by more Masters.

IEC 870-5-101 protocol configuration is using all parameters described in *Common parameters*.

Mode of Connected device

Master

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

Address translation

Table

Mask

Slave

Broadcast accept

- **Advanced parameters**
  - **Address mode**
    Even if IEC 870-5-101 is the standard, there are some users which customized this standard according their needs. When addressed byte has been moved, RipEX has to read it on the correct location.
    - **IEC101**
      Address byte location according to IEC 870-5-101 standard.
      Broadcast from Master station is generated when address byte is 0xFF.
    - **2B ADDR**
      Two byte address (IEC 870-5-101 standard is 1 Byte). The frame is 1 Byte longer than standard one. There is Intel sequence of bytes: low byte, high byte. Mask Address translation has to be used, because Table one is limited just to one byte address length.
      Broadcast from Master station is generated when low address byte is 0xFF and high address byte is 0x00.
    - **ENERGO**
      The Control byte in standard IEC packet is omitted. The frame is 1 Byte shorter than standard one.
      Broadcast from Master station is generated when address byte is 0x00.
    - **SINAUT**
      The sequence of Address byte and Control byte in the frame is changed-over.
      Broadcast from Master station is generated when address byte is 0x00.

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 RipEX configuration. The DNP3 allows both Master-Slave polling as well as spontaneous communication from remote units.

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

Address translation

Table

Mask

UNI

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

Generally two communication modes are typical for UNI protocol: In the first one, communication has to be 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 in full, without any modifications.

Underlined parameters are described in *Common parameters*.

Mode of Connected device

Master

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

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

  Example:
  The Address mode is set to Binary (2B LSB first), the Address mask is set to 7FF0 and the Address position is set to 2. The SCADA message starts with bytes (in hex) 02 DA 92 C3 .. The 2-Byte address is read as 0x92DA (note the LSB came first in the message), Then 0x7FF0 mask is applied and the resulting value 0x12D0 (0x92DA & 0x7FF0) is used as the input for the translation.
- **Poll response control**
  List box: On, Off
  Default = On

On – The Master accepts only one response per a request and it must come from the 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.

Broadcast

Address translation

Table

Mask

Slave

Broadcast accept

Comli

Comli is a serial polling-type communication protocol used by Master-Slave application.
When RipEX radio network run in Router mode, more Comli Masters can be used within one Radio network and one Slave can be polled by more Masters.
Broadcasts packets are not used, so the configuration is using only some parameters described *Common parameters*.

Mode of Connected device

Master

Address translation

Table

Mask

Slave

DF1

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

- **Block control mode**
  List box: BCC, CRC

Default = BCC
According to the DF1 specification, either BCC or CRC for Block control mode (data integrity) can be used.

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

Address translation

Table

Mask

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

Profibus

RipEX supports Profibus DP (Process Field Bus, Decentralized Periphery) the widest-spread version of Profibus. The Profibus protocol configuration uses all parameters described in
Common parameters.

Mode of Connected device

Master

Broadcast

Address translation

Table

Mask

Slave

Broadcast accept

C24

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

When a RipEX radio network runs in the Router mode, multiple C24 Masters can be used within one Radio network and one Slave can be polled by more than one Master.

Underlined parameters are described in *Common parameters*.

Mode of Connected device

Master

Address translation

Table

Mask

Slave

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

- **Frames format**
  List box: Format1,Format2,Format3,Format4,Format5
  Default = Format1
  One of the possible C24 Frames formats can be selected. According to the C24 protocol specification, it is possible to set Frames formats 1-4 for Protocol frames 1C-3C and formats 1-5 for 4C.

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

- **Local ACK**
  List box: Off, On
  Default = Off
  Available for Protocol frame 1C only. When **On**, ACK on COM1(2) is send locally from this unit, not over the Radio channel.

RP570

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

When a RipEX radio network runs in the Router mode, multiple RP570 Masters can be used within one Radio network and one Slave can be polled by more than one Master.

Underlined parameters are described in *Common parameters*.

Mode of Connected device

Master

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

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

- **RB Net period [s]**
  Default = 10

The RipEX responds to the RB packets locally and in the set RB period the RB packets are transferred over the network.

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

Address translation

Table

Mask

Slave

Slave

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

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

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

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

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

Cactus

Cactus is a serial polling-type communication protocol used in Master-Slave applications.
When a RipEX radio network runs in the Router mode, multiple Cactus Masters can be used within one Radio network and one Slave can be polled by more than one Master.

Underlined parameters are described in Common parameters.

Mode of Connected device

Master

Broadcast

Note: There is not the possibility to set Broadcast address, since Cactus broadcast messages always have the address 0x00. Hence when the Broadcast is On, packets with this destination are handled as broadcasts.

Address translation

Table

Mask

Slave

Broadcast accept

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

ITT Flygt

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

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

Mode of Connected device

Master

Broadcast

Note: There is not a possibility to set the Broadcast address, since ITT Flygt broadcast messages always have the address 0xFFFF. Hence when the Broadcast is On, packets with this destination are handled as broadcasts.

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

Address translation

Table

Mask

Slave

Broadcast accept

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

7.4. Routing

Routing table **is active only when Router mode** (Settings/Device/Operating mode) is set. In such a case RipEX works as a standard IP router with 2 independent interfaces: Radio and ETH. Each interface has its own MAC address, IP address and Mask. IP packets are then processed according the Routing table.
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 ETH or IP of Radio interfaces. The source IP address of outgoing packets from COM ports is equal to IP address of interface (either Radio or Ethernet) through packet has been sent. Outgoing interface is determined in Routing table according the destination IP.
The IP addressing scheme can be chosen arbitrarily, only 127.0.0.0/8 and 192.0.2.233/30 restriction applies.

7.4.1. Menu Routing

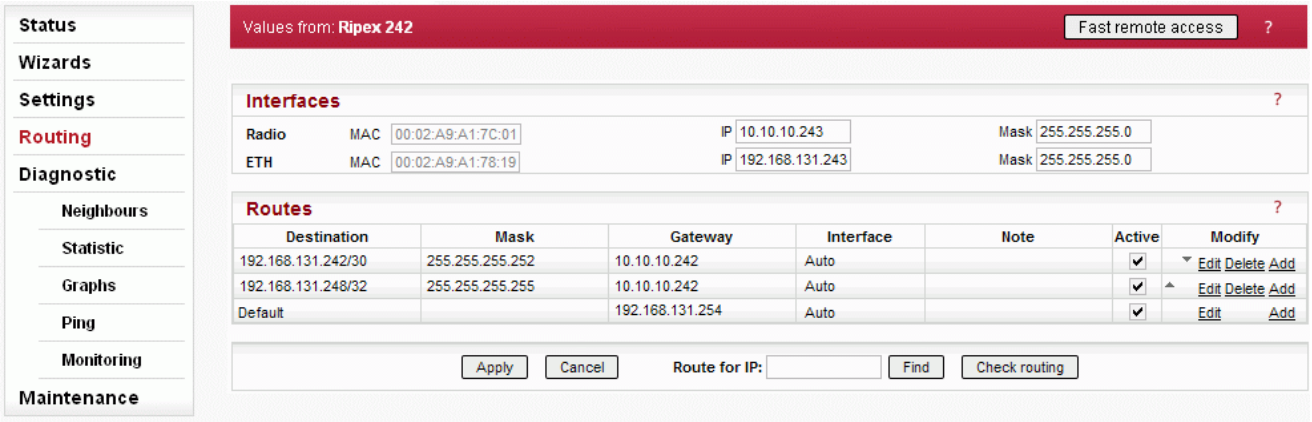


Fig. 7.9: Menu Routing

Interfaces

Radio

IP address and Mask define the IP network (Radio LAN) within RipEX can communicate directly over the Radio channel, however the radio repeater (defined as the gateway in the route) can be used. All units which are supposed to communicate directly have to be within the same Radio LAN.

ETH

IP address and Mask define the IP network (LAN) in which RipEX can communicate directly over the Ethernet. All devices which should be accessible directly have to be within the same LAN.

Routes

Destination, Mask, Gateway

Each IP packet, received by RipEX through any interface (Radio, ETH, COM1 or COM2), has got a destination IP address. RipEX (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 (Radio, ETH), otherwise the packet is discarded.
Each line 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 is not defined (0.0.0.0), the packet is discarded.
The network (Destination and Mask) can by specified in both formats. Either 10.11.12.13/24 in Destination or 10.11.12.13 in Destination and 255.255.255.0. in Mask columns. RipEX displays and converts both formats. There is also a balloon tip while the cursor is in the specific line on the Mask. It shows which IP addresses are included in the network which is routed to the respective Gateway.

Interface

It may happen that networks defined by IP and Mask of router interfaces overlap. In such a case it is necessary to define to which interface (Radio, ETH) the packet should be forwarded.
When Auto is selected, the packet is forwarded automatically to the correct interface.

Note

You may add a note to each route with your comments up to 16 characters for your convenience. (E.g. “Central station” etc.).

Active

You may tick/un-tick each route in order to make it active/not active. This feature is advantageous e.g. when one needs to redirect some route temporarily.

Modify

Edit Delete Add buttons allow to edit or add or delete a line. One may order the lines using up and down arrows.

Buttons

- **Apply** - applies and saves the changes.
- **Cancel** - restores original values.
- **Find** - finds (highlights the respective line in the table) the route for a specific IP address if exists.
- **Check routing** - highlights duplicate routes for specific IP if they exist.

7.5. Diagnostic

7.5.1. Neighbours and Statistic

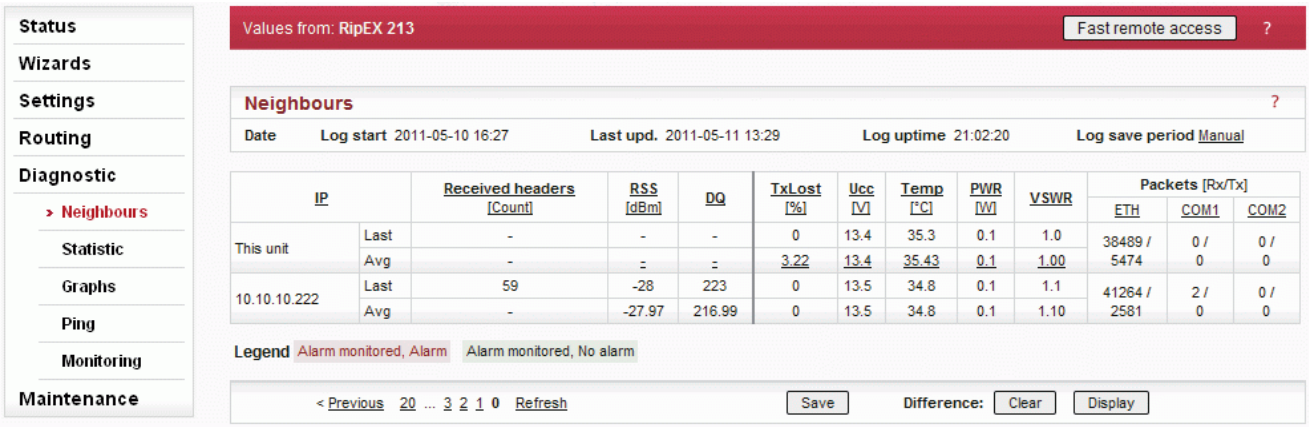


Fig. 7.10: Menu Neighbours

Neighbours and Statistics follow the same pattern.
Most importantly, they share a common time frame. One Log save period and one Difference log (pair of Clear and Display buttons) apply to both logs.
For both logs there is a history of 20 log files available, so the total history of saved values is 20 days (assuming the default value of 1440 min. is used as Log save period). The files are organized in a ring buffer. Whenever a new file is opened or the Operating mode is changed, the numbers of files are shifted, i.e. 0->1, 1->2, etc.
Then both the Neighbours and the Statistic log values are accumulated and weight-averaged over the whole Log save period (one day by default). Hence a fresh change in a traffic pattern is not completely averaged out when the recent log is e.g. 23 hours long.
When a fresh and shorter sample of the log values is needed, there is a Difference log available. It uses an independent buffer for data and can be cleared and displayed anytime.

Buttons

All buttons are common for both logs, Neighbours and Statistic:

- **Save** button – the log is manually saved, stored in the history file and cleared. This equals to situation when the Log save period expires. When the Operating mode (Bridge / Router) is changed, the log is also Saved.
  Note: Remember that both the Neighbours and Statistic logs are saved.
- Difference

  Clear button – when pressed, the Difference log is cleared. The standard Neighbour and Statistic logs are not touched. Similarly, when the Log save period expires and the Neighbour and Statistic logs are cleared, the values in Difference log are not touched.
  Note: Remember that both Neighbours and Statistic logs are cleared.

  Display button – displays values of the Difference log, i.e. the values accumulated from time when the Set button has been pressed.

Notice, that the Log start, Last upd. and Log uptime labels at the top change to Diff. start, Diff. upd. and Diff. uptime when the Difference log is displayed. They show the respective values for Difference log.

- History
  There is a possibility to display history logs using standard buttons. They are placed on the left side of the button bar. The Refresh button displays the latest log values.

Top bar

- **Date** Information about the actual date and time in the RipEX. It can be set in Settings/Device/Time menu.
- **Log start**
  Date and time when the log has been cleared and started.
  The log is cleared and started when Log save period expires or when Save buton is pressed or when power is switched On.
- **Last update**
  Date and time when log has been displayed. For actual values click the Refresh button.
- **Log uptime**
  The difference between Log start and Last update.
- **Log Save period**
  It redirects to Settings/Device/Neighbours&Statistics where Statistic&Neighbours log save period can be set.
  Also the Watched values broadcasting period can be set there. This is a period in which RipEX periodically broadcasts its Watched values to neighbouring units, where they are saved and can be displayed in the Neighbours table.

Neighbours

Neighbours log provides information about neighbouring units (Neighbour = RipEX, which can be accessed directly over the radio channel, i.e. without a repeater).
Protocol on Radio channel uses MAC addresses. A unit can learn the IP address of its neighbour only when it receives its broadcast of Watched values (it contains both MAC and IP addresses). Thus when Watched values broadcasting is Off in a Neighbour (Settings/Device/Neighbours&Statistics), there is MAC address on the respective line in the Neighbours table. When a known IP adress of a Neighbour changes, the unit cumulates data to the old IP address till it receives the next Watched values broadcast. Maximum number of Neighbours listed in the table is 100. If this number is exceeded, the least significant Neighbour is omitted. The first criterion is whether this RipEX communicates with the Neighbour and the second criterion is the RSS level.

Neighbours Table

Generally:

- there are balloon tips with on line help for column names
- the table can be sorted (descending/ascending) by any column, by clicking the column name
- two values are displayed for each item: Last and Average. Last is the last value received, the Average is an average over all values received since the start of the log. The values received recently weigh up to 50% more in the average than the older ones.
- if a value in the table is underlined, it is a link to Graphs
- green background indicates, that the item is monitored for alarm and its average value is within the “normal” range (Settings/Device/Alarm management)

- red background indicates, that the item is monitored for alarm and its average value is in the alarm range (Settings/Device/Alarm management)
- IP addresses:
  - **Bridge mode**
    Due to broadcast pattern of traffic in Radio channel, all frames generated by user application(s) cumulate in one line in the Neighbour table. When diagnostic or service frames (e.g. Watched values) are transmitted in the network, they are listed in separate lines, distinguished by IP address of their respective Ethernet interfaces.
  - **Router mode**
    MAC addresses of Radio interface are used for link layer communication on Radio channel. When RipEX knows the IP address corresponding with the MAC address (the IP has been the destination IP of a packet transferred), IP address is displayed. If the IP address is not known, the MAC address is displayed.

  The first three columns are logged by the receiving RipEX itself.
  - **Received headers [Count]**
    Total number of frame headers received from the respective RipEX.
  - **RSS [dBm]**
    Received Signal Strength.
  - **DQ**
    Data Quality of received frames. The DQ value is about proportional to BER (bit error ratio) and about independent of the data rate and modulation used. Consequently when data rate is lowered, the DQ value increases and the other way round. Judging the DQ values requires experience, rule-of-thumb figures are as followsvalues: DQ below 100 means the link is unusable, aroundt 125 short packets starthould getting through, about 160 and above can be considered “good” values.

  The remaining columns contain values broadcasted by neighbouring units in their Watched values broadcasting periods(Settings/Device/Neighbours&Statistics).
  - **TxLost [%]**
    The probability of a transmitted frame being lost (100 * Lost frames / All transmitted frames). This value is broadcasted only when Router mode is used and ACK is On.
  - **Ucc [V]**
    Power voltage measured on power input.
  - **Temp [°C]**
    Temperature inside of the RipEX.
  - **PWR [W]**
    The actual value of Radio output power measured by RipEX itself.
  - **VSWR**
    Voltage Standing Wave Ratio (1.0=best, 1.0–1.8=acceptable, >2.5=indicates a serious problem in antenna or feeder)
  - **Packets [Rx/Tx]**
    The total number of packets received from / transmitted to ETH, COM1, COM2 interfaces. Can be used for interface activity diagnostic.

Statistic

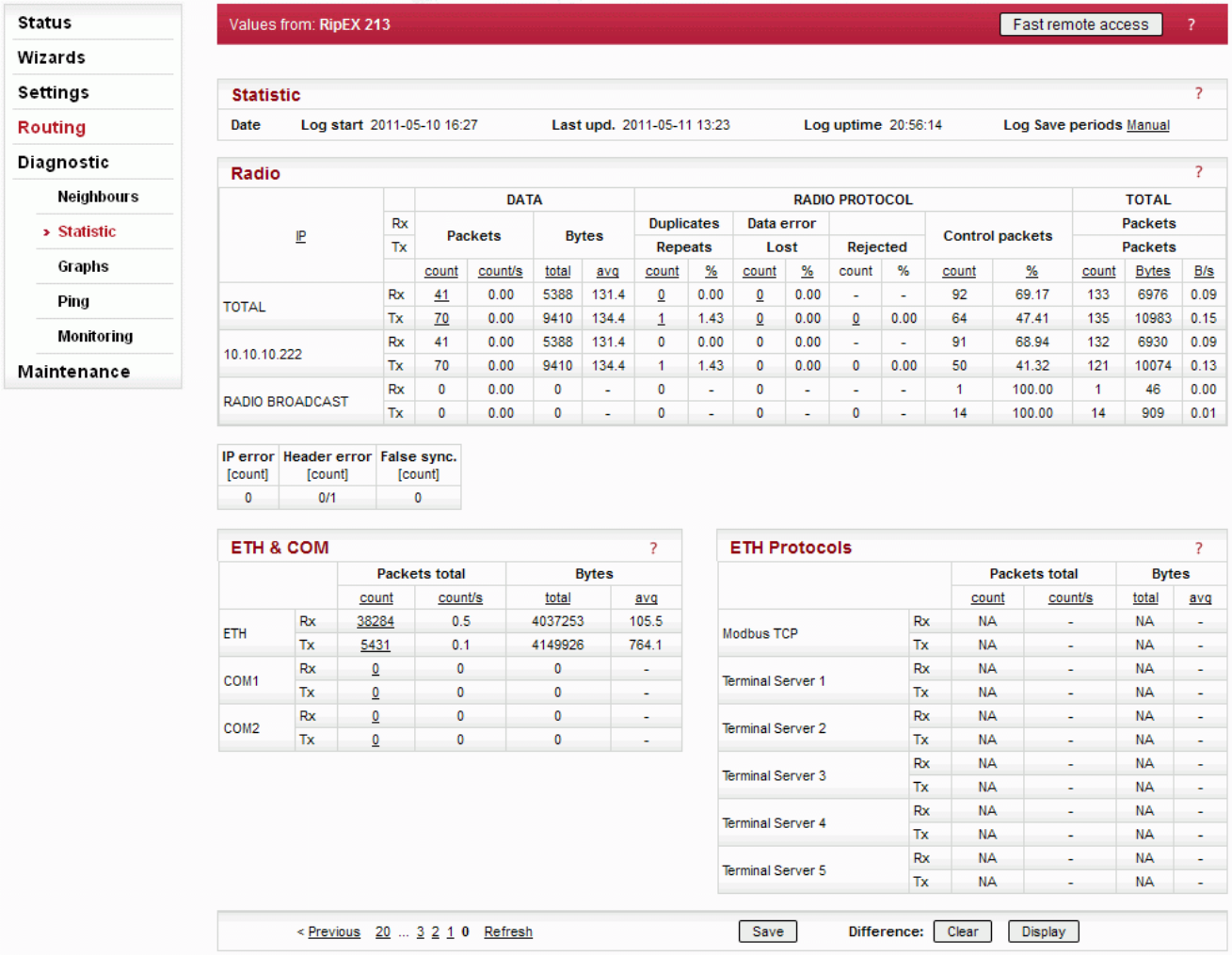


Fig. 7.11: Menu Statistic

Statistic log provides information about communication on all interfaces: Radio, ETH, COM1, COM2. Balloon tips provide on line help for all column names. These tips explain the meanings and the way of calculation of individual values.
Meaning of IP addresses listed:
Rx - for received (Rx) packets, the IP source address from UDP header is displayed. Values in DATA part of the table are calculated for this source IP (origin), values in RADIO PROTOCOL part are for the last radio hop.
Tx - for transmitted (Tx) packets, the IP destination address from UDP header is displayed. Values in DATA part of the table are calculated for this destination IP (final destination), values in RADIO PROTOCOL part are for the next radio hop.
Note: Remember that the IP source and IP destination addresses of user IP packets are not the IP addresses of RipEXes who transport them.

7.5.2. Graphs

Graphs functionalities as well as meanings of **Overview**, **Detail**, **Sampling period** are described in the help Settings/Device.

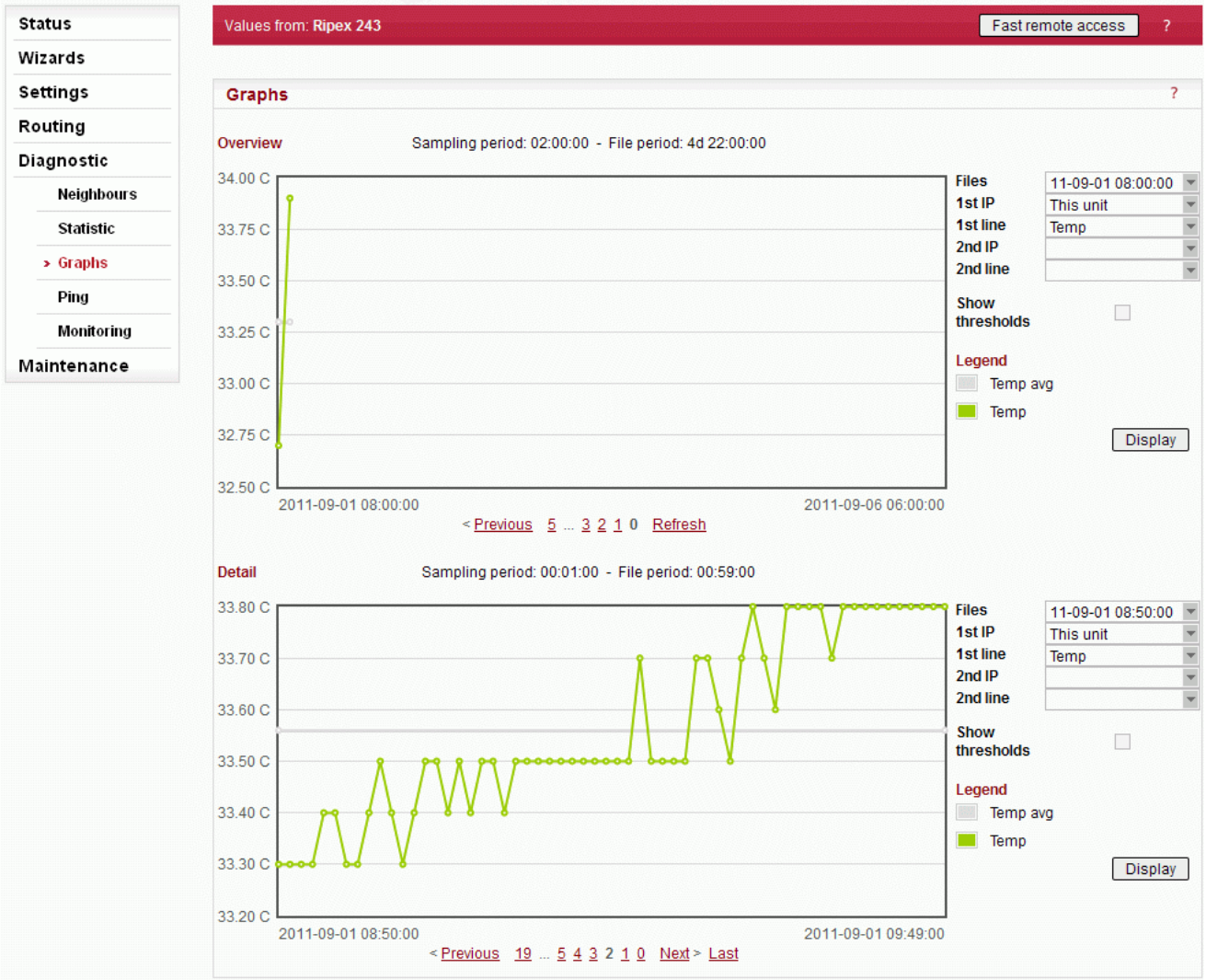


Fig. 7.12: Menu Graphs

- **File period**
  File period corresponds with time, for which the values have been recorded in the file. The 60 samples per graph file result in (depending on the Sampling period) 60 (2d 11:00:00), 120 (4d 23:00:00), 240 (9d 23:00:00) or 720 (29d 23:00:00) hours recorded in each file.
- **Available files**
  List box: possible values
  Default = the newest file
  There is a list of files, which are saved in RipEX and which can be displayed. Date and time corresponds with the start of the file.
- **1st IP**
  List box: possible values
  Default = This unit
  List of IP addresses of RipEXes. from which the graph values are available. The list of recorded units can be set in Settings/Device/Graphs. More in help Settings/Device.
- **1st line**
  List box: possible values
  Default = TxLost
  There is a list of values, which can be displayed. These values are also recorded in Neighbours or Statistic files. You can find their meanings in help Neighbours&Statistic.

- **2nd IP, 2nd line**
  It is possible to display two values from the same unit or from two different ones.
- **Show thresholds**
  You can show thresholds for the displayed value which are set in the unit (Settings/Device/Alarm management).
- **Alarm**
  When displayed value is out of threshold, a red line on the bottom of the graph is shown. Date and time is displayed in balloon tip then.
- **History**
  There is a possibility to change displayed file(s) using standard buttons (Previous 10…6 5 4 .. Next). They are placed below the graph.
- **Refresh**
  Refresh - complete refresh of displayed values.

7.5.3. Tools

Ping

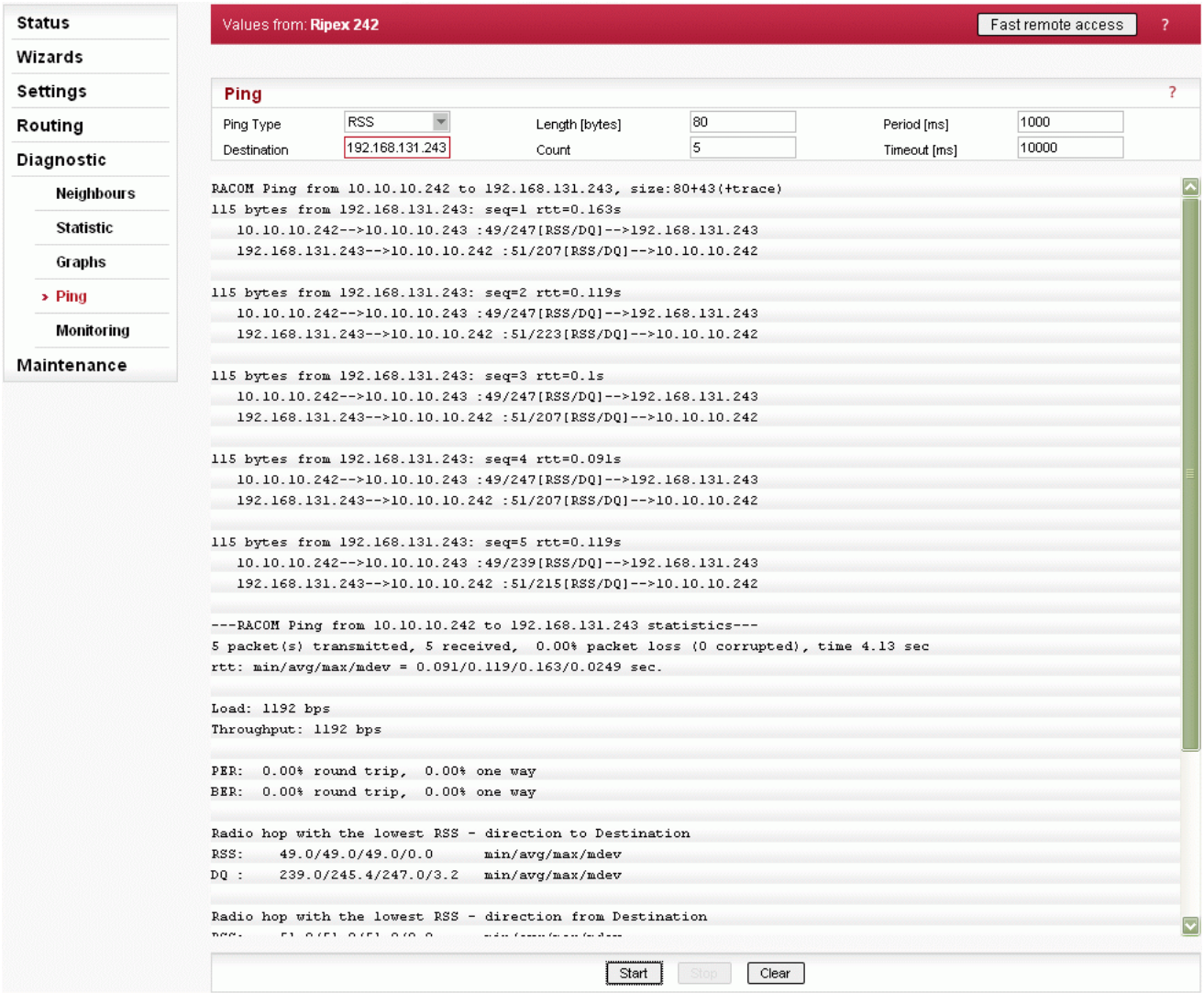


Fig. 7.13: Menu Ping

Ping (Packet InterNet Groper) is a utility used to test the reachability of a particular host on an IP network. It operates by sending echo request packets to the target host and waiting for an echo response. In the process it measures the rtt (round trip time - the time from transmission to reception) and records any packet loss.
The source IP address of Ping in RipEX is always the IP address of Radio interface (Settings/ETH/IP) While using Ping, be sure that correct routing between source and destination IP addresses exists. Also pinged device has to have ICMP echo response enabled. RipEX has the ICMP echo response always enabled.
Note: Ping utility generates on-line report each 2 seconds while you are connected to Local unit and each 10 sec. while it is generated from Remote unit and it is transffered over Radio channel.

- **Ping Type**
  List box: ICMP, RSS
  Default = RSS
  - **ICMP**
    This is a standard ICMP (Internet Control Message Protocol) ping. It can be used against either RipEX or any device connected to RipEX Radio network.
  - **RSS**
    RSS Ping Type uses a special UDP packets and provides extension report which includes:
    - RSS and DQ information for each radio hop for each individual ping
    - RSS and DQ statistic (average, min., max.) for radio hop with the lowest RSS in both directions
    - Histogram of rtt of pings divided to 5 intervals
    - Load and Throughput
    - PER (Packet Error Rate)
    - BER (Bit Error Rate)
- **Destination**
  Default = 127.0.0.1
  Destination IP address
- **Length [bytes]**
  Default = 80
  The length of user data, the range from 8 to 4096 Byte. Some overhead to this Length is always added like these:
  ICMP - 28 bytes
  RSS - 43 bytes for IP+UDP+RACOM header + 8 bytes (Trace-RSS and DQ) per each radio hop + 4 bytes (marking in server)
  RSS ping can not be longer than 3/4 MTU.
- **Count**
  Default = 5
  Number of pings to be transmitted. The allowed range is from 1 to 1024.
- **Period [ms]**
  Default = 1000
  When this Period expires, the next Ping is transmitted. The range is from 1000 (1 sec.) to 3600000 (1 hour).
- **Timeout [ms]**
  Default = 10000
  Timeout from 1000 (1 sec.) to 3600000 (1 hour).
  When ping (the response) is not received within this timeout, it is counted as lost.
- **Report**
  A short report is generated in run-time for each individual ping packet. When the Ping utility is stopped, an overall statistic report is displayed.
  - **ICMP**
    Standard Linux ping reports are provided:
    - **Run-time report:**

"88 bytes from 192.168.131.243: icmp_req=1 ttl=63 time=360 ms"
88 bytes = total packet lenght
192.168.131.243 = destination IP
icmp_req = ping sequence number
ttl = time to live, max. number of hops (passing through router) of the packet in the network
time = rtt (round trip time), the time from transmission of ICMP echo request to reception of ICMP echo response

- **Statistic report:**
  "5 packets transmitted, 5 received, 0% packet loss, time 4002ms"
  "rtt min/avg/max/mdev = 327.229/377.519/462.590/45.516 ms"
  time = total time of ping utility (From Start to Stop buttons)
  rtt min/avg/max/mdev = round trip time, minimal/average/maximal/standard deviation

- **RSS**
  - **Run-time report:**
    "131 bytes from 192.168.131.243: seq=1 rtt=0.805s"
    "10.10.10.241-->10.10.10.242 :56/209[RSS/DQ]-->10.10.10.243:51/225[RSS/DQ]-->192.168.131.243"
    "192.168.131.243-->10.10.10.242 :46/214[RSS/DQ]-->10.10.10.241 :57/213[RSS/DQ]-->10.10.10.241"
    131 bytes = RSS packet size (RACOM header + data + trace)
    10.10.10.242 = repeater IP
    192.168.131.243 = destination IP
    seq = ping sequence number
    rtt = round trip time, the time from transmission to reception
  - **Statistic report:**

    "5 packet(s) transmitted, 5 received, 0.00% packet loss (0 corrupted), time 4.48 sec"
    "rtt: min/avg/max/mdev = 0.371/0.483/0.805/0.166 sec."
    corrupted = number of packets which have been received (UDP header is OK) nevertheless their data have been corrupted (CRC over data is not OK)
    time = the total time of ping utility (From Start to Stop buttons)
    rtt min/avg/max/mdev = round trip time, minimal/average/maximal/standard deviation

    "Load: 1098 bps"
    "Throughput: 1098 bps"
    Load = the load generated by Ping utility
    Throughput = the througput provided by Radio network

    "PER: 0.00% round trip, 0.00% one-way"
    "BER: 0.00% round trip, 0.00% one-way"
    PER - Packet Error Rate, i.e. the probability of a packet being lost. It is calculated for both the whole round trip and a one-way trip.
    BER - Bit Error Rate, the probability of one bit received with incorrect value. Only packets, no bits can be lost in packet radio network. When a single bit is received wrong, the whole packet is lost. The BER is calculated from the PER based on this assumption.

    "Radio hop with lowest RSS – direction to Destination"
    "RSS: 56.0/56.8/58.0/0.7 min/avg/max/mdev"
    "DQ : 208.0/219.0/232.0/9.4 min/avg/max/mdev"

    "Radio hop with lowest RSS – direction from Destination"
    "RSS: 56.0/56.4/57.0/0.5 min/avg/max/mdev"
    "DQ : 208.0/216.2/223.0/5.3 min/avg/max/mdev"

There is RSS (Received Signal Strenght) and DQ (Data Quality) information from the radio hop with lowest RSS, separately for both directions (To and From the destination RipEX). The mdev values for both the RSS and DQ are provided, giving idea on signal homogeneity. The lower values are recorded, the more reliable the link should be. The “Homogenity” shows the jitter of RSS values from individual pings.

"rtt histogram (time interval in sec.: %, count)"
" 0.000 - 2.500: 100.00% 5" XXXXXXXXXX
" 2.500 - 5.000: 0.00% 0"
" 5.000 - 7.500: 0.00% 0"
" 7.500 - 10.000: 0.00% 0"
"10.000 - inf: 0.00% 0"
There is the distribution of rtt (round trip times) of received pings. Time intervals in the table are 1/4 of the Timeout set in ping parameters. The XXXX... characters at the end of the line form a simple bar chart.

- **Buttons**

  Start - starts pinging
  Stop - stops pinging, Statistic report is displayed afterwards
  Clear - clears the reports on the screen

Monitoring

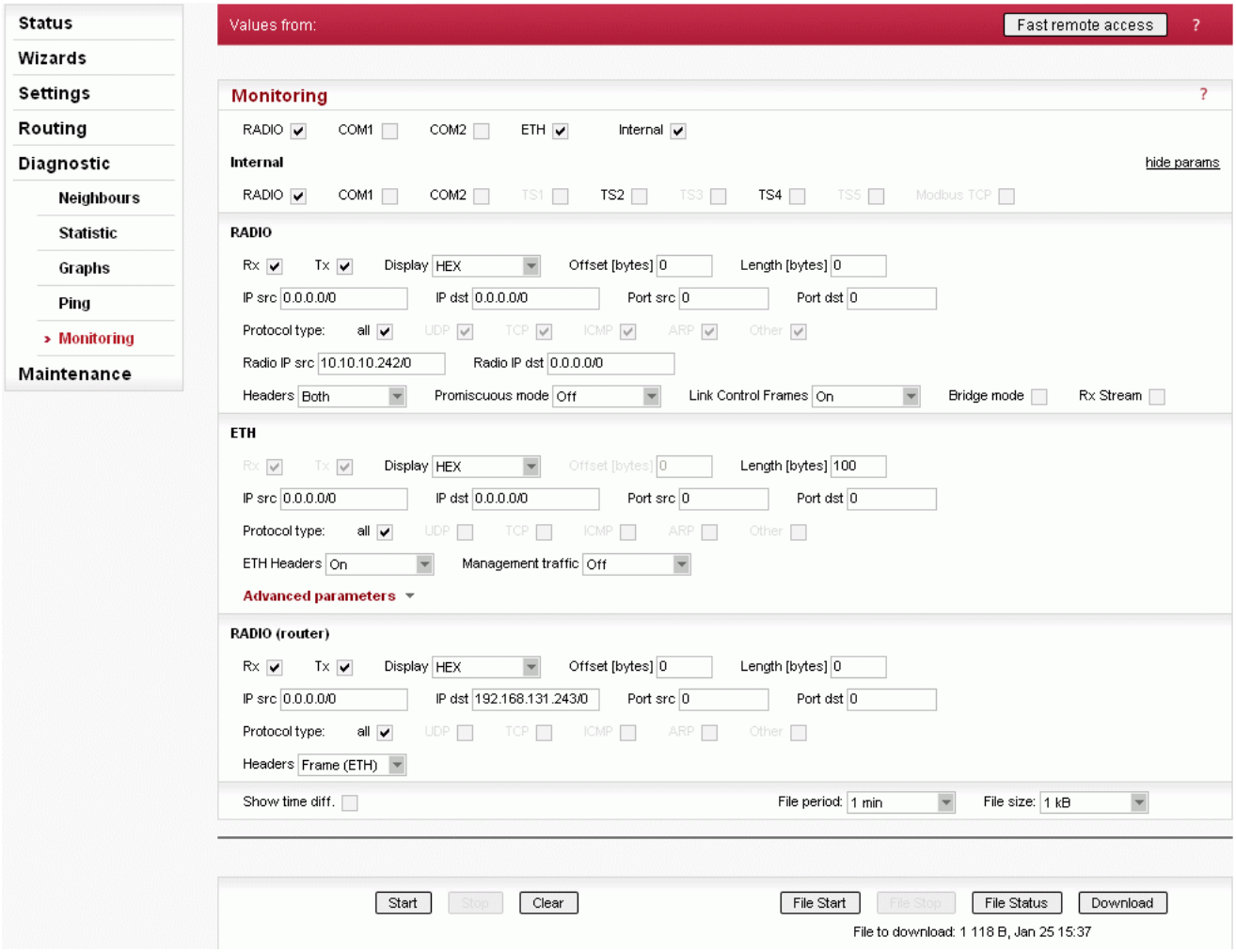


Fig. 7.14: Menu Monitoring

Monitoring is an advanced on-line diagnostic tool, which enables a detailed analysis of communication over any of the interfaces of a RipEX router. In addition to all the physical interfaces (RADIO, ETH, COM1, COM2), 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 RipEX (e.g. a remote RipEX) and downloaded later.
Description of internal interfaces can be found below.

- **Interfaces**
  Tick boxes:
  RADIO, COM1, COM2, ETH, Internal
  When ticked, the setting for the respective interface(s) is enabled. When the "Internal" interface is ticked, another set of interface tick-boxes appears as follows:

  Internal:
  RADIO, COM1, COM2, TS1, TS2, TS3, TS4, TS5, Modbus TCP
  When ticked, the setting for the respective internal interface(s) is enabled (see the description below).
- **Common parameters for all interfaces:** Destination IP address
  - **Rx**

- **Tx**
  Tick boxes.
  When ticked, packets (frames, messages) coming in the respective direction are monitored. 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. COM(phy)) is monitored, the Tx also means packets being transmitted from the RipEX over the respective interface (Rx means "received"}. Understanding the directions over the internal interfaces may not be that straightforward, please consult the diagram below for clarification.
  Please note the separate monitoring of Rx or Tx frames is not possible at the ETH interface.
- **Display**
  List box: HEX, HEX+ASCII, ASCII
  Default = HEX
  The format of monitoring output.
- **Offset [bytes]**
  Default = 0
  Number of bytes from the beginning of packet/frame, which will not be displayed. The Length of bytes will be displayed starting from the immediately next byte.
  This feature is not available at the ETH interface.
- **Length [bytes]**
  Default = 100
  Number of bytes, which will 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): 01AB3798A28593CD6B96
  Monitoring output: 3798A285

- **Filter parameters for IP/ARP packets**
  (available for RADIO, ETH and Internal RADIO (router), COMn(router), TSn(router), Modbus TCP(router)):
  - **IP src**
    IP source address range in the following format: aaa.bbb.ccc.ddd/mask
  - **IP dst**
    IP destination address range in the following format: aaa.bbb.ccc.ddd/mask
  - **Port src**
    TCP/UDP source port (range) in the following format: aaaa(-bbbb)
  - **Port dst**
    TCP/UDP destination port (range) in the following format: aaaa(-bbbb)
  - **Protocol type**
    (available for RADIO, ETH and Internal RADIO (router))
    Tick boxes for displaying specific protocols only. "Other" means displaying everything except the four listed protocols (even non-IP frames in case of the RADIO interface).
- **Interface specific parameters - RADIO**
  - **Radio IP src**
    The Radio IP source address of the frame has to be within the range defined: aaa.bbb.ccc.ddd/mask.
  - **Radio IP dst**
    The Radio IP destination address of the frame has to be within the range defined: aaa.bbb.ccc.ddd/mask.
  - **Headers:**
    List box: None, Radio Link, Data Coding, Both
    Default = None
    - None – only the Radio Link Protocol data is displayed

- Radio Link – Radio Link Control Header is displayed. It contains e.g. frame type, No., Radio MAC addresses etc.
- Data Coding – Data Coding Header is displayed. It contains information on data part compression, fragmentation and encryption.
- Both – Both the above mentioned headers are displayed.

Note that it may be quite difficult to locate the original payload in the data part of a Radio Link Protocol frame. Depending on the operation mode (Bridge vs. Router) and the interface used by the application (ETH, COM, Terminal Server...), different protocol headers (ETH, IP, UDP...) may be present and the whole data part may be compressed and encrypted.

- **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 RipEX unit and broadcast frames are processed further by monitoring filters.
  - On – all frames detected on the Radio channel are passed to monitoring filters
- **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 which pass the other monitoring filters are displayed
- **Bridge mode**
- **Router mode**
  Tick boxes.
  When RADIO interface is in the promiscuous mode, the unit is capable to monitor (receive) the frames which are transmitted in different operation mode (Bridge x Router) than the one set in this unit. Although such frames cannot be fully analysed by the monitoring engine, their content is displayed when the respective mode tick box is ticked. Note that only the applicable tick box is visible.
- **Rx stream**
  Tick box.
  When ticked, received stream mode frames are included in the monitoring output. Applies to Bridge mode with Stream mode frame closing only. Warning : Stream mode traffic typically consists of large number of short frames, hence excessive amount of monitoring data may be generated. Note that TX frames in stream mode are not monitored.

- **Interface specific parameters - ETH**
  - **ETH Headers**
    List box: On, Off
    Default = Off
    When On, the ETH header is included in the monitoring output. Otherwise only the IP packet is displayed.
  - **Management traffic**
    List box: On, Off
    Default=Off
    When Off, datagrams to and from HTTPS, HTTP and SSH ports in this unit are not monitored. This avoids monitoring loop under normal circumstances, i.e. when the on-line monitoring is viewed on local PC connected via the ETH interface.
  - **Advanced parameters:**
    - **User rule**
      The standard tcpdump program is used for ETH monitoring. An arbitrary user rule in tcpdump syntax can be written in the text box. The rule is then added after the rules generated from the filters set for the ETH interface on this web page.

- **Internal - RADIO (router):**
  - **Headers:**
    List box: None, Packet (IP), Frame (ETH)
    Default: None
    - None – Only the payload data is displayed, e.g. the data part of a UDP datagram.
    - Packet (IP) – Headers up to Packet layer are included, i.e. the full IP packet is displayed.
    - Frame (ETH) – The full Ethernet frame is displayed, i.e. including the ETH header
- **Monitoring output control**
  - **Show time diff.**
    Tick box.
    Default = Unticked
    When ticked, the time difference between subsequent packets is displayed in the monitoring output.
  - **File 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
  - **File size**
    List box: 1 KB, 10 KB, 50KB, 100 KB, 500KB, 1 MB, max (~2MB)
    Default = 100 KB
    Upon clicking the File start button, the file is cleared and the monitoring output is copied into it. When the selected File period expires or the File size has been reached, whichever event occurs first, the file is closed and left waiting to be downloaded later. The start and stop of monitoring to file is independent of the on-line monitoring, i.e. the monitoring output is recorded even when the on-line monitoring is stopped.
- **Buttons**

  Buttons located at the bottom of the monitoring screen come in two groups:
  left: **Start**, **Stop**, **Clear** buttons, which control the on-line monitoring, and
  right: **File Start**, **File Stop**, **File Status**, **Download** buttons, which control the recording into the file.
  The two processes can be started/stopped by the respective buttons independently any time. Only one of the **Start**/**Stop** (**File Start**/**File Stop**) button pair is accessible at a time, depending on the status of the respective monitoring process (the other button is gray).
  The **Clear** button clears the screen with on-line monitoring output, even when the monitoring is running at the moment.
  The **File Status** button refreshes the status of the file which is stored in RipEX and of the recording process. It is recommended to use this button whenever you can not be sure whether your browser is synchronized with the server in the RipEX.
  The **Download** button invokes the Download File dialog.
  Whenever the **Start** or **File Start** button is activated, the current settings of the monitoring from your web page are applied. When you change any setting on the page, both Start and File Start buttons indicate that a change has been made. They turn red when the respective monitoring process is idle and they change into Apply button when the monitoring is running, i.e. when the respective Start (File Start) button has been gray. Clicking the Apply button enforces the configuration change (e.g. adding one more interface) to the running monitoring process
- **Internal interfaces description**

  Internal interfaces are the interfaces between a SW module and the central router module. All these interfaces can be located in Fig. 1 below:

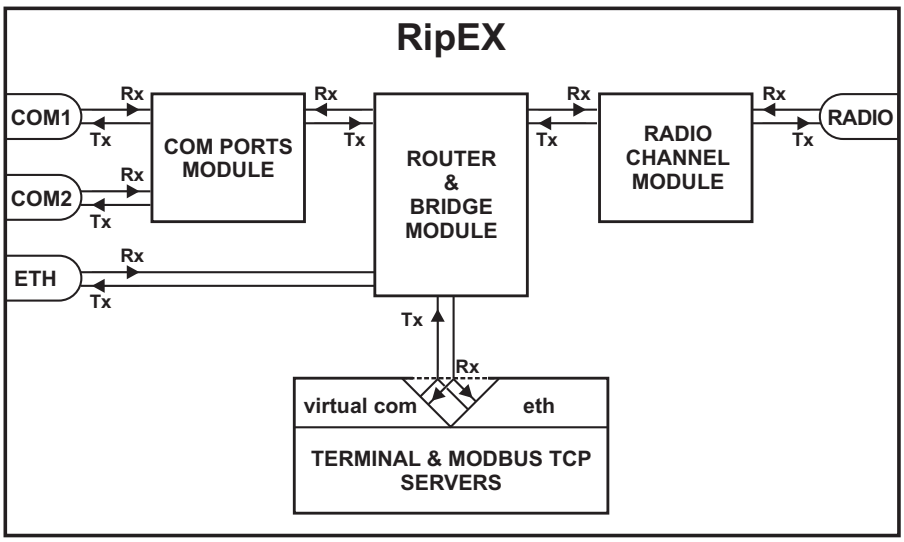


Fig. 7.15: Monitoring

The central router and bridge module acts as a standard IP router or bridge, i.e. decides to which interface an IP packet goes next. The COM ports module does the conversion from messages received over the serial ports to UDP datagrams and vice-versa. The Radio channel module wraps (unwraps) IP packets into radio channel frames and handles all sorts of service frames. Terminal servers process messages from/to virtual COM ports, transforming them into/from the same UDP datagrams as the COM port module does. The Modbus TCP server similarly processes packets of Modbus TCP(RTU) protocol - see the relevant application note (Modbus TCP/RTU) for details. Since it is possible to monitor the messages from virtual COM and the resulting UDP datagrams independently, the TSn and the Modbus TCP have two internal interfaces – distinguished as (com) and (router).

7.6. Maintenance

7.6.1. SW feature keys

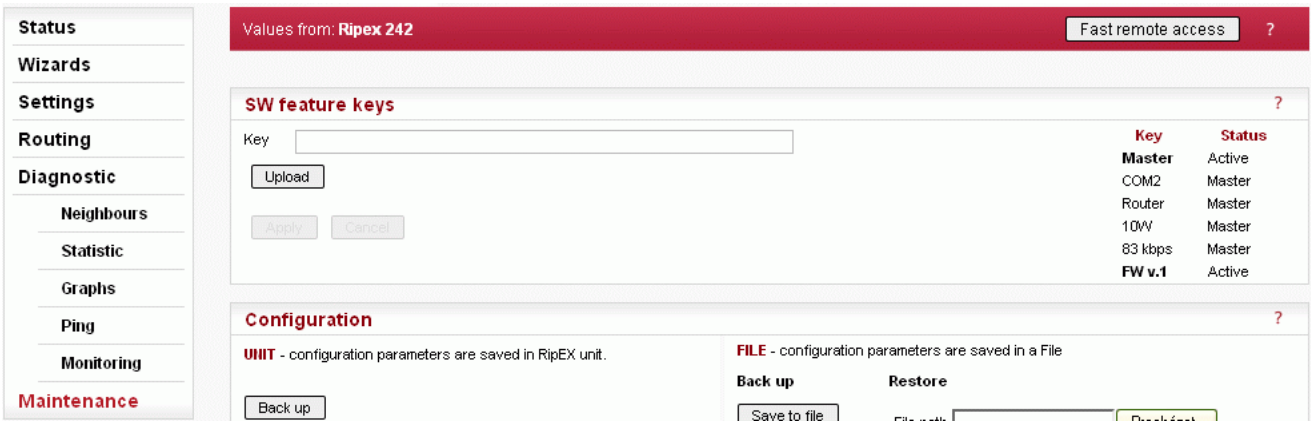


Fig. 7.16: Menu SW feature keys

Certain advanced RipEX features have to be activated by software keys. On the right side one may see the list of available keys and their respective statuses.
Possible status values:

- **Not present**
- **Active**
- **Active (timeout dd:hh:mm:ss)** – the key can be time limited. For such a key, the remaining time of activity is displayed (1d 07:33:20). Time of activity of a key is counted only when the unit is switched on. Time limited key can be put on hold, i.e. temporarily deactivated. Press the respective Hold button (possibly several Hold buttons for several selected keys) and then press the Apply button to put the selected key(s) on hold.

  On hold (timeout dd:hh:mm:ss) – the key is On hold, i.e. temporarily not active. To re-activatete such key, press the Activate and then Apply buttons.
- **Master –** when Master key (unlocks all keys) is active.
- **Master (On hold)** – The time-limited key for a specific feature is On hold, however the feature is active because of the Master key. Buttons Hold and Activate manage a specific feature key, never the Master key.

Fill in the key you have received from RACOM or your distributor.

- **Upload** – when pressed, the selected SW key is uploaded into the RipEX, however it is not active yet. You can subsequently upload more keys.
- **Apply** – when pressed, all the uploaded keys are activated and/or statuses of Time limited keys are changed following their respective buttons Activate or Hold have been pressed. Afterwards the unit automatically reboots.

7.6.2. Configuration

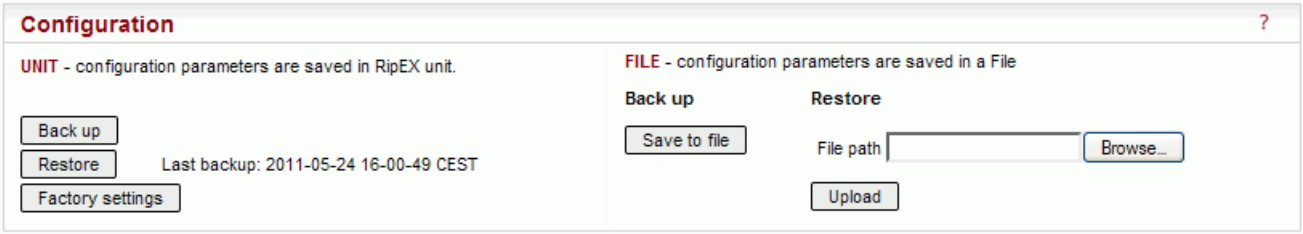


Fig. 7.17: Menu Maintenance Configuration

- **UNIT**
  - **Back up** – Back up saves the active configuration into a backup file in the unit.
  - **Restore** – configuration saved in the backup file in the unit is activated and the unit reboots.
  - **Factory settings** – sets the factory defaults and activates them. Neighbours, Statistic and Graphs databases are cleared. The unit reboots afterwards.

    The following items are NOT cleared when the Factorry settings are applied:
    1. Technical support package
    2. Firmware archive
    3. Configuration backup
    4. Folder /home/… in Linux

    When you need to reset the device access parameters (the login, password and ethernet IP) to defaults, press the RESET button on RipEX's bottom-side enclosure for 15 sec. More in Section 4.2.6, "Reset button".
- **FILE**
  - **Save to file** – saves the active configuration into a file.

Configuration can be uploaded from a file. Fill in the file path, or browse your disk in order to find the file. When a file is selected, it can be uploaded.

- **Upload** – uploads configuration from the selected file and activates it. The unit reboots afterwards.

7.6.3. Firmware

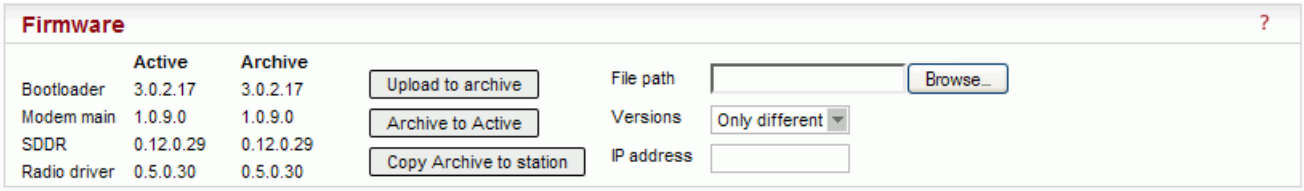


Fig. 7.18: Menu Maintenance Firmware

The firmware in the unit consists of several parts, however they come in one firmware package (file_name.cpio). Individual part names and their versions can be seen. There can be two versions of firmware packages stored within the unit – "Active" and "Archive". Unit is always using the Active version. The Archive version is there just for convenience and safety of firmware manipulations. It can be also uploaded to a remote unit over the Radio channel.

- **Upload to Archive** – Fill in the file path, or browse your disk in order to find the file. When the file is selected and the "Upload to Archive" button pressed, it is uploaded and becomes the Archive firmware.
- **Archive to Active** – when pressed, the Active firmware is substituted by the Archive firmware. Either "All" or only "Only the different" versions are replaced according to the **Versions** list box setting. The unit reboots afterwards.
- **Copy Archive to station** – The Archive firmware package can be copied to another unit. Fill in the **IP address** of the desired unit and press the button.

7.6.4. Password

Fig. 7.19: Menu Maintenance Password

It is highly recommended to change default password (admin) even if the user name remains always the same (admin). When the Apply button is pressed, the unit reboots.

7.6.5. Miscellaneous

- **Reboot** – when pressed, the unit correctly shuts down and starts again (performs the cold start which equals to a power cycle). The reboot time is approx. 25 sec.

7.6.6. Technical support package

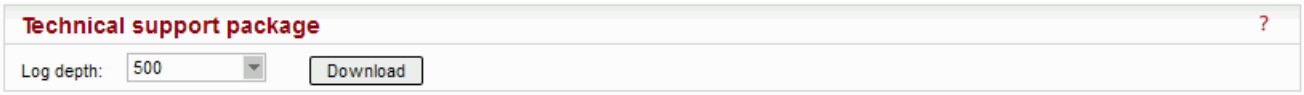


Fig. 7.20: Menu Maintenance Configuration

Technical support package is the file where some internal events are recorded. It can be used by RACOM technical support when a deeper diagnostic is required. The most recent part of it can be downloaded to the local PC.

- **Log depth**
  List box: possible values
  Default = 500
  This is the number of rows downloaded. The greater the number of rows, the longer the history to be found in the file. However more lines means greater file size as well. When downloaded from a remote unit over Radio channel in poor signal conditions, a lower Log depth should be selected.

8. CLI Configuration

CLI interface (Command Line Interface) is an alternative to HTTPS. You can work with the CLI interface in text mode using an appropriate client, either ssh (putty) or telnet.

Connecting with a putty client. Type the following command into the window *Host Name* (or IP address):

```
admin@192.168.169.169
```

Press Open. Then enter the password *admin*.

```
Thu Mar 31 10:56:47 CEST 2011
Welcome to RipEX Command Line Interface (CLI) on station: RipEX 50

For help try: cli_help

CLI(admin):~$
```

The `cli_help` command shows a list of all available functions. The commands can be completed using the Tab key. If you select the command with the left mouse button, you can copy it to the clipboard and then use the right mouse button to insert it into the location of the cursor. You can use the -t parameter to send commands to remote RipEX's. Every command gives a comprehensive help when invoked with -h or –help parameter.

An example of a parameter request for the COM1 port of the RipEX with IP 192.168.1.1:

```
CLI(admin):~$ cli_cnf_show_com 1 -t 192.168.1.1
COM UDP port setting: Default (d)
COM UDP port (manual): 50001
COM link type: RS232 (RS232)
COM bitrate: 19200 (19200)
COM data bits: 8 (8)
COM parity: None (n)
COM stop bits: 1 (1)
COM idle size: 5 chars
COM MTU: 1600 bytes
COM handshake: None (n)
COM break length: 1000 chars
COM protocol: None (n)
```

The CLI is a powerful tool for advanced management of RipEX, especially suited for automated tasks. It is best learned through its own help system, hence it is not described in further detail here.

9. Troubleshooting

1. **I don’t know what my RipEX’s IP is – how do I connect?**

   - Use the "X5" – external ETH/USB adapter and a PC as a DHCP client. Type 10.9.8.7 into your browser’s location field.

   - Alternatively, you can reset your RipEX to default access by pressing the Reset button for a long time, see Section 4.2.6, “Reset button”

     . Afterwards, you can use the IP 192.168.169.169/24 to connect to the RipEX. Note that, in addition to resseting access parameters to defaults, your firewall rules will be cleared as well.

2. **My PC is unable to connect to the RipEX.**

   - In PC settings, Network protocol (TCP/IP)/Properties, the following configuration is sometimes used:

     ```
     General tab - Automatically receive address from a DHCP server
     Alternate configuration tab - User defined configuration,
     e.g. 192.168.169.250
     ```

     Use this configuration instead:

     ```
     General tab - Use the following IP,
     e.g. 192.168.169.250
     ```

   - Verify your PC’s IP address from the command line:

     ```
     Start/Run/command
     ipconfig
     ```

     Send a ping to the RipEX:

     ```
     ping 192.168.169.169
     ```

     If the ping runs successfully, look for a problem with the browser configuration. Sometimes the browser may need minutes to make new connection.

3. **I’m configuring the RipEX in its default state but it’s not working.**

   - There is another RipEX with the default configuration in close vicinity. Switch it off.

4. **I have configured one RipEX in its default state. But I cannot connect to another.**

   - Your PC keeps a table of IP addresses and their associated MAC addresses. You can view it from the command line:

     ```
     Start/Run/command
     arp -a

     IP address          physical address   type
     192.168.169.169     00-02-a9-00-fe-2c  dynamic
     ```

     All RipEX’s share the default IP address but their MAC addresses are different, meaning this record interferes with your purpose. The timeout for automatic cache clearing may be longer so you can delete the entry manually by typing:

```
arp -d 192.168.169.169
```

or delete the entire table by typing:

```
arp -d *
```

Then you can ping the newly connected RipEX again.

5. **I have assigned the RipEX a new IP address and my PC lost connection to it.**

   - Change the PC's IP address so that it is on the same subnet as the RipEX.

6. **I entered the Router mode and lost connection to the other RipEX's.**

   - Enter correct data into the routing tables in all RipEX's.

7. **The RSS Ping test shows low RSS for the required speed.**

   - Use higher output, a unidirectional antenna, better direct the antenna, use a better feed line, taller pole. If nothing helps, lower the speed.

8. **The RSS Ping test reports good RSS but low DQ.**

   - When the DQ value is much lower then it should be at the given RSS, typicaly it is a case of multi-path propagation. It can cause serious problems to data communication, especially when high data rates are used. Since the interfering signals come from different directions, changing the direction of the antenna may solve the problem. A unidirectional antenna should be used in the first place. Metallic objects in close vicinity of the antenna may cause harmful reflections, relocating the antenna by few meters may help. Change of polarization at both ends of the link could be the solution as well.

9. **The RSS Ping test shows bad homogeneity.**

   - Quite often the bad homogeneity comes together with a low DQ. In that case follow the advice given in the previous paragraph. If the DQ does correspond to the RSS level, you should look for unstable elements along the signal route – a poorly installed antenna or cable, moving obstacles (e.g. cars in front of the antenna), shifting reflective areas etc. If you cannot remove the cause of disturbances, you will need to ensure signal is strong enough to cope with it.

10. Safety, environment, licensing

10.1. Frequency

The radio modem must be operated only in accordance with the valid frequency license issued by national frequency authority and all radio parametres have to be set exactly as listed.

Important

Use of frequencies between 406.0 and 406.1 MHz is worldwide-allocated only for International Satellite Search and Rescue System. These frequencies are used for distress beacons and are incessantly monitored by the ground and satellite Cospas-Sarsat system. Other use of these frequencies is forbidden.

10.2. Safety distance

Do not stay in close vicinity of the antenna when the radio modem is in operation. The safety distance with respect to the US health limits of the electromagnetic field intensity are in table Minimum Safety Distance below. The distances apply for output power 10 W. Details can be found at www.fcc.gov/oet/info/documents/bulletins.

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 bellow comply with all applicable standards for human exposure of general public to RF electromagnetic fields.

Tab. 10.1: Minimum Safety Distance 160 MHz

160 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]
OV160.1	single dipole	4.6	2.9	185	83
OV160.2	stacked double dipole	7.6	5.8	261	117
SA160.3	5 element directional Yagi	8.0	6.3	273	122
SA160.5	9 element directional Yagi	12.5	17.8	459	205

160 MHz/2 m band – 5 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]
OV160.1	single dipole	4.6	2.9	131	58
OV160.2	stacked double dipole	7.6	5.8	184	83
SA160.3	5 element directional Yagi	8.0	6.3	193	86
SA160.5	9 element directional Yagi	12.5	17.8	324	145

160 MHz/2 m band – 4 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]
OV160.1	single dipole	4.6	2.9	117	52
OV160.2	stacked double dipole	7.6	5.8	165	74
SA160.3	5 element directional Yagi	8.0	6.3	173	77
SA160.5	9 element directional Yagi	12.5	17.8	290	130

160 MHz/2 m band – 3 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]
OV160.1	single dipole	4.6	2.9	101	45
OV160.2	stacked double dipole	7.6	5.8	143	64
SA160.3	5 element directional Yagi	8.0	6.3	150	67
SA160.5	9 element directional Yagi	12.5	17.8	251	112

160 MHz/2 m band – 2 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]
OV160.1	single dipole	4.6	2.9	83	37
OV160.2	stacked double dipole	7.6	5.8	117	52
SA160.3	5 element directional Yagi	8.0	6.3	122	55
SA160.5	9 element directional Yagi	12.5	17.8	205	92

160 MHz/2 m band – 1 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]
OV160.1	single dipole	4.6	2.9	58	26
OV160.2	stacked double dipole	7.6	5.8	83	37
SA160.3	5 element directional Yagi	8.0	6.3	86	39
SA160.5	9 element directional Yagi	12.5	17.8	145	65

160 MHz/2 m band – 0.5 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]
OV160.1	single dipole	4.6	2.9	41	19
OV160.2	stacked double dipole	7.6	5.8	58	26
SA160.3	5 element directional Yagi	8.0	6.3	61	27
SA160.5	9 element directional Yagi	12.5	17.8	103	46

160 MHz/2 m band – 0.2 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]
OV160.1	single dipole	4.6	2.9	26	12
OV160.2	stacked double dipole	7.6	5.8	37	17
SA160.3	5 element directional Yagi	8.0	6.3	39	17
SA160.5	9 element directional Yagi	12.5	17.8	65	29

160 MHz/2 m band – 0.1 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]
OV160.1	single dipole	4.6	2.9	19	8
OV160.2	stacked double dipole	7.6	5.8	26	12
SA160.3	5 element directional Yagi	8.0	6.3	27	12
SA160.5	9 element directional Yagi	12.5	17.8	46	21

Tab. 10.2: Minimum Safety Distance 300–400 MHz

300–400 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	122	55
OV380.2	stacked double dipole	7.6	5.8	172	77
SA380.3	3 element directional Yagi	7.6	5.8	172	77
SA380.5	5 element directional Yagi	8.7	7.4	195	87
SA380.9	9 element directional Yagi	12.5	17.8	302	135

300–400 MHz/70 cm band – 5 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	86	39
OV380.2	stacked double dipole	7.6	5.8	122	54
SA380.3	3 element directional Yagi	7.6	5.8	122	54
SA380.5	5 element directional Yagi	8.7	7.4	138	62
SA380.9	9 element directional Yagi	12.5	17.8	214	96

300–400 MHz/70 cm band – 4 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	77	34
OV380.2	stacked double dipole	7.6	5.8	109	49
SA380.3	3 element directional Yagi	7.6	5.8	109	49
SA380.5	5 element directional Yagi	8.7	7.4	124	55
SA380.9	9 element directional Yagi	12.5	17.8	191	86

300–400 MHz/70 cm band – 3 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	67	30
OV380.2	stacked double dipole	7.6	5.8	94	42
SA380.3	3 element directional Yagi	7.6	5.8	94	42
SA380.5	5 element directional Yagi	8.7	7.4	107	48
SA380.9	9 element directional Yagi	12.5	17.8	166	74

300–400 MHz/70 cm band – 2 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	54	24
OV380.2	stacked double dipole	7.6	5.8	77	34
SA380.3	3 element directional Yagi	7.6	5.8	77	34
SA380.5	5 element directional Yagi	8.7	7.4	87	39

300–400 MHz/70 cm band – 2 W RF power					
SA380.9	9 element directional Yagi	12.5	17.8	135	61

300–400 MHz/70 cm band – 1 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	39	17
OV380.2	stacked double dipole	7.6	5.8	54	24
SA380.3	3 element directional Yagi	7.6	5.8	54	24
SA380.5	5 element directional Yagi	8.7	7.4	62	28
SA380.9	9 element directional Yagi	12.5	17.8	96	43

300–400 MHz/70 cm band – 0.5 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	27	12
OV380.2	stacked double dipole	7.6	5.8	39	17
SA380.3	3 element directional Yagi	7.6	5.8	39	17
SA380.5	5 element directional Yagi	8.7	7.4	44	20
SA380.9	9 element directional Yagi	12.5	17.8	68	30

300–400 MHz/70 cm band – 0.2 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	17	8
OV380.2	stacked double dipole	7.6	5.8	24	11
SA380.3	3 element directional Yagi	7.6	5.8	24	11
SA380.5	5 element directional Yagi	8.7	7.4	28	12
SA380.9	9 element directional Yagi	12.5	17.8	43	19

300–400 MHz/70 cm band – 0.1 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	12	5
OV380.2	stacked double dipole	7.6	5.8	17	8
SA380.3	3 element directional Yagi	7.6	5.8	17	8
SA380.5	5 element directional Yagi	8.7	7.4	20	9
SA380.9	9 element directional Yagi	12.5	17.8	30	14

10.3. High temperature

If the RipEX is operated in an environment where the ambient temperature exceeds 55 °C, the RipEX must be installed within a restricted access location to prevent human contact with the enclosure heatsink.

10.4. RoHS and WEEE compliance

The RipEX is fully compliant with the European Commission"s RoHS (Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment) and WEEE (Waste Electrical and Electronic Equipment) environmental directives.

RoHS Restriction of hazardous substances (RoHS)

The RoHS Directive prohibits the sale in the European Union of electronic equipment containing these hazardous substances: lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyls (PBBs), and polybrominated diphenyl ethers (PBDEs).

End-of-life recycling programme (WEEE)

The WEEE Directive concerns the recovery, reuse, and recycling of electronic and electrical equipment. Under the Directive, used equipment must be marked, collected separately, and disposed of properly. Racom has instigated a programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive (EU Waste Electrical and Electronic Equipment 2002/96/EC).

The WEEE Directive concerns the recovery, reuse, and recycling of electronic and electrical equipment. Under the Directive, used equipment must be marked, collected separately, and disposed of properly. Racom has instigated a programme to manage the reuse, recycling, and recovery of waste in an environmentally safe manner using processes that comply with the WEEE Directive (EU Waste Electrical and Electronic Equipment 2002/96/EC).

Battery Disposal—This product may contain a battery. Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. Batteries are marked with a symbol, which may include let-

tering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling return the battery to your supplier or to a designated collection point. For more information see: www.weeerohsinfo.com

10.5. Conditions of Liability for Defects and Instructions for Safe Operation of Equipment

Please read these safety instructions carefully before using the product:

- Liability for defects does not apply to any product that has been used in a manner which conflicts with the instructions contained in this operator manual, or if the case in which the radio modem is located has been opened, or if the equipment has been tampered with.
- The radio equipment can only be operated on frequencies stipulated by the body authorised 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 unauthorised way.
- Equipment mentioned in this operator manual may only be used in accordance with instructions contained in this manual. Error-free and safe operation of this equipment is only guaranteed if this equipment is transported, stored, operated and controlled in the proper manner. The same applies to equipment maintenance.
- In order to prevent damage to the radio modem and other terminal equipment the supply must always be disconnected upon connecting or disconnecting the cable to the radio modem data interface. It is necessary to ensure that connected equipment has been grounded to the same potential.
- Only undermentioned manufacturer is entitled to repair any devices.

10.6. Important Notifications

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

Conditions of use of this product software abide by the license mentioned below. The program spread by this license has been freed with the purpose to be useful, but without any specific guarantee. The author or another company or person is not responsible for secondary, accidental or related damages resulting from application of this product under any circumstances.

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

RACOM Open Software License

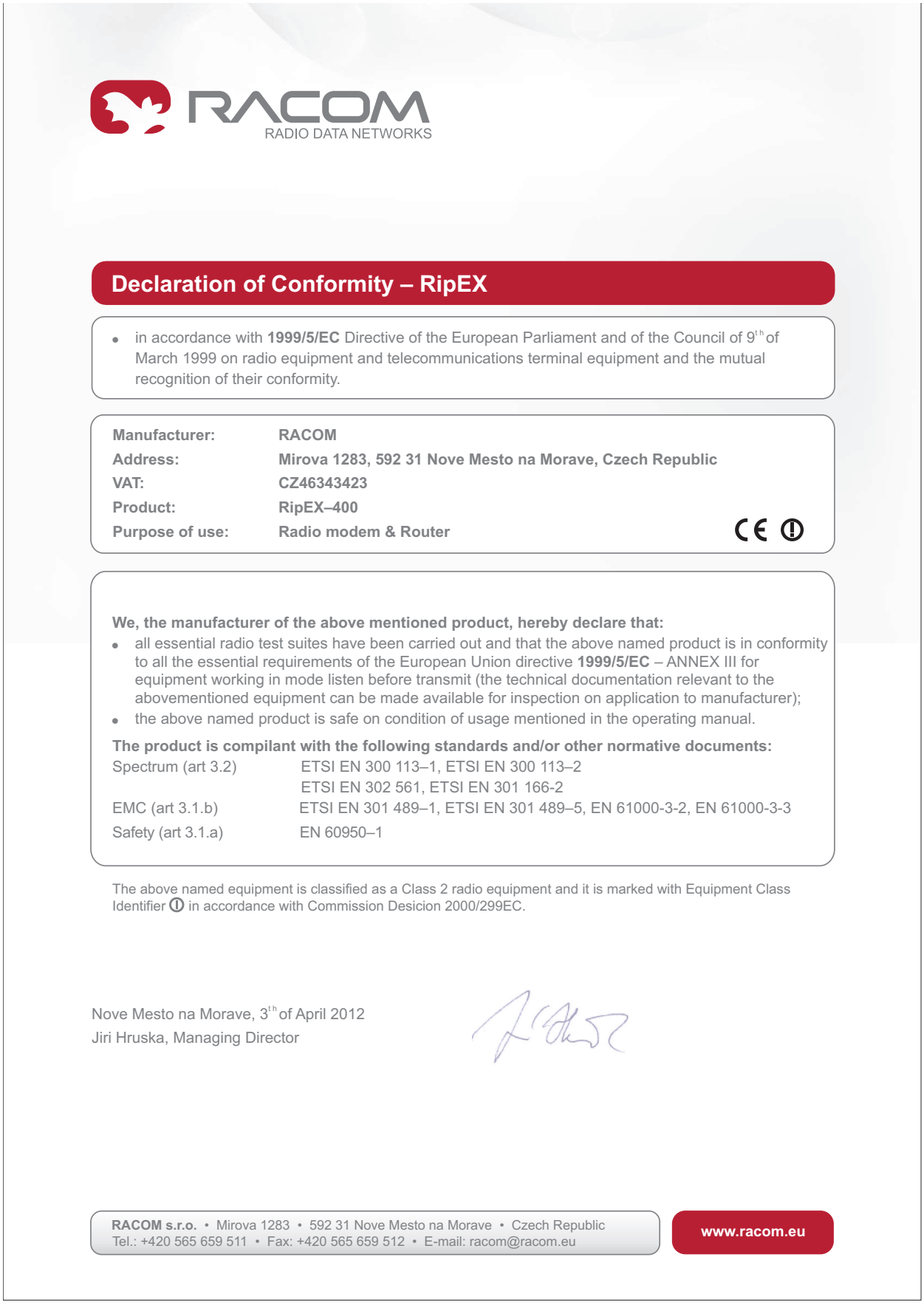
Version 1.0, November 2009

Everyone can copy and spread word-for-word copies of this license, but any change is not permitted.

The program (binary version) is available for free on the contacts listed on http://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 licences, declarations of responsibility exclusion and notifications. Exact terms of GPL, LGPL and some further licences 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 licences on contacts listed on http://www.racom.eu. This product also includes software developed by the University of California, Berkeley and its contributors.

10.7. Product Conformity

Hereby, RACOM s. r. o., declares that this RipEX radio modem & router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/ES. This equipment therefore bears the CE marking. The warning exclamation mark in the circle marks the radio modem as class 2 equipment denoting radio equipment with possible limitations or with requirements on authorisation to use radio equipment in certain countries.



RACOM
RADIO DATA NETWORKS

Declaration of Conformity – RipEX

- in accordance with **1999/5/EC** Directive of the European Parliament and of the Council of 9th of March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Manufacturer:	**RACOM**
Address:	**Mirova 1283, 592 31 Nove Mesto na Morave, Czech Republic**
VAT:	**CZ46343423**
Product:	**RipEX–400**
Purpose of use:	**Radio modem & Router**

CE

We, the manufacturer of the above mentioned product, hereby declare that:

- all essential radio test suites have been carried out and that the above named product is in conformity to all the essential requirements of the European Union directive **1999/5/EC** – ANNEX III for equipment working in mode listen before transmit (the technical documentation relevant to the abovementioned equipment can be made available for inspection on application to manufacturer);
- the above named product is safe on condition of usage mentioned in the operating manual.

The product is compilant with the following standards and/or other normative documents:

Spectrum (art 3.2)	ETSI EN 300 113–1, ETSI EN 300 113–2 ETSI EN 302 561, ETSI EN 301 166-2
EMC (art 3.1.b)	ETSI EN 301 489–1, ETSI EN 301 489–5, EN 61000-3-2, EN 61000-3-3
Safety (art 3.1.a)	EN 60950–1

The above named equipment is classified as a Class 2 radio equipment and it is marked with Equipment Class Identifier ⓘ in accordance with Commission Desicion 2000/299EC.

Nove Mesto na Morave, 3th of April 2012
Jiri Hruska, Managing Director

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic
Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

www.racom.eu

Fig. 10.1: RipEX consistency declaration

Appendix A. Abbreviations

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

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

Index

R

S

T

U

Appendix B. Revision History

Revision
This manual was prepared to cover a specific version of firmware code. Accordingly, some screens and features may differ from the actual unit you are working with. While every reasonable effort has been made to ensure the accuracy of this publication, product improvements may also result in minor differences between the manual and the product shipped to you.

Revision 1.1 2011-08-31
First issue

Revision 1.2 2011-12-31
PoE is not supported in RipEX from 1.1.2012, so all information about PoE has been removed

Revision 1.3 2011-01-26
Added information about Monitoring Upgraded information about Terminal servers (IP port dynamical changes support)
New serial SCADA protocols - RP570, C24 Melsec, ITT Flygt, Cactus