RACOM
RADIO DATA NETWORKS

User manual

RipEX
Radio modem & Router

version 0.0
5/17/2011
fw 1.0.4.0

= PRELIMINARY =

Table of Contents

List of Figures

List of Tables

Getting started

RipEX is a widely configurable compact radio modem, more precisely a radio IP router. All you have to do to put it into operation is to connect it to an antenna and a power supply and configure it using a PC and a web browser.
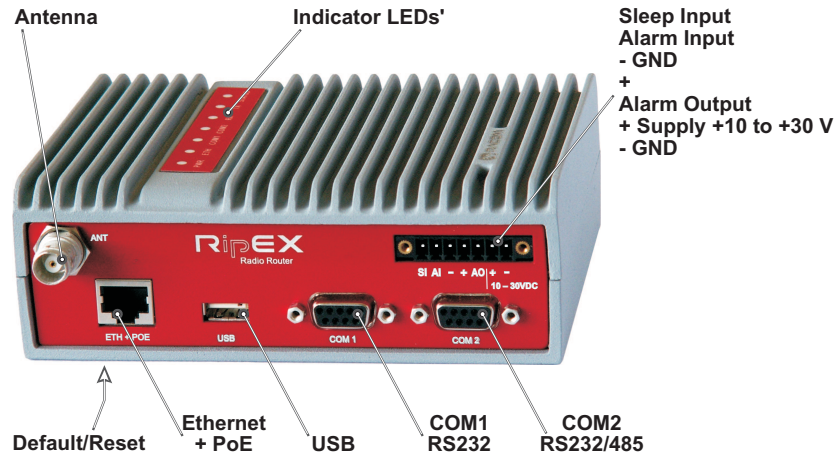
Fig. 1: RipEX radio router

RipEX access defaults: IP 192.168.169.169/24, username: admin, password: admin

Set a static IP 192.168.169.x/24 on your PC, power on the RipEX and wait 25 seconds for the RipEX OS to boot. Connect your PC to RipEXs' ETH interface, start your browser and type https://192.168.169.169 in the address line. When accessing RipEX for the first time, you have to accept the https security certificate issued by Racom.

Before attempting to do any configuration, make sure your RipEX is the only one powered on around. Since all units coming from factory share the same default settings, you could be accessing a different unit over the air without being aware.

When accessing over the optional "X5" USB/ETH adapter, your PC will get its IP settings from the built-in DHCP server and you have to type https://10.9.8.7 in your browser. Remaining steps are equal and you do not need to worry about other RipEX's, you will be connected to the local unit under any circumstances.

SCADA radio network step-by-step

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

1. Design your network to ensure RF signal levels meet system requirements.
2. Calculate and estimate the network throughput and response times when loaded by your application.
3. Perform a bench-test with 3-5 sets of RipEX's and SCADA equipment (Chapter 4, *Bench test*).
4. Design the addressing and routing scheme of the network (Chapter 2, *RipEX in detail* and *RipEX App notes, Routing*[1])
5. Preconfigure all RipEX's (Section 4.4, "Basic setup").
6. Install individual sites

---

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

1. Mount RipEX into cabinet (Section 5.1, "Mounting").
2. Install antenna (Section 5.2, "Antenna mounting").
3. Install feed line (Section 5.3, "Antenna feed line").
4. Ensure proper grounding (Section 5.4, "Grounding").
5. Run cables and plug-in all connectors except from the SCADA equipment (Section 3.2, "Connectors")
6. Apply power supply to RipEX
7. Test radio link quality (Section 4.5, "Functional test").
8. Check routing by the ping tool (Section 6.5.3, "Tools") to verify accessibility of all IP addresses with which the unit will communicate.
9. Connect the SCADA equipment

7. Test your application

1. RipEX – Radio router

1.1. Introduction

RipEX is a best-in-class radio modem, not only in terms of data transfer speed. This Software Defined Radio with Linux OS has been designed with attention to detail, performance and quality. All relevant state-of-the-art concepts have been carefully implemented.

RipEX provides 24x7 reliable service for mission-critical applications like SCADA & Telemetry for Utilities, SmartGrid power networks or transaction networks connecting lottery terminals, POS or ATM's.

Any unit can serve as the central master, repeater, remote terminal, or all of these simultaneously, with a configuration interface easily accessible from a web browser.

Anybody with even basic knowledge of IP networking can set up a RipEX within a matter of minutes and maintain the network quite easily.

1.2. Key Features

- Exceptional data speeds on the radio channel
  - 83 kbps / 25 kHz, 42 kbps / 12.5 kHz, 21 kbps / 6.25 kHz

- 1x ETH, 2x COM, 1x USB
  - Simultaneously on radio channel. COM1-RS232, COM2-RS232 or RS485, software configurable. USB for independent service access via USB/ETH adapter

- 135–175; 290–350; 350–470; 928–960 MHz
  - Software-selectable channel spacing 25, 12.5 or 6.25 kHz

- 10 watts
  - Transmission output control, nine stages from 0.1 to 10 W

- Energy saving
  - Sleep mode - 0.07 VA, controlled via a digital input.
  Save mode - 1.5 VA, wake up by receiving a packet from the radio channel

- Extended temperature range
  -30 to+55 ºC certified, -40 to+70 ºC functional

- Easy to configure and maintain
  - Web interface,
  - Wizards,
  - On-line help,
  - Balloon tips,
  - Fastest web access to remote units

- Bridge or Router
  - RipEX is a device with native IP support which can be set as a standard bridge or router.

- Modbus, IEC101, DNP3, Comli, DF1, Profibus, Modbus TCP, IEC104, etc.
  - Unique implementation of industrial protocols enables a secure addressed transmission of all packets in all directions

- Anti-collision protocol on radio channel
  - Allows multi polling & report-by-exception concurrently for several independent applications sim-ultaneously

- Turbo – 3x higher throughput
  - Optimisation method which joins short packets, compresses data, optimises both the traffic to the link peer and the sharing of the radio channel capacity among the links.

- Embedded diagnostic & NMS
  - Real time and historical (20 periods, e.g. days) statistics and graphs for the unit and its neighbours.
  - SNMP including generation of TRAP alarms when preset thresholds are exceeded

- 256 AES encryption
  - The most secure encryption meets FIPS 140 2 requirements

- Pay only for what you need
  - Software authorisation keys allow you to add advanced features when needed

- Reliability
  - 3 years warranty, rugged die cast aluminium case, military or industrial components
  - Every single unit tested in a climatic chamber as well as in real traffic

1.3. Standards

Radio	ETSI EN 300 113-2 V 1.4.2
	ETSI EN 302 561 V1.2.1
	FCC part 90
EMC	ETSI EN 301 489-1 V 1.8.1
	ETSI EN 301 489-5 V 1.3.1
Safety	CENELEC EN 60 950-1:2006
Vibration	CENELEC EN 61 373:1999
ETH	IEEE 802.3i
	IEEE 802.3u
	IEEE 802.3af
RS232	EIA-232-F
RS485	EIA RS-485
IEC101	IEC 60870-5-101
IEC104	IEC 60870-5-104
DNP3	IEEE 1815-2010
Profibus DP-V0	IEC 61158 Type 3

2. RipEX in detail

2.1. Modes of operation

Radio modem RipEX is best suited for transmission of a large number of short messages where a guaranteed delivery time is required, i.e. for mission critical applications.

RipEX has the following basic uses:

- Polling

  In poll-response networks a central master unit communicates with a number of remote radiomodems one at a time. The master unit exchanges data with the currently connected remote radio, and when finished, it establishes a new connection with the next remote radio according to the polling order.

- Report-by-exception

  In report-by-exception networks remote units can be contacted similarly to polling networks. In addition, any remote unit can spontaneously send data to the master unit (typically an alarm).

- Mesh

  In mesh type networks any radio modem in the network can access any other radio modem randomly and spontaneously. Mesh network can also host polling or report-by-exception applications, even in several instances.

2.2. Bridge mode

A packet received through any interface is broadcast to the appropriate interfaces of all units within the network. Packets received on COM are broadcast to both COM1 and COM2 at remote sites, allowing you to connect 2 RTU's to any radio modem.

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

Beside standard packet termination by an "Idle" period on the serial port (a pause between received bytes) the bridge mode also offers "streaming". While in streaming mode, transmission on the radio channel starts immediately, without waiting for the end of the received frame on COM => zero latency.

The bridge mode is suitable for all polling applications.

2.2.1. Detailed Description

Bridge mode is suitable for Point-to-Multipoint networks, where Master-Slave applications with polling-type communication protocol are used. RipEX in bridge mode is as easy to use as a simple transparent device, while providing communication reliability and spectrum efficiency by employing a sophisticated protocol in the radio channel.

In bridge mode, the radio channel protocol do not solve collisions. There is a CRC check of data integrity, however, 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 the radio channel.

ETH - The whole network of RipEX radiomodems behaves as a standard ethernet network bridge. Each ETH interface automatically learns which devices (MAC addresses) are located in the local LAN and which devices are accessible over the radio channel. Consequently, only the ethernet frames addressed to remote devices are physically transmitted on the radio channel. This arrangement saves the precious RF spectrum from extra load which would be otherwise generated by local traffic in the LAN (the LAN to which the respective ETH interface is connected).

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

There is a special parameter TX delay (*Adv. Config., Device*), which should be used when all substations (RTU's) reply to a broadcast query from the master station. In such case massive collisions would ensue because all substations (RTU's) would reply at nearly the same time. To prevent such 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.

2.2.2. Functionality example

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

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

The single digits in illustrations are "site names" and do not necessarily correspond with actual addresses of both the RipEX's and SCADA equipment. Address configuration examples are given in the *next chapter*.
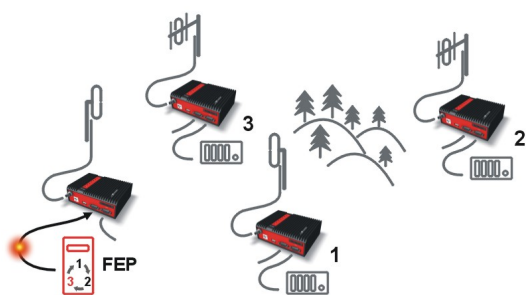
Step 1

Polling cycle starts:
FEP sends a request packet for RTU3 through COM1 to the connected RipEX.
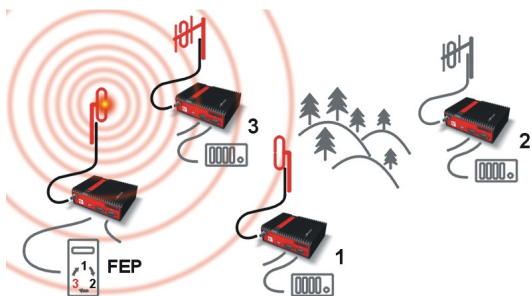
Step 2

FEP's RipEX broadcasts this packet on Radio channel. RipEX3 and RipEX1 receive this packet.
RipEX2 doesn't receive this packet, because it is not within radio coverage of FEP's RipEX.
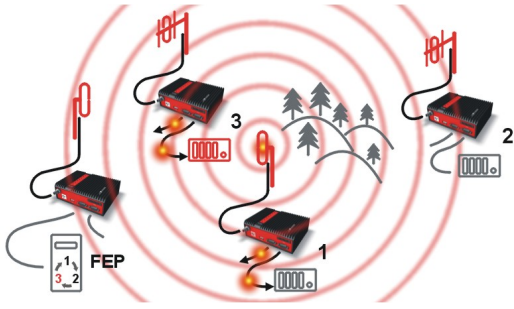
Step 3

RipEX3 and RipEX1 send the received packet to their COM1 and COM2.
Packet is addressed to RTU3, so only RTU3 responds.
RipEX1 is set as a repeater, so it retransmits the packet on Radio channel. Packet is received by all RipEXes.
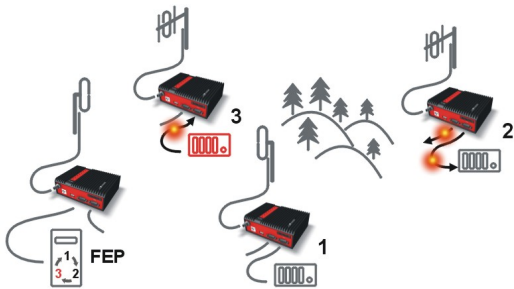
Step 4

RipEX2 sends repeated packet to its COM1 and COM2.
RTU2 doesn't react, because the packet is addressed to RTU3.
RipEX3 and FEP's RipEX **do not** send the repeated packet to their COM ports, because it has already been sent (RipEX3) or received (FEP's RipEX) on their COM (anti-duplication mechanism).
RTU3 sends the reply packet.
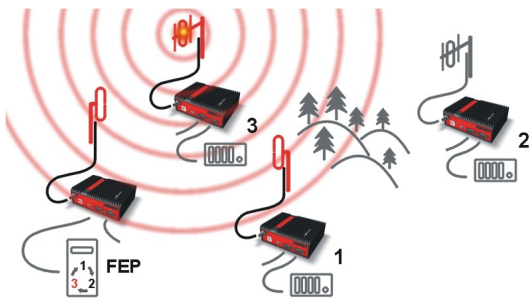
Step 5

RipEX3 broadcasts the reply packet from RTU3 on Radio channel.
Packet is received by RipEX1 and FEP's RipEX.
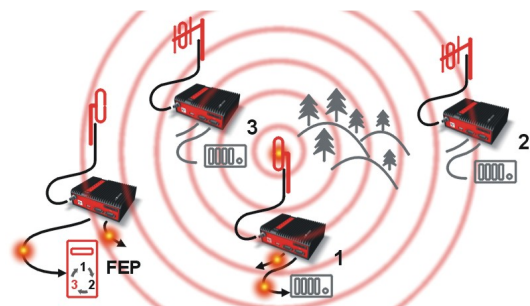
Step 6

FEP's RipEX sends the packet (the reply from RTU3) to FEP through COM1.
RipEX1 sends this packet to RTU1. RTU1 doesn't react, because the packet is addressed to FEP.
RipEX1 repeats the packet on Radio channel.
All RipEXes receive the packet.
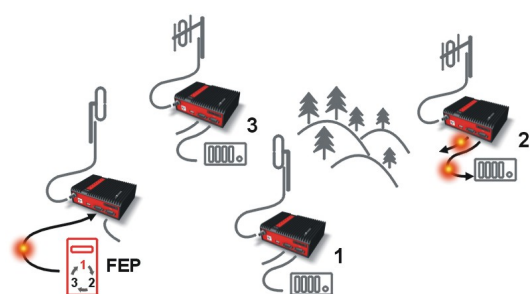
Step 7

RipEX2 sends repeated packet to its COM1 and COM2.
RTU2 doesn't react, because the packet is addressed to FEP.
RipEX3 and FEP's RipEXes **do not** send the repeated packet to their COM ports, because it has been handled already.
FEP processes the reply from RTU3 and polling cycle continues…..

2.2.3. Configuration examples

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

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

192.168.5.13/24 **3**

192.168.5.3/24

192.168.5.12/24 **2**

192.168.5.2/24

192.168.5.51/24 **50**

192.168.5.50/24 **FEP**

REPEATER

192.168.5.11/24 **1**

192.168.5.1/24
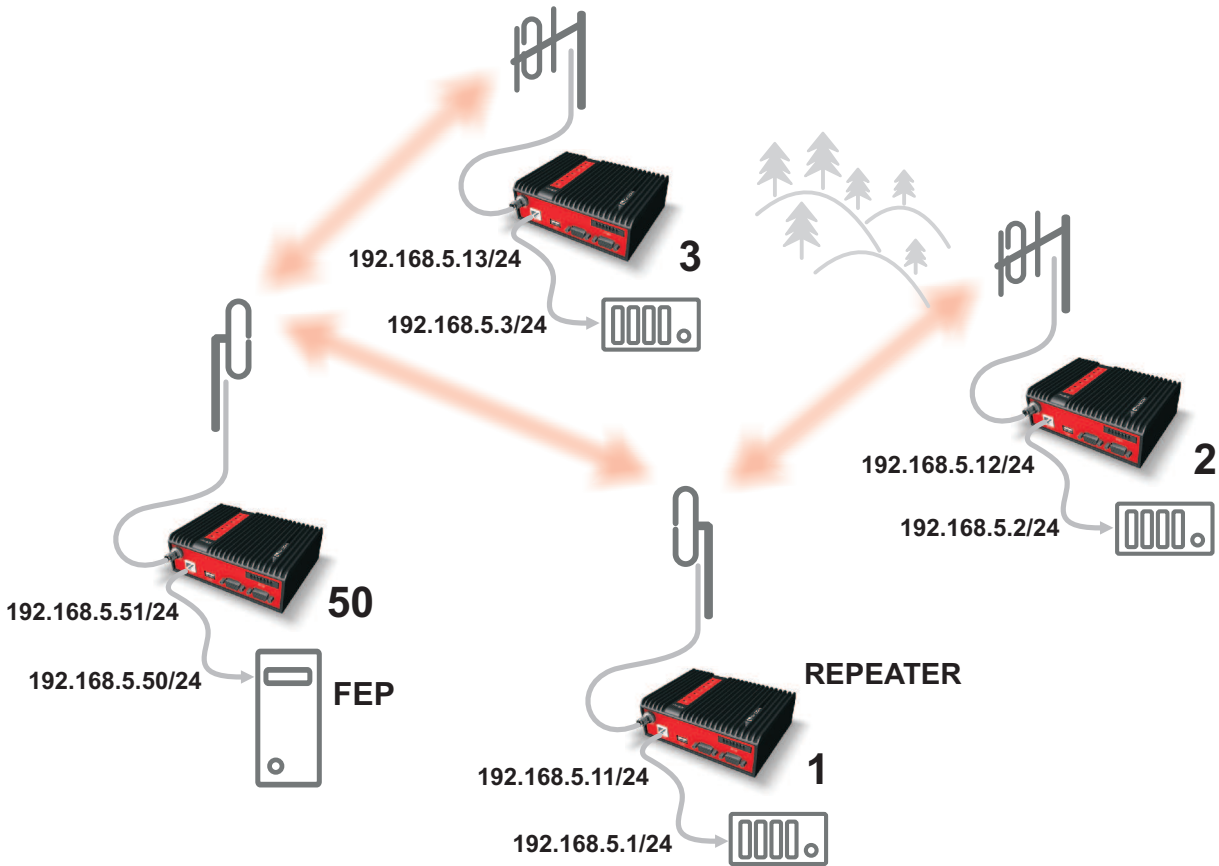
Fig. 2.1: Bridge mode example

Repeater

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

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

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

Examples:

1. Repeaters connected serially
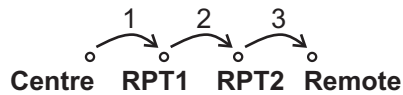
A packet is transmitted and repeated in steps 1, 2, 3.
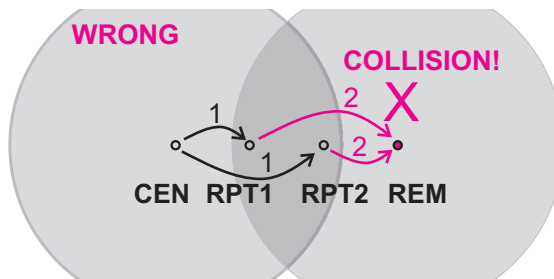
In improperly designed networks collisions happen if aremote radio modem lies in the range of two repeaters (see the image): the packet sent from the centre (1) is received by both repeaters. It is repeated by them both (2) causing a collision at the remote. In other words – there should not be more than one repeater where the centre and remotes' coverage areas overlap.
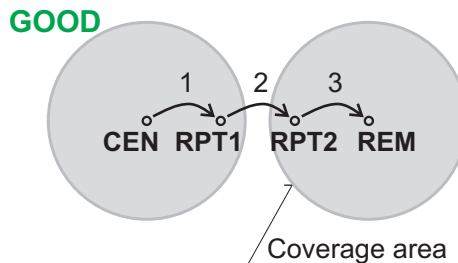
Solution 1.
Adjust signal coverage so that RPT2 is out of range of the centre and RPT1 is out of the range of the remote radio modem. This can be achieved for example by reducing the output power or using a unidirectional antenna.
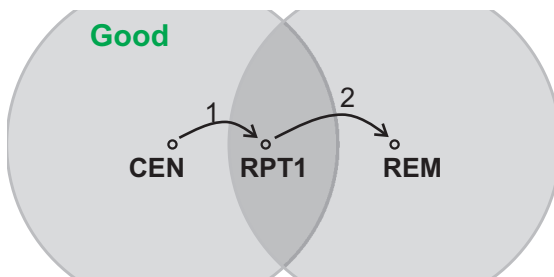
Solution 2.
Use a single repeater. (Whenever network layout allows that.)

2. Parallel repeaters
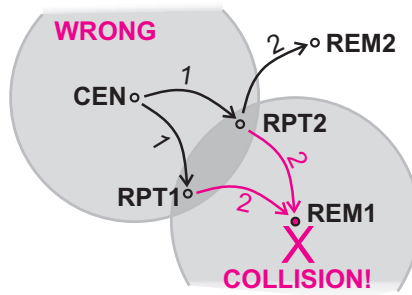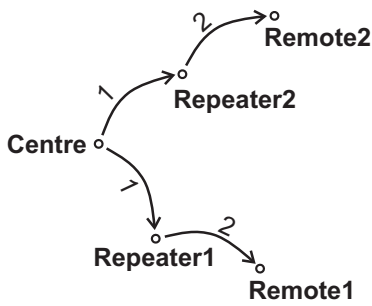
Improperly designed network:

- RipEX REM1 is within the range of two repeaters (RPT1 and RPT2). The repeaters receive a packet (1) from the centre (CEN) and repeat it at the same time (2) causing a collision at REM1.
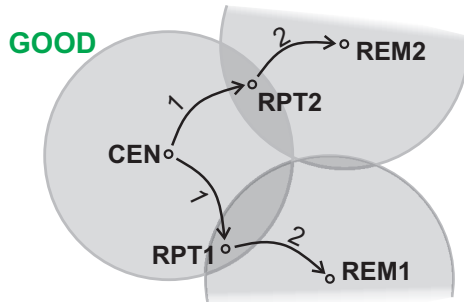
Well-designed network:

- A remote is only in the range of a single repeater (REM1-RPT1, REM2-RPT2).
There is always only one repeater where the centre and remote coverage areas overlap.

2.3. Router mode

RipEX works as a standard IP router with two interfaces (radio and ethernet) and two COM port devices. There is a sophisticated anti-collision protocol on the radio channel, which checks and verifies every single packet. Being an IP router, each unit can simultaneously work as a store-and-forward repeater and deliver packets to the connected equipment.

The router mode is suitable for all uses. In contrast to the bridge mode, a packet reception is confirmed over the radio channel even in very simple polling type applications, and if necessary the packet is retransmitted.

2.3.1. Detailed Description

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, retransmissions and CRC checks 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 its own MAC address, IP address and mask.

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

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

2.3.2. Functionality example

In the following example, there are two independent SCADA devices connected to RipEX's two COM ports. One is designated RTU (Remote Telemetry Unit) and is assumed to be polled from the centre by the FEP (Front End Processor). The other is labelled PLC (Programmable Logic Controller) and is assumed to communicate spontaneously with arbitrary chosen peer PLCs.
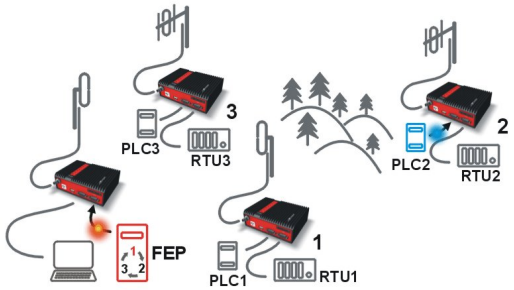
Step 1

FEP sends a request packet for RTU1 through COM2 to its connected RipEX.
Simultaneously PLC2 sends a packet for PLC1 to RipEX2 through COM1.
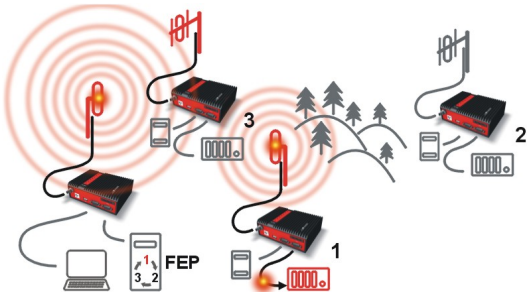
Step 2

FEP's RipEX transmits an addressed packet for RTU1 on Radio channel.
RipEX1 receives this packet, checks data integrity and transmits the acknowledgement.
At the same time packet is sent to RTU1 through COM2.
RipEX3 receives this packet too. It doesn't react, because this packet is directed to RipEX1 only.
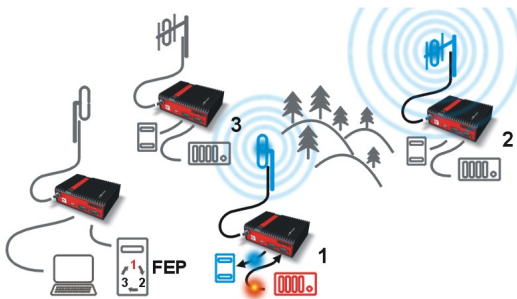
Step 3

RipEX2 waits till previous transaction on Radio channel is finished (anti-collision mechanism).
Then RipEX2 transmits on Radio channel the addressed packet for PLC1.
RipEX1 receives this packet, checks data integrity and transmits acknowledgement.
At the same time packet is sent to PLC1 through COM1.
Simultaneously the reply packet from RTU1 for FEP is received on COM2.
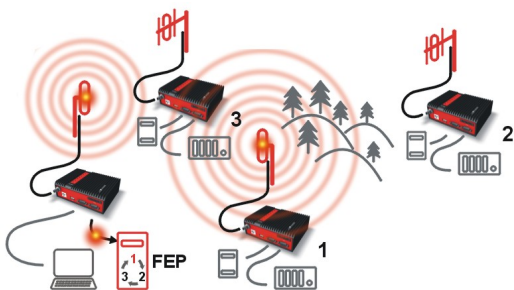
Step 4

RipEX1 transmitts the reply packet from RTU1 for FEP on Radio channel.
All RipEXes receive this packet. This packet is addressed to FEP's RipEX, so only FEP's RipEX reacts. It checks data integrity and transmits the acknowledgement to RipEX1.
At the same time the packet is sent to FEP through COM2.
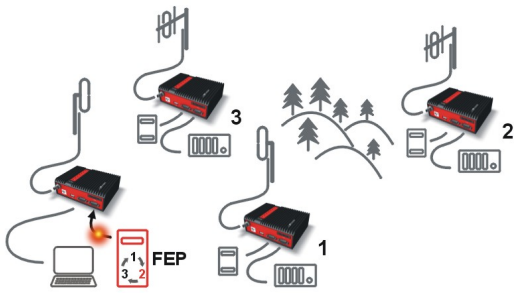
Step 5

FEP receives the response from RTU1 and polling cycle continues…

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

2.3.3. Configuration examples

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

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

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

Note

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

Example:
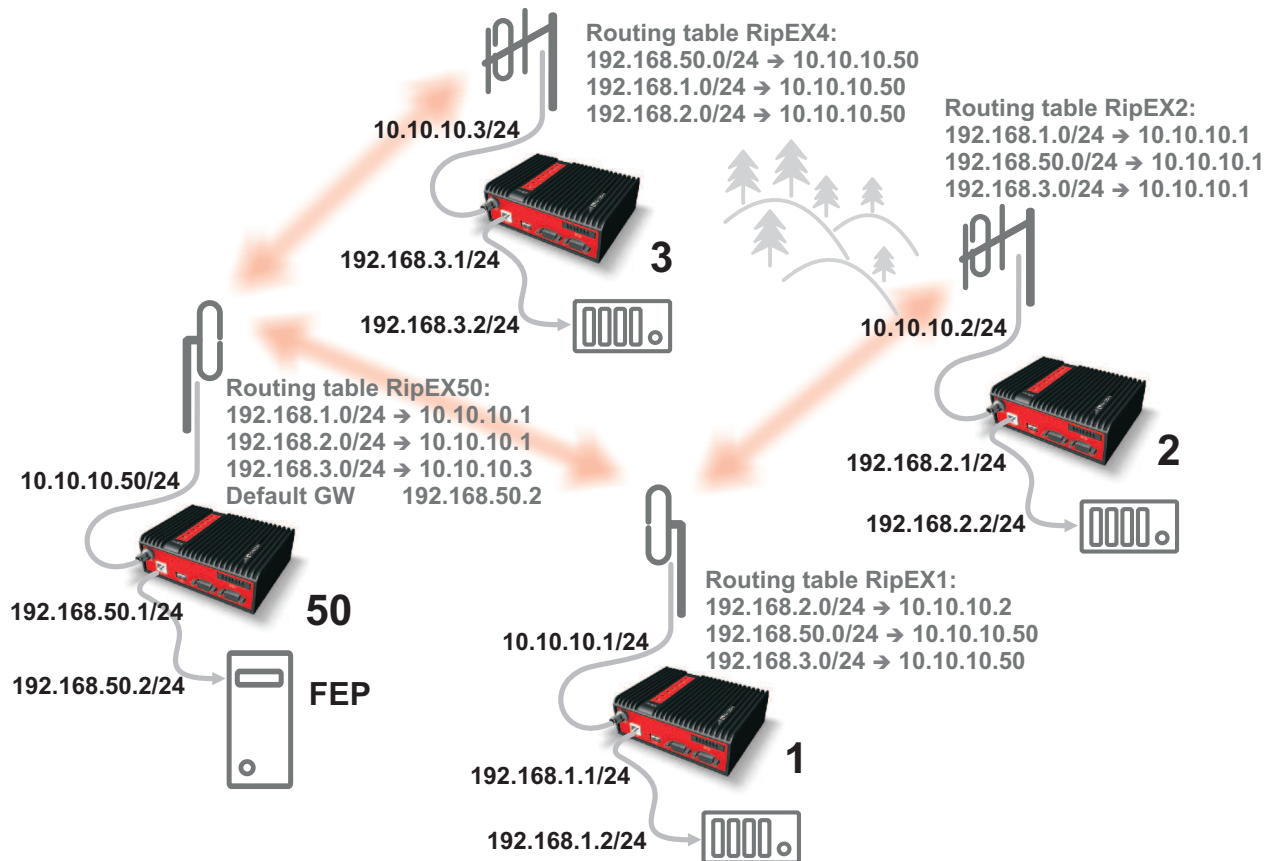
Fig. 2.2: Addressing

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

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

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

2.3.4. Addressing hints

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

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

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

Routing table RipEX4:
192.168.0.0/16 ➔ 10.10.10.50

10.10.10.4/24

Routing table RipEX2:
192.168.0.0/16 ➔ 10.10.10.1

192.168.4.1/24   3

192.168.4.2/24

10.10.10.2/24

Routing table RipEX50:
192.168.0.0/22 ➔ 10.10.10.1
192.168.4.0/22 ➔ 10.10.10.4
Default GW   192.168.50.2

192.168.2.1/24   2

10.10.10.50/24

192.168.2.2/24

192.168.50.1/24   50

Routing table RipEX1:
192.168.2.0/24 ➔ 10.10.10.2
192.168.0.0/16 ➔ 10.10.10.50

10.10.10.1/24

192.168.50.2/24   FEP

192.168.1.1/24   1

192.168.1.2/24

Fig. 2.3: Optimised addressing

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

2.4. Serial SCADA protocols

Even when the SCADA devices are connected via serial port, communication remains secured and address-based in all directions (centre-RTU, RTU-centre, RTU-RTU).

In router mode, RipEX utilises a unique implementation of various SCADA protocols (Modbus, IEC101, DNP3, Comli, DF1, Profibus). In this implementation SCADA protocol addresses are mapped to RipEX addresses and individual packets are transmitted as acknowledged unicasts. Polled remote units respond to the unit that contacted them (multi master network possible) using secure packets. When needed, RTU-RTU parallel communication is also possible.

2.4.1. Detailed Description

Each SCADA protocol, such as Modbus, DNP3, IEC101, DF1, etc., has its own unique message format, and more importantly, its unique way of addressing remote units. The basic task for protocol utility is to check whether a received frame is in the correct protocol format and uncorrupted. Most of the SCADA protocols use 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 environment, so the basic task for the protocol interface utility is to convert SCADA serial packets to UDP datagrams. Address translation settings are used to define the destination IP address and UDP port. Then these UDP datagrams are sent to RipEX router, processed and typically forwarded as unicasts over the radio channel to their destination. If 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), the datagram is again forwarded according to the routing table.

Note: UDP datagrams can be acknowledged on the radio channel (ACK parameter of router mode) but they are not acknowledged on the ethernet channel.

When a 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. Either it is delivered to COM1(2) port daemon, where the datagram is decapsulated and the data received on serial interface of the source unit is forwarded to COM1(2), or the UDP port is that of a Terminal server or any other special protocol daemon on Ethernet like Modbus TCP etc. Then the datagram is processed by that daemon accordingly to the respective settings.

RipEX uses a unique, sophisticated protocol on the radio channel. It guaranties data integrity even under heavy interference or weak signal conditions due to the 32 bit CRC used, minimises the likelihood of a collision and retransmits frames when collision happens, 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: The anti-collision protocol feature is available only in the router mode. The bridge mode is suitable for simple Master-Slave arrangements with polling-type application protocol.

2.5. Combination of IP and serial communication

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

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

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

RipEX also provides a built-in converter Modus RTU – Modus TCP, where data structure is not the same, so one application may combine both protocols, Modus RTU and Modus TCP.

2.5.1. Detailed Description

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

Examples of the use:

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

- There is no hardware serial interface on the computer

- Serial cable between RipEX and computer would be too long. E.g. the RipEX is installed very close to the antenna to reduce feed line loss.

- LAN already exists between the computer and the point of installation

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

In special cases, the terminal server can reduce network load from TCP applications . A TCP session can be terminated locally at the terminal server in RipEX, user data extracted from the TCP messages and processed as if it came from a COM port. When the data reaches the destination RipEX, it can be transferred to the RTU either via the serial interface or via TCP (UDP), using the terminal server again.

2.6. Diagnostics & network management

RipEX radiomodem offers a wide range of built-in diagnostics and network management tools.

2.6.1. Logs

There are 'Neighbours' and Statistic logs in RipEX. 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 the Log save period).

Neighbours

The 'Neighbours' log provides information about neighbouring units (RipEX's which can be accessed directly over the radio channel, i.e. without a repeater). Every RipEX on the network regularly broadcasts its status, the set of so called "Watched values": the probability of packet loss when transmitting data over the radio channel, current supply voltage, internal temperature, measured RF output power, the Voltage Standing Wave Ratio on the antenna feed line and the total number of packets received from / transmitted to ETH, COM1, COM2 interfaces. In addition, the RipEX that records this data in its log

also keeps track of how many times it listened to its neighbouring unit as well as of the RSS and DQ recorded. See *Adv. Conf., Diagnostic* for more.

Statistic

The 'Statistic' log provides information about the volume of data traffic on all interfaces: radio, ETH, COM1, COM2. It offers detailed information about the number of transmitted packets, their size and the throughput per second. Moreover, a detailed division into user and service packets is available for the radio channel. See chapter *Adv. Conf., Diagnostic* for more.

2.6.2. Graphs

An independent database periodically stores the Watched values (see 'Neighbours' log above) from up to five neighbouring RipEX's and from the local one, there including most important values from the Statistic log. All these values can be displayed as graphs.

The graphs are available in summary and detailed versions. Detailed logging is triggered on when a threshold value has been reached for the specific item to enable a more detailed investigation into the units' operation when an alarm event occurs. Each graph can display two different elements at once, including their set thresholds. Each of the values may originate from a different RipEX unit.

See chapter *Adv. Conf., Graphs* for more.

2.6.3. SNMP

RipEX implements an SNMP client ver. 1. The values provided by RipEX are shown in the MIB table. RipEX also allows generating SNMP traps when thresholds have been reached for the monitored values: RSScom, DQcom, TXLost[%], Ucc, Temp, PWR, VSWR, ETH[Rx/Tx], COM1[Rx/Tx], COM2[Rx/Tx], HW Alarm Input.

See chapter *RipEX App notes, SNMP for RACOM RipEX*[1] for more.

2.6.4. Ping

To diagnose the individual radio links RipEX is equipped with an enhanced Ping tool. In addition to the standard info such as the number of sent and received packets or the round trip time, it provides the overall load, the resulting throughput, BER, PER and specific data about the quality of the radio transmission, RSS and DQ for the weakest radio link on the route.

2.7. Firmware update and upgrade

Occasionally RipEX firmware update or upgrade is released. An update improves functionality and/or fix software bugs. Updates can be downloaded for free from www.racom.eu.

A firmware upgrade implements significant improvements and new functions which take the product to a new level. Downloading and applying a firmware upgrade is the same as with firmware update. However a software key may have to be purchased and applied to activate the new functionality or the upgrade itself (see the next chapter).

---

[1] http://www.racom.eu/eng/products/m/ripex-an/snmp.html

2.8. Software feature keys

Certain advanced RipEX features are activated with software keys. Among such code protected features are the *Router mode, High speed, COM2, 10 W*. This enables the users to initially purchase only the functionality they require and buy additional functions as the requirements and expectations grow. This protects 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.

Software keys are always tied to a specific RipEX production code. When purchasing a software key, this production code must be given.

Network Planning

This chapter has not been completed yet.

3. Product

RipEX is built into a rugged die-cast aluminium casing that allows for multiple installation possibilities, see Section 5.1, "Mounting".

3.1. Dimensions
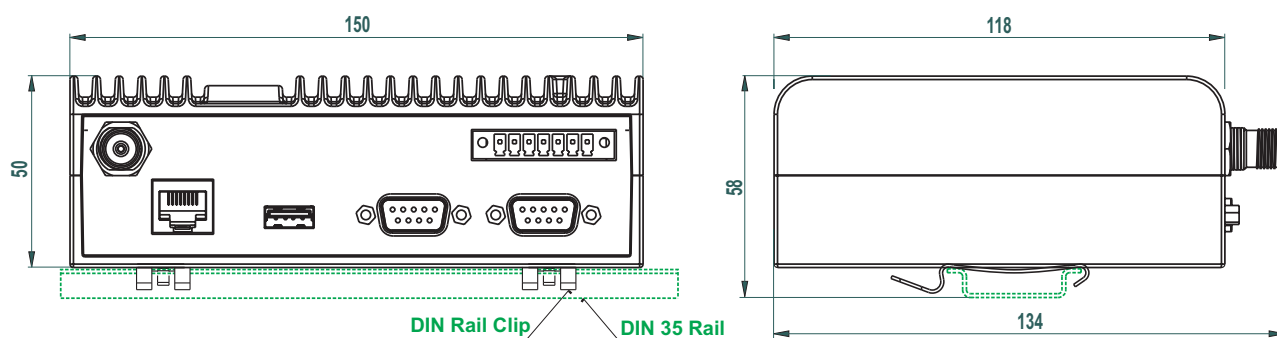
Fig. 3.1: RipEX dimensions, see more
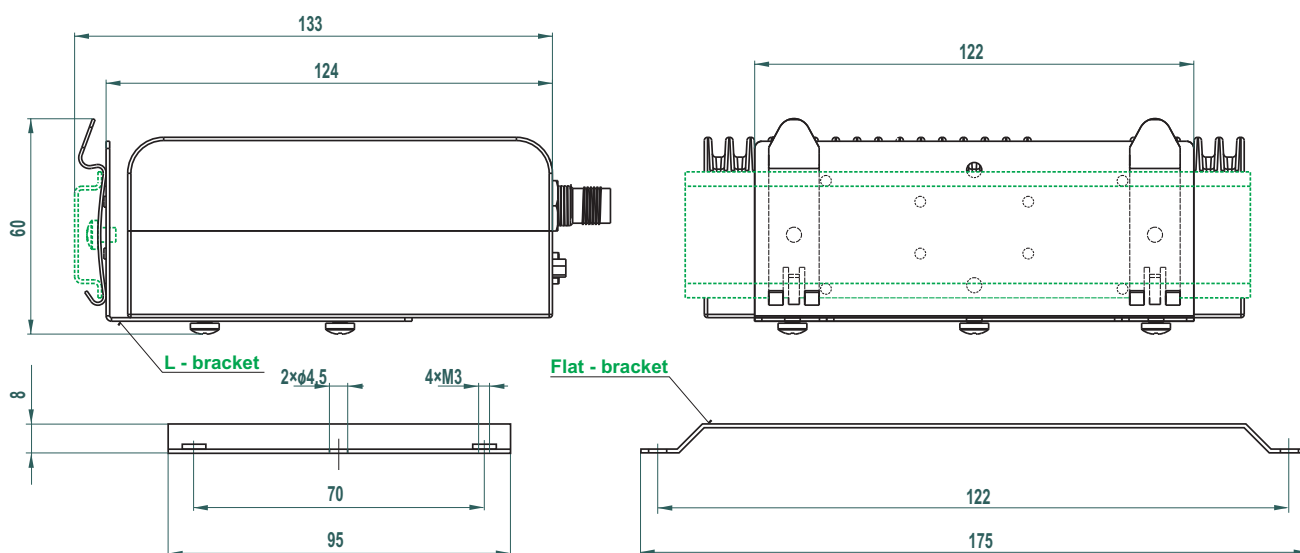
Fig. 3.2: L-bracket and Flat-bracket, see more

3.2. Connectors

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

ANTENNA

ETH/USB ADAPTER

**ETH data equipment, RTU
LAN, control PC**

COM1

COM2 data equipment, RTU

+ –
ALARM OUT.
ALARM INPUT
SLEEP - WAKE UP
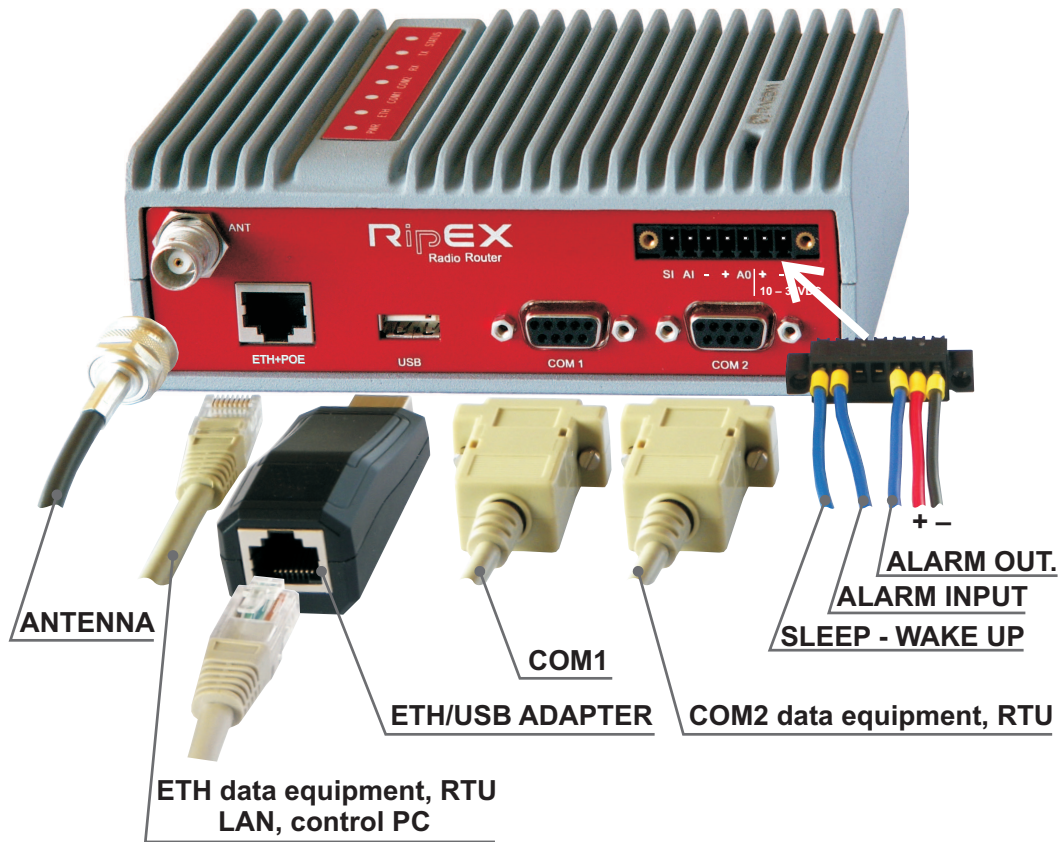
Fig. 3.3: Connectors

3.2.1. Antenna

An antenna can connect to RipEX via TNC female 50 ohm connector.

A model with two antenna connectors can be supplied to order, in which the Rx and Tx antennas are separate. See chapter Section 3.5, "Model offerings".

Fig. 3.4: Antenna connector TNC

Fig. 3.5: Separated Rx and TX antennas

Warning: RipEX radio modem may be damaged when operated without an antenna or a dummy load.

3.2.2. Power and Control

This connector connects to a power supply (if the RipEX isn't PoE powered) and it contains control signals. A Plug with screw-terminals and retaining screws for power and control connector is supplied with each RipEX. It is Tyco 7 pin terminal block plug, part No. 1776192-7, contact pitch 3,81 mm. The connector is designed for electric wires with a cross section of 0.5 to 1.5 mm^2. Strip the wire leads to 6 mm (1/4 inch). Isolated cables should receive PKC 108 or less end sleeves before they are inserted in the clip. Insert the cables in the wire ports, tightening securely.

Tab. 3.1: Pin assignement

pin	labeled	signal
1	SI	SLEEP IN
2	AI	ALARM IN
3	-	- (GND) – for SLEEP IN, ALARM IN
4	+	+ (PWR) – for ALARM OUT
5	AO	ALARM OUT
6	+ 10-30VDC	+ PWR (10 to 30 V)
7	- 10-30VDC	- PWR (GND)

Pins 3 and 7, 4 and 6 are connected internally.
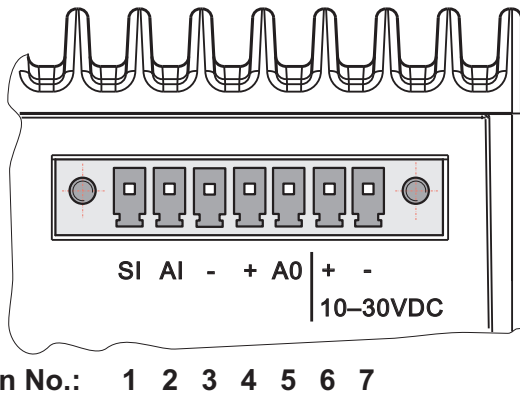
Fig. 3.6: Supply connector
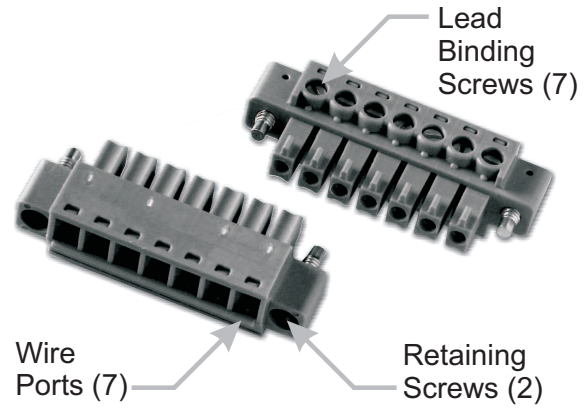
Fig. 3.7: Power and Control - cable plug

SLEEP IN

SLEEP IN is the digital input for activating the Sleep mode. When this pin is grounded (for example when connected to pin 3), the RipEX switches into the Sleep mode. Using Power management (*Advanced Config.*), the Entering the Sleep mode can be delayed by a set time. Disconnecting SLEEP IN from GND (-) ends the Sleep mode. Note that RipEX takes 25 seconds to wake up from the Sleep mode.
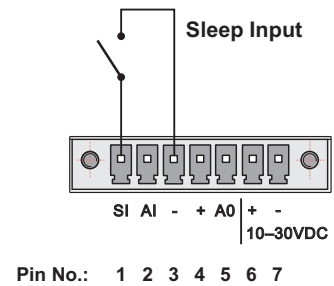
ALARM IN

ALARM IN is a digital input. If grounded (e.g. by connecting to PIN 3), an external alarm is triggered. This alarm can be used for example to transmit information using SNMP trap, informing for instance about a power outage or RTU problem. For details about Alarm management see chapter *Advanced Configuration*.
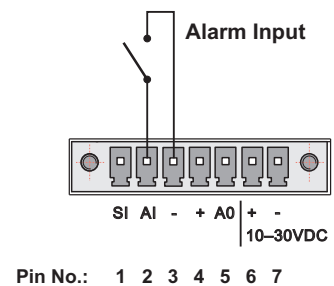
ALARM OUT

ALARM OUT is a digital output. It can be activated in Alarm management settings, chapter *Advanced Configuration*. It may be used for instance to switch on the Fan kit if the preset maximum internal temperature is exceeded or to inform the connected RTU about a RipEX alarm. If an alarm is triggered, ALARM OUT is internally connected to GND. If the external device requires connection to positive terminal of the power supply, PIN 4 should be used.
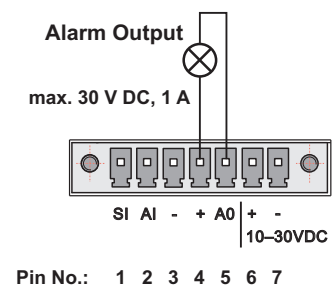
PWR

The PWR pins labelled + and - serve to connect a power supply 10 – 30 VDC. The requirements for a power supply are defined in Section 5.6, "Power supply" and Section 3.4, "Technical specification".

3.2.3. ETH + PoE

Standard RJ45 connector for ethernet connection. RipEX has 10/100 BaseT Auto MDI/MDIX interface so it can connect to 10 Mbps or 100 Mbps ethernet network. The speed can be selected manually or recognised automatically by RipEX. RipEX is provided with Auto MDI/MDIX function which allows it to connect over both standard and cross cables, adapting itself automatically.

This connector enables also powering RipEX over PoE (Power over Ethernet) supply according to the standard IEEE802.3af. When a RipEX is powered over PoE, its output is limited to 1 W, because of the IEEE802.3af standard power limitations. You can also use a passive PoE injector for PoE supply.

PoE - pin assignement

Tab. 3.2: Ethernet to cable connector connections

PIN	Signal	Direct cable	Crossed cable
1	TX+	orange - white	green - white
2	TX-	orange	green
3	RX+	green - white	orange - white
4	PoE+	blue	blue
5	PoE+	blue - white	blue -white
6	Rx-	green	orange
7	PoE-	brown - white	brown - white
8	PoE-	brown	brown
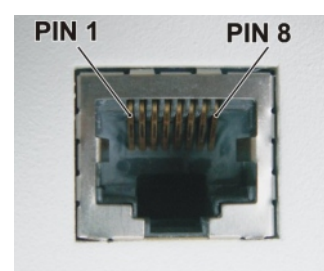
Fig. 3.8: RJ-45F

PoE – via Ethernet connector RJ-45 using PoE standard IEEE802.3af. Voltage 36-57 V. Common version of supplying:

Power supply connection:

- plus to pins 4+5
- minus to pins 7+8

Power supply polarity can be reversed

3.2.4. COM1 and COM2

RipEX provides two serial interfaces COM1 and COM2 terminated by DSUB9F connectors. COM1 is always RS232, COM2 can be configured as RS232 or RS485 (more in *Adv. Conf., COM's*).

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

Tab. 3.3: COM1,2 pin description

DSUB9F	COM1, 2 – RS232		COM2 – RS485	
pin	signal	In/ Out	signal	In/ Out
1	CD	O	—	
2	RxD	O	line B	I/O
3	TxD	I	line A	I/O
4	DTR	I	—	
5	GND		GND	
6	DSR	O	—	
7	RTS	I	—	
8	CTS	O	—	
9	—	—	—	

Fig. 3.9: Serial connector

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

3.2.5. USB

RipEX uses USB 1.1, Host A interface. USB interface is wired as standard:

Tab. 3.4: USB pin description

USB pin	signal	wire
1	+5 V	red
2	Data(-)	white
3	Data (+)	green
4	GND zem.	black
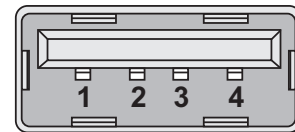
Fig. 3.10: Serial connector

The USB interface is designed for the connection to the "X5" – external ETH/USB adapter. The "X5" is an optional accessory to RipEX, for more see Section 4.3, "Connecting RipEX to a programming PC". The adapter is used for service access to RipEX's web configuration interface.

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

3.2.6. Reset button

RipEX's bottom-side enclosure includes a reset button accessible through an opening. When this button is pressed, the STATUS diode on the LED panel goes dark (indicating that the button has been pressed). If you hold the button for 5 seconds, the STATUS diode starts flashing slowly indicating that the reset is complete. If you continue to hold the button for 15 or more seconds (the STATUS diode starts flashing quickly) and then release it, you will reset the device's access information to default: parameters such as the login, password and ethernet IP will be reset to their defaults. Resetting access parameters to defaults results also in clearing all firewall rules (which may have been blocking the access by accident). Remember to re-install your firewall if you are using one.

Fig. 3.11: Reset

Note

To reset the RipEX only use the RESET button as described above or use the button in RipEX's web configuration, see *Adv. Conf., Maintenance*. Never use a power cycle (disconnecting and reconnecting power supply) to reset it. While power cycle resets, or rather reboots the RipEX, its software will not terminate correctly resulting in logs, statistics and graphs not saved properly.

3.2.7. GPS

RipEX can be equipped with an internal GPS, see Section 3.5, "Model offerings". The GPS module is used for time synchronisation of the NTP server inside RipEX. See *Adv. Conf., Time* for more. In this case the front panel contains a SMA female 50 ohm connector for connecting the GPS antenna.

Fig. 3.12: GPS Connector SMA

3.3. Indication LEDs

Fig. 3.13: Indication LEDs

Tab. 3.5: Key to LEDs

	Color	Description
STATUS	Green	The RipEX OS (Linux) is running succesfuly
	Dark	Reset button has been pressed
	Green flashes slowly	reset after five-seconds pressing the Reset button
	Green flashes quickly	default access after 15-seconds pressing the Reset button
	Red	Status alarm
TX	Red	transmitting to radio channel
RX	Green	receiver is synchronised to a packet
	Yellow	there is a signal stronger than -80 dBm on Radio channel
COM2	Green	data receiving
	Yellow	data transmitting
COM1	Green	data receiving
	Yellow	data transmitting
ETH	Yellow ON	100 Mb/s speed
	Yellow OFF	10 Mb/s speed
	Green ON	connected
	Green flashes	ethernet data
PWR	Green	powered succesfuly
	Blinks with a period of 1 sec	Save mode
	Flashes once per 3 sec	Sleep mode

3.4. Technical specification

Tab. 3.6: Technical parameters

Radio parameters	
Frequency bands	135–175*; 300–370*; 370–470; 928–960* MHz
Channel spacing	6.25 / 12.5 / 25 kHz
Frequency stability	+/- 1.0 ppm
Modulation	16DEQAM, D8PSK, π/4DQPSK, 4CPFSK, 2CPFSK Detail
RF Data rate	max. 83.33 kbps / 25 kHz
	max. 41.66 kbps / 12.5 kHz
	max. 20.83 kbps / 6.25 kHz Detail
FEC (Forward Error Correction)	On/Off, 3/4 Trellis code with Viterbi soft-decoder
Transmitter	
Carrier Output power	0.1 to 10W programmable
	0.1 - 0.2 - 0.5 - 1.0 - 2.0 - 3.0 - 4.0 - 5.0 - 10 W
	(0.1 to 2W for > 42kbps/25 kHz)
	(0.1 - 1W for PoE supply)
Duty cycle	Continuous
Rx to Tx Time	< 1.5 ms
Intermodulation Attenuation	> 40 dB
Spurious Emissions (Conducted)	< -36 dB
Radiated Spurious Emissions	ETSI EN 300113
Adjacent channel power	< -60 dBc
Transient adjacent channel power	< -60 dBc
Receiver	
Sensitivity	Detail
Blocking	> 84 dB
Anti-aliasing Selectivity	50 kHz @ -3dB BW
Tx to Rx Time	< 1.5 ms
Maximum Receiver Input Power	20 dBm (100 mW)
Rx Spurious Emissions (Conducted)	< -56 dBm
Adjancent selectivity	Detail
Co-channel rejection	Detail
Intermodulation response rejection	Detail
Blocking or desensitization	Detail
Spurious response rejection	> 70 dB

Electrical

Primary power		10 to 30 VDC, negative GND	
		or PoE (36 - 57 V, IEEE802.3af standard)	
Rx		5 VA (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 Watts	
	1 W	1.1 A / 13.8 V; 0.6 A/ 24V; 15 Watts	
	5 W	2.4 A / 13.8 V; 1.3 A/ 24V; 33 Watts	
	10 W	3.0 A / 13.8 V; 1.6 A/ 24V; 42 Watts	
Tx 16DEQAM, D8PSK, π/4DQPSK	0.1 W	2.2 A / 13.8 V; 1.25 A/ 24V; 30 Watts	
	1 W	2.2 A / 13.8 V; 1.25 A/ 24V; 30 Watts	
	2 W	2.2 A / 13.8 V; 1.25 A/ 24V; 30 Watts	
Sleep mode		5 mA / 13.8 V; 3 mA / 24 V; 0.07 Watts	
Save mode		120 mA / 13.8 V; 70 mA / 24 V; 1.5 Watts	

Interfaces

Ethernet	10/100 Base-T Auto MDI/MDIX	RJ45
COM 1	RS232	DB9F
	300 - 230 400 bps	
COM 2	RS232/RS485 SW configurable	DB9F
	300 - 230 400 bps	
USB	USB 1.1	Host A
Antenna	50 Ohms	TNC female

LED panel

7x tri-color status LEDs	Power, ETH, COM1, COM2, Rx, Tx, Status

Enviromental

Operating temperature	-25 to +55 °C (-13 to +131 °F) certified
	-40 to +70 °C (-40 to +158 °F) functional
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 x 150 W x 118 mm D (1.97 x 5.9 x 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 3x 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 300 113-1 V1.6.2 (2009-11)
	ETSI EN 302 561 V1.2.1 (2009-12)
	ETSI EN 301 166-1 V1.3.2 (2009-11)
	FCC Part 90
EMC (electromagnetic compatibility)	ETSI EN 301 489-1 V 1.8.1 (2008-04)
	ETSI EN 301 489-5 V 1.3.1 (2002-08)
Electrical Safety	EN 60950-1 ed.2 : 2006

* not available yet

Channel spacing 25 kHz
Exponential modulation | Symbol rate 10.42 kBaud || CE + FCC

ACS – Adjacent channel selectivity
IMRR – Intermodulation response rejection
BD – Blocking or desensivitation

Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard			Sensitivity			Co-channel rejection		ACS *	IMRR	BD
				EN 300 113	EN 302 561	FCC part 90	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degrad.	12dB degrad.	3dB degrad.	3dB degrad.	3dB degrad.
[-]	[-]	[kBaud]	[kbit/s]				[dBm]	[dBm]	[dBm]	[dB]	[dB]	[dB]	[dB]	[dB]
2CPFSK	0,75	10,42	7,81	Comply	Comply LBT	Comply	-118	-115	-111	-7	-4	61	74	91
2CPFSK	1,00	10,42	10,42	Comply	Comply LBT	Comply	-117	-114	-110	-8	-5	60	73	89
4CPFSK	0,75	10,42	15,63	Comply	Comply LBT	Comply	-115	-112	-107	-12	-9	57	71	86
4CPFSK	1,00	10,42	20,83	Comply	Comply LBT	Comply	-113	-110	-104	-13	-10	55	70	84

Channel spacing 25 kHz
Exponential modulation | Symbol rate 10.42 kBaud || FCC

ACS – Adjacent channel selectivity
IMRR – Intermodulation response rejection
BD – Blocking or desensivitation

Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard			Sensitivity			Co-channel rejection		ACS *	IMRR	BD
				EN 300 113	EN 302 561	FCC part 90	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degrad.	12dB degrad.	3dB degrad.	3dB degrad.	3dB degrad.
[-]	[-]	[kBaud]	[kbit/s]				[dBm]	[dBm]	[dBm]	[dB]	[dB]	[dB]	[dB]	[dB]
2CPFSK	0,75	10,42	7,81	Comply	Comply LBT	Comply	-119	-117	-112	-6	-3	61	75	92
2CPFSK	1,00	10,42	10,42	Comply	Comply LBT	Comply	-118	-116	-111	-7	-4	60	74	90
4CPFSK	0,75	10,42	15,63	Comply	Comply LBT	Comply	-116	-113	-108	-11	-8	57	72	87
4CPFSK	1,00	10,42	20,83	Comply	Comply LBT	Comply	-114	-111	-105	-12	-9	55	71	86

FCC rules allow a higher value ot the unwanted adjacent power to be permitted. Hence a frequency deviation in CPFSK mode is increased to get slightly better values of the Ripex receiver sensitivity (and overall communication efficiency).

Channel spacing 25 kHz
Linear modulation | Symbol rate 17.36 kBaud || CE(LBT)+FCC

ACS – Adjacent channel selectivity
IMRR – Intermodulation response rejection
BD – Blocking or desensivitation

Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard			Sensitivity			Co-channel rejection		ACS *	IMRR	BD
				EN 300 113	EN 302 561	FCC part 90	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degrad.	12dB degrad.	3dB degrad.	3dB degrad.	3dB degrad.
[-]	[-]	[kBaud]	[kbit/s]				[dBm]	[dBm]	[dBm]	[dB]	[dB]	[dB]	[dB]	[dB]
π/4-DQPSK	0,75	17,36	26,04	Comply	Comply LBT	Comply	-114	-111	-107	-12	-9	56	72	83
π/4-DQPSK	1,00	17,36	34,72	Comply	Comply LBT	Comply	-112	-109	-105	-13	-10	54	70	81
D8PSK	0,75	17,36	39,06	Comply	Comply LBT	Comply	-108	-105	-99	-16	-13	50	67	81
D8PSK	1,00	17,36	52,08	Comply	Comply LBT	Comply	-106	-103	-96	-17	-14	48	65	79
16DEQAM	0,75	17,36	52,08	Comply	Comply LBT	Comply	-106	-103	-96	-20	-17	48	64	79
16DEQAM	1,00	17,36	69,44	Comply	Comply LBT	Comply	-104	-101	-94	-22	-19	46	62	77

Channel spacing 25 kHz
Linear modulation | Symbol rate 20.83 kBaud || CE+FCC

ACS – Adjacent channel selectivity
IMRR – Intermodulation response rejection
BD – Blocking or desensivitation

Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard			Sensitivity			Co-channel rejection		ACS *	IMRR	BD
				EN 300 113	EN 302 561	FCC part 90	BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degrad.	12dB degrad.	3dB degrad.	3dB degrad.	3dB degrad.
[-]	[-]	[kBaud]	[kbit/s]				[dBm]	[dBm]	[dBm]	[dB]	[dB]	[dB]	[dB]	[dB]
π/4-DQPSK	0,75	20,83	31,25	Comply	Comply	Comply	-113	-110	-106	-12	-9	55	71	82
π/4-DQPSK	1,00	20,83	41,66	Comply	Comply	Comply	-111	-108	-104	-13	-10	53	69	80
D8PSK	0,75	20,83	46,87	Comply	Comply	Comply	-106	-103	-98	-16	-13	49	66	79
D8PSK	1,00	20,83	62,49	Comply	Comply	Comply	-104	-101	-95	-17	-14	47	64	77
16DEQAM	0,75	20,83	62,49	Comply	Comply	Comply	-104	-101	-95	-20	-17	47	63	77
16DEQAM	1,00	20,83	83,32	Comply	Comply	Comply	-102	-99	-93	-22	-19	45	61	75

All values are guarenteed for temperatures from -25 to +55 °C (-13 to +131 °F) and for all frequency channels
* roofing filter (anti-aliasing) 50 kHz BW-3 dB
LBT – Listen Before Transmitt
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 and the Intermodulation response rejection. 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 (or the Intermodulation response rejection) 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.

Channel spacing 12.5 kHz
Exponential modulation | Symbol rate 5.21 kBaud || CE + FCC

Classification						Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
[-]	[-]	[kBaud]	[kbit/s]	EN 300 113	FCC part 90	[dBm]	[dBm]	[dBm]	[dB]
2CPFSK	0,75	5,21	3,91	Comply	Comply	-120	-117	-113	-7
2CPFSK	1,00	5,21	5,21	Comply	Comply	-119	-116	-112	-8
4CPFSK	0,75	5,21	7,81	Comply	Comply	-117	-114	-108	-12
4CPFSK	1,00	5,21	10,42	Comply	Comply	-115	-112	-105	-13

Channel spacing 12.5 kHz
Exponential modulation | Symbol rate 5.21 kBaud || FCC

Classification						Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
[-]	[-]	[kBaud]	[kbit/s]	EN 300 113	FCC part 90	[dBm]	[dBm]	[dBm]	[dB]
2CPFSK	0,75	5,21	3,91	Comply	Comply	-121	-119	-114	-6
2CPFSK	1,00	5,21	5,21	Comply	Comply	-120	-118	-113	-7
4CPFSK	0,75	5,21	7,81	Comply	Comply	-118	-115	-109	-11
4CPFSK	1,00	5,21	10,42	Comply	Comply	-116	-113	-106	-12

FCC rules allow a higher value ot the unwanted adjacent power to be permitted. Hence a frequency deviation in CPFSK mode is increased to get slightly better values of the Ripex receiver sensitivity (and overall communication efficiency).

Channel spacing 12.5 kHz
Linear modulation | Symbol rate 8.68 kBaud || CE+FCC

Classification						Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
[-]	[-]	[kBaud]	[kbit/s]	EN 300 113	FCC part 90	[dBm]	[dBm]	[dBm]	[dB]
π/4-DQPSK	0,75	8,68	13,02	Comply	Comply	-116	-114	-110	-12
π/4-DQPSK	1,00	8,68	17,36	Comply	Comply	-115	-112	-108	-13
D8PSK	0,75	8,68	19,53	Comply	Comply	-110	-107	-102	-16
D8PSK	1,00	8,68	26,04	Comply	Comply	-108	-105	-99	-17
16DEQAM	0,75	8,68	26,04	Comply	Comply	-108	-106	-100	-20
16DEQAM	1,00	8,68	34,72	Comply	Comply	-106	-103	-97	-22

Channel spacing 12.5 kHz
Linear modulation | Symbol rate 10.42 kBaud || CE+FCC

Classification						Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
[-]	[-]	[kBaud]	[kbit/s]	EN 300 113	FCC part 90	[dBm]	[dBm]	[dBm]	[dB]
π/4-DQPSK	0,75	10,42	15,62	Comply	Comply	-115	-113	-109	-13
π/4-DQPSK	1,00	10,42	20,83	Comply	Comply	-114	-111	-106	-14
D8PSK	0,75	10,42	23,44	Comply	Comply	-109	-106	-101	-17
D8PSK	1,00	10,42	31,25	Comply	Comply	-107	-104	-98	-18
16DEQAM	0,75	10,42	31,25	Comply	Comply	-107	-104	-99	-21
16DEQAM	1,00	10,42	41,67	Comply	Comply	-105	-102	-96	-23

Channel spacing 6.25 kHz
Exponential modulation | Symbol rate 2.6 kBaud || CE + FCC

	Classification					Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
				EN 300 113	FCC part 90				
[-]	[-]	[kBaud]	[kbit/s]			[dBm]	[dBm]	[dBm]	[dB]
2CPFSK	0,75	2,604167	1,953125	Comply	Comply	-122	-120	-114	-7
2CPFSK	1	2,604167	2,6041667	Comply	Comply	-121	-119	-113	-8
4CPFSK	0,75	2,604167	3,90625	Comply	Comply	-119	-116	-111	-12
4CPFSK	1	2,604167	5,2083333	Comply	Comply	-117	-114	-108	-13

Channel spacing 6.25 kHz
Exponential modulation | Symbol rate 2.6 kBaud || FCC

	Classification					Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
				EN 300 113	FCC part 90				
[-]	[-]	[kBaud]	[kbit/s]			[dBm]	[dBm]	[dBm]	[dB]
2CPFSK	0,75	2,604167	1,953125	Comply	Comply	-123	-121	-115	-6
2CPFSK	1	2,604167	2,6041667	Comply	Comply	-122	-120	-114	-7
4CPFSK	0,75	2,604167	3,90625	Comply	Comply	-120	-117	-112	-11
4CPFSK	1	2,604167	5,2083333	Comply	Comply	-118	-115	-109	-12

FCC rules allow a higher value ot the unwanted adjacent power to be permitted. Hence a frequency deviation in CPFSK mode is increased to get slightly better values of the Ripex receiver sensitivity (and overall communication efficiency).

Channel spacing 6.25 kHz
Linear modulation | Symbol rate 4.34 kBaud || CE+FCC

	Classification					Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
				EN 300 113	FCC part 90				
[-]	[-]	[kBaud]	[kbit/s]			[dBm]	[dBm]	[dBm]	[dB]
p/4-DQPSK	0,75	4,340278	6,5104167	Comply	Comply	-118	-116	-113	-12
p/4-DQPSK	1	4,340278	8,6805556	Comply	Comply	-117	-114	-111	-13
D8PSK	0,75	4,340278	9,765625	Comply	Comply	-112	-110	-105	-16
D8PSK	1	4,340278	13,020833	Comply	Comply	-110	-107	-102	-17
16DEQAM	0,75	4,340278	13,020833	Comply	Comply	-110	-107	-103	-20
16DEQAM	1	4,340278	17,361111	Comply	Comply	-108	-105	-100	-22

Channel spacing 6.25 kHz
Linear modulation | Symbol rate 5.21 kBaud || CE+FCC

	Classification					Sensitivity			Co-channel rejection
Modulation	FEC Code Rate	Symbol Rate	Raw Bit Rate	Standard		BER 10^{-2}	BER 10^{-3}	BER 10^{-6}	3dB degradation
				EN 300 113	FCC part 90				
[-]	[-]	[kBaud]	[kbit/s]			[dBm]	[dBm]	[dBm]	[dB]
p/4-DQPSK	0,75	5,208333	7,8125	Comply	Comply	-117	-115	-112	-13
p/4-DQPSK	1	5,208333	10,416667	Comply	Comply	-116	-113	-110	-14
D8PSK	0,75	5,208333	11,71875	Comply	Comply	-111	-109	-104	-17
D8PSK	1	5,208333	15,625	Comply	Comply	-109	-106	-101	-18
16DEQAM	0,75	5,208333	15,625	Comply	Comply	-109	-106	-102	-21
16DEQAM	1	5,208333	20,833333	Comply	Comply	-107	-104	-99	-23

3.5. 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*).

Ordering code:

RIPEX–xxxy

xxx = **370**   370–402 MHz
         400   400–432 MHz
         430   430–462 MHz

y = **empty**   basic model
         D   separate connectors for RX and TX antennas
         G   internal GPS module   430–462 MHz

Examples:

RIPEX–370   – RipEX for frequencies from 370 to 402 MHz
RIPEX–400G   – RipEX for frequencies from 400 to 432 MHz, with GPS module
RIPEX–430DG   – RipEX for frequencies from 430 to 462 MHz,
                     with two antenna connectors, with GPS module

Fig. 3.14: Ordering code

3.6. Accessories

1. **RipEX Fan kit**

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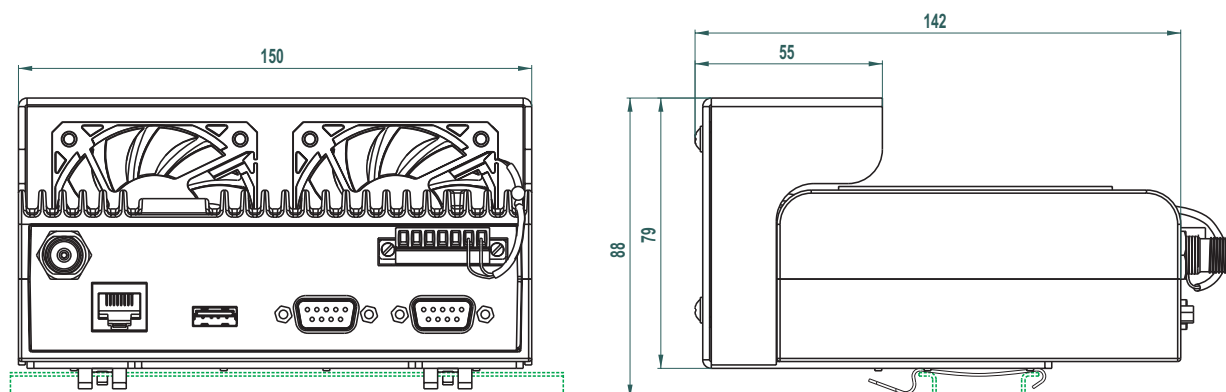

Fig. 3.15: Assembly dimensions with fan

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.
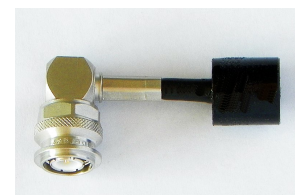

Fig. 3.16: Dummy load

3. **RipEX - L-bracket**

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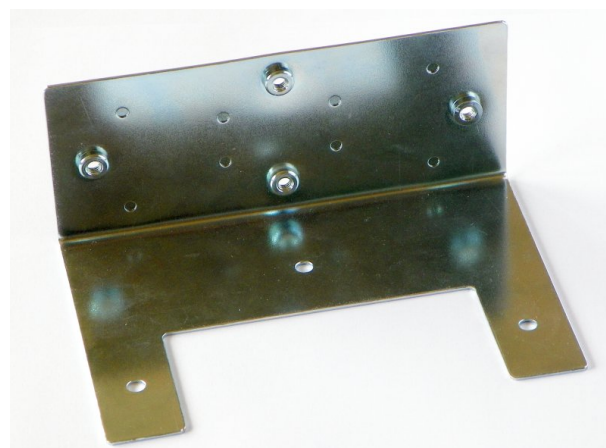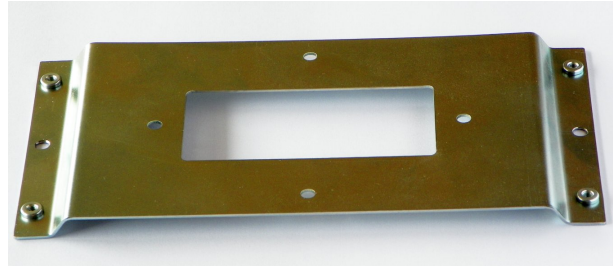

Fig. 3.17: L-bracket

4. **RipEX - Flat-bracket**

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

Fig. 3.18: 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. 3.19: 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 4.3, "Connecting RipEX to a programming PC".

Fig. 3.20: 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. 3.21: 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

1x Backup battery

3x Dummy load antenna

1x Pig-tail for connecting an external antenna

1x L-bracket, 1x Flat-bracket

1x Fan kit

1x X5 - ETH/USB adapter

Network cable

Printed user manual

Outside dimension: 455 x 365 x 185 mm

Weight ca. 4 kg (excluding the RipEx's)

4. Bench test

4.1. Connecting 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 3.6, "Technical parameters". When using a PoE power source, use the PoE standard IEEE 802.3af. 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.
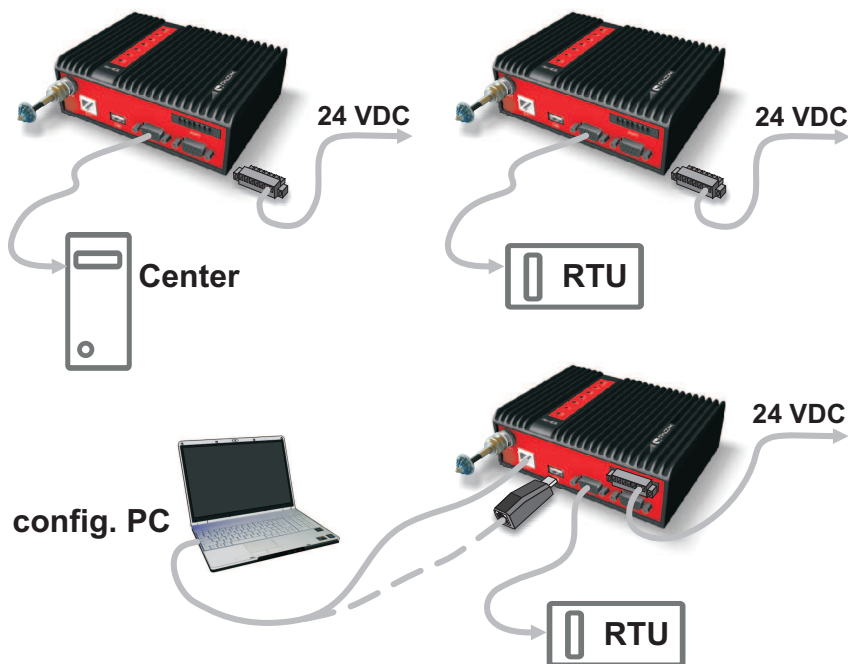
Fig. 4.1: Bench test

4.2. Powering up your RipEX

Switch on your power supply. LED PWR flashes quickly and after 8 seconds it switches to 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 3.3, "Indication LEDs".

4.3. 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

https://10.42.42.255
PC DHCP

https://192.168.169.169
PC 192.168.169.250

Fig. 4.2: 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)
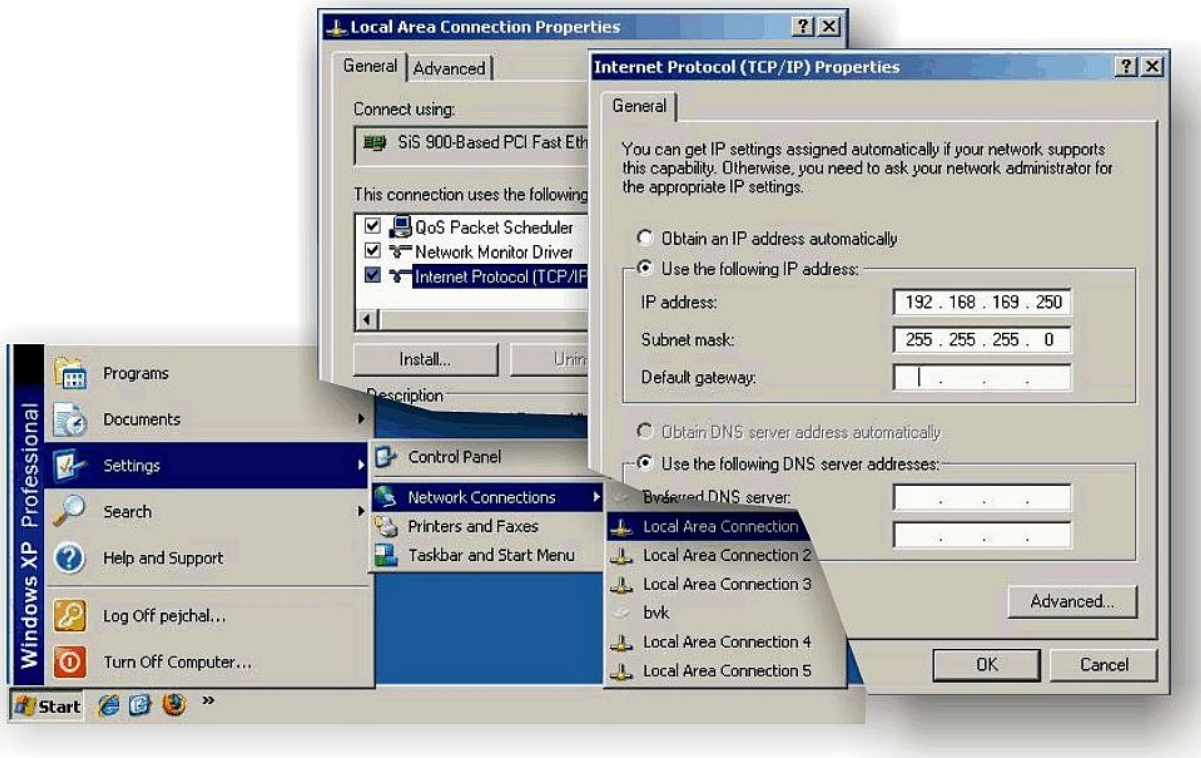   Some Operating systems may require you to reboot your PC.

Fig. 4.3: 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:
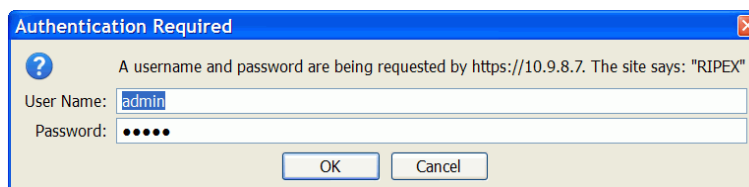
Fig. 4.4: Authentication

The default entries for a new RipEX are:

User name: admin
Password: admin
Click OK.

Initial screen should appear then:

Fig. 4.5: 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 3.2.6, "Reset button".

4.4. 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 6, *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, Routing[1].

4.5. 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 3.3, "Indication LEDs".

---

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

5. Installation

Step-by-step checklist

1. Mount RipEX into cabinet (Section 5.1, "Mounting").
2. Install antenna (Section 5.2, "Antenna mounting").
3. Install feed line (Section 5.3, "Antenna feed line").
4. Ensure proper grounding (Section 5.4, "Grounding").
5. Run cables and plug-in all connectors except from the SCADA equipment (Section 3.2, "Connectors").
6. Apply power supply to RipEX
7. Connect configuration PC (Section 4.3, "Connecting RipEX to a programming PC").
8. Configure RipEX (Chapter 6, *Advanced Configuration*).
9. Test radio link quality (Section 4.5, "Functional test").
10. Check routing by the ping tool (Section 6.5.3, "Tools") to verify accessibility of all IP addresses with which the unit will communicate.
11. Connect the SCADA equipment.
12. Test your application.

5.1. Mounting

5.1.1. 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. 5.1: Flat lengthwise mounting to DIN rail – recommended
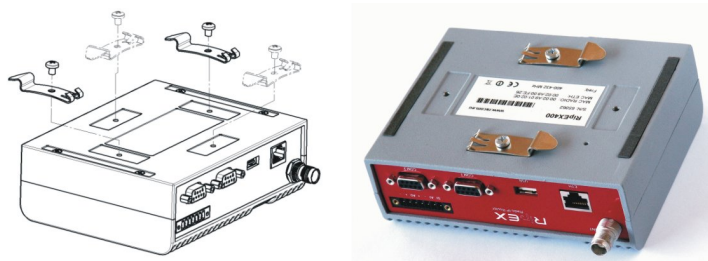
Fig. 5.2: Flat widthwise mounting to DIN rail

For vertical mounting to DIN rail, L-bracket (optional accessory) is used.
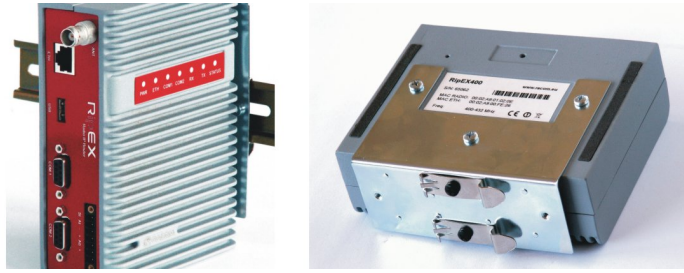
Fig. 5.3: Vertical widthwise mounting to DIN rail
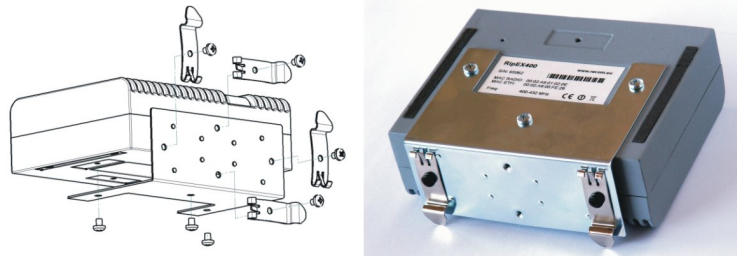
Fig. 5.4: Vertical lengthwise mounting to DIN rail

5.1.2. Flat mounting

For flat mounting directly to the support you must use the Flat bracket (an optional accessory).
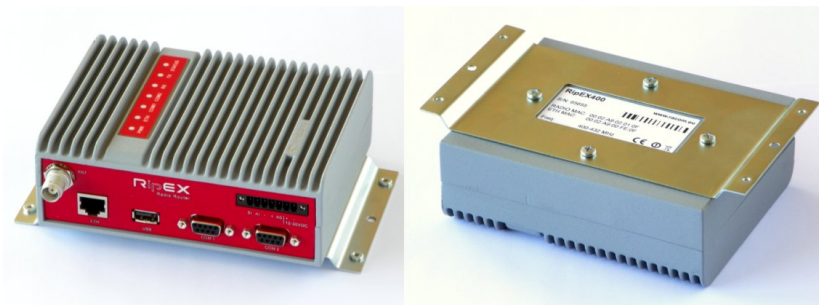
Fig. 5.5: Flat mounting using Flat bracket

5.1.3. 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. 5.6: Rack shelf

5.1.4. 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 M4x8 screws.
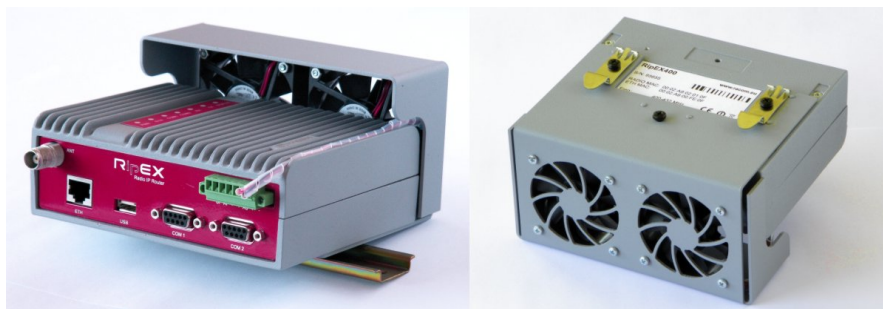
Fig. 5.7: Fan kit mounting

The fan kit may be controlled using the Alarm Output (Control and Power connector, Section 3.2.2, "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.

Fan Kit

SI AI - + A0 | + -
                | 10–30VDC

Pin No.:   1 2 3 4 5 6 7
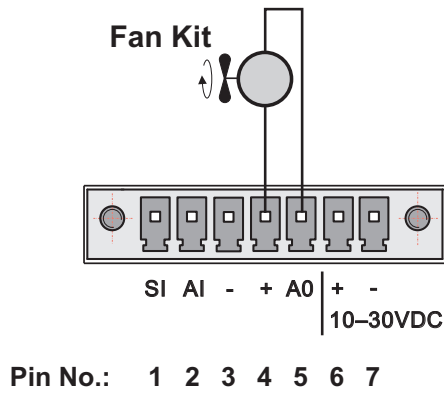
Fig. 5.8: Fan kit using Alarm Output, recommended

Fan Kit

SI AI - + A0 | + -
                | 10–30VDC

Pin No.:   1 2 3 4 5 6 7

Fig. 5.9: Fan kit, always on

5.2. 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. A proper network planning, including field signal measurements, should decide antenna types in 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's dimensions and weight, to ensure the adequate stability. Follow the antenna manufacturer's instructions during installation.

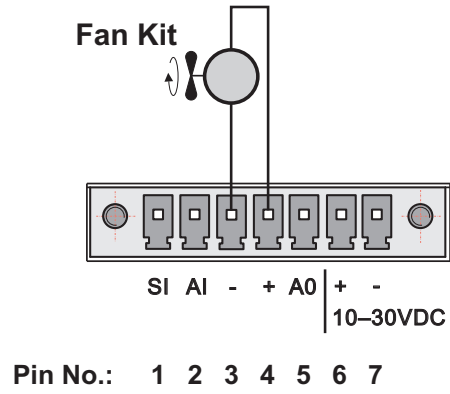Antenna should never be installed close to potential sources of interference, especially electronic devices like computers or switching power supplies. A typical example of totally wrong placement is mounting a whip antenna directly on top of the box containing all the industrial equipment which is supposed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

5.3. Antenna feed line

Antenna feed line should be chosen so that its attenuation does not exceed 3 to 6 dB as a rule of thumb, see Section 2.8, "Network Planning". Use impedance 50 ohm 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.

5.4. 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.

5.5. Connectors

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

You will find the connectors' pin-outs in chapter Section 3.2, "Connectors".

5.6. 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.

The power supply should be connected in one of following two ways:

• 10-30 VDC

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.

+10 to +30 V

Fig. 5.10: 10-30 VDC Supplying

- PoE

The RipEX can also be powered over the ethernet interface using PoE (Power over Ethernet) according to the standard IEEE 802.3af, i.e. 36 to 57 V (48 V nominally). The RF output of the RipEX is limited to 1 W if PoE powered.

Always follow the power supply manufacturer's instructions and recommendations.

ETH + PoE

Fig. 5.11: PoE Supplying

6. Advanced Configuration

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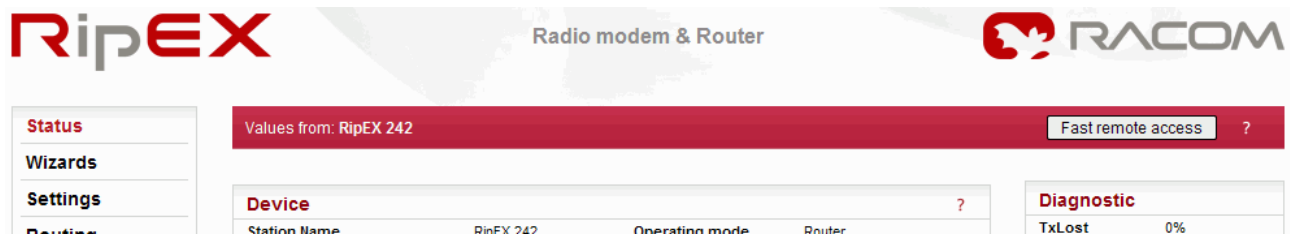
6.1. Menu header

Fig. 6.1: Menu Header

6.1.1. Generally

RipEX can be easily managed using any web browser (Mozilla Firefox, Microsoft Internet Explorer, etc.) from your computer. If there is an IP connection between the computer and the respective RipEX, you can simply enter IP addresss of any RipEX in the network directly to address line of the browser 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 Radio channel, resulting in quite long response times.

When you need to manage an over-the-air connected RipEX, log-in a RipEX, to which your computer is connected using either cable (via LAN) or high speed WAN (e.g. Internet). The RipEX into which you are logged-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 Router mode, the IP address of either Radio or Ethernet interface in remote unit can be used for this 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 Bridge mode, IP addreses of Ethernet interfaces are used for both, Local and Remote units. Be carefull, each RipEX MUST have its unique IP address and all these IP addresses have to be within the same IP network (defined by Mask) when remote management is required in Bridge mode.

Values from

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

Local

This is IP address of "locally" connected RipEX. This IP equals to the IP in the address line of your browser.

Remote

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

Connect

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

Disconnect

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

6.2. Status

Fig. 6.2: Menu Status

6.2.1. 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.

6.2.2. 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.

6.3. Settings

Fig. 6.3: Menu Settings

6.3.1. 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 is not any DNS (Domain Name Server) used in RipEX netowrk.

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.

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 IP address of Ethernet interface itself is not significant. Each ETH interface automatically learns which devices (MAC addresses) lay 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 be otherwise 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 broadcasted 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 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.
    IIt is possible to use even more than one Repeater within a network. To eliminate the risk of creating a loop, Number of repeaters has to be set in all units in the network, including Repeater units themselves.

  - **Number of repeaters**
    Default = 0
    If there is a repeater (or more of them) in the network, the total number of repeaters within the network MUST be set in all units in the network, including Repeater units themselves. After transmitting to or receiving from 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 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 parameter Number of repeaters is zero, i.e. in a network without repeaters.

- **TX delay [ms]**
Default = 0
It delays forwarding of all frames from user interfaces (ETH&COM's) to Radio channel for 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 collision, TX delay should be set individually in each slave RipEX. The lenght 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 broadcasted 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 incomming bytes, the byte after gap is treated as the first byte and process starts again from the beginning. Stuffing is never transmitted between block of bytes.

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

  When 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 control of data integrity. If the Baud rate of COM is significantly lower than Modulation rate on 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 the Repeater in the network.

Router

Router mode is suitable for Multipoint networks, where Multi-master apllications with any combination of polling and/or spontaneous data protocols can be used. The proprietary link-layer protocol on Radio channel is very sophisticated, it can transmitt both unicast and broadcast frames, it has the collision avoidance capability, it uses frame acknowledgement and retransmissions and 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 router Default gateway (apply to both interfaces) in the Routing table.

The COM ports are treated in 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 packet according its setting of Retries.

    Note: The acknowledgement/retransmission scheme is an embeded 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. packet is transmitted only once and it is not repeated.
- **Retries [No]**
  Default = 3
  When acknowledge from receiving RipEX is not received, the frame is retransmitted. The number of possible retries is specified.
- **RSS threshold [-dBm]**
  Default = 120
  RSS (Received Signal Strength) limit for access to Radio channel. RipEX does not start the 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.

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
    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 accurancy of time, which NTP server provides.
  - **Delay [ms]** This is the delay of packet (1/2 round trip time), which RipEX received from NTP server while asked for synchronization. This delay is compensated in 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 implemented.

On-line help for each individual item is provided by balloon tips (when cursor is placed over the item name).

- **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 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 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 botom side of RipEX (press it for 15% sec.) in order to set Default access, which restores 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 treshold, the selected action(s) is(are) invoked.

Note: At least 10 values have to be included in average value, otherwise alarm is not checked.

- **Treshold**
  List box: Default, Manual,
  Default = Default
  Default – Default (recommended) values are set and can not be edited.
  Manual – Tresholds 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 treshold 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.**", HW Alarm Output is active and its normal status (no alarm) is open or closed, respectively.

  HW Alarm Output is a pin (open n-p-n colector) on screw terminal connector on 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"

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 1,5W. When it receives a packet for its IP address, it wakes up. However data from this first received packet is lost.
  - 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
    RipEX stays on for the set time from the moment of its wake up.
  - Reset timeout on received packet
    List box: On, Off
    Default = On
    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 0,07W. The time needed for complete wake-up is approx. 25 seconds (booting time).

  - **Timeout from sleep request [sec.]**
    Default = 300
    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
    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 carefull to use this feature.

  - **Neighbours&Statistic log save period [min]**

Default = 1440 min (1 day)
This is the period, in which Neighbours and Statistic 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: Alarm, Single, Continuously
        Default = Alarm
        Detail graph data sampling is started based on selected event from list box:
        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 normaly and no other file is opened.

Single – a single Detail graph file is manually started immediatelly after the Apply button is clicked.

Continuously – Detail graph files are periodically saved in the same way as Overview graph files are.

6.3.2. Radio

Fig. 6.4: 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 1.25 kHz.
The value entered must be within the frequency tuning range of the product as follows:
RipEX160: 140–170 MHz
RipEX400: 400–440 MHz
XXX

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
Possible values in list box depen on the Modulation rate set. When PoE power supply is used, possible values of RF power are limited as well. 10 W is available only when the respective SW feature key is active.

Channel spacing [kHz]**

List box: possible values
Default = 25 kHz

The wider channel the higher Modulation rate is possible

Modulation rate [kbps]

- **Approval**
  List box: possible values
  - **CE**
    Radio parameters meet ETSI EN 300 113-1 V1.6.2 (2009-11), ETSI EN 302 561 V1.2.1 (2009-12) and FCC part 90
  - **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.
  - **CE LBT**
    Radio parameters meet ETSI EN 300 113-1 V1.6.2 (2009-11) and ETSI EN 302 561 V1.2.1 (2009-12) parameters for LBT (Listen Before Transmitt) mode

- **Modulation rate [kbps]**
  List box: possible values
  Default = 83.33|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 (up to an 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.

Turbo*

List box: On, Off

Default = Off

Turbo 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 continous 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 adition 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 Turbo depends on many factors (data content, packet lenghts, network layout etc.), the total increase of network throughput can be anything from 0 to 200%, or even more in special cases.

Note: Apart of this Turbo, there is an independent compression on 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 lenght 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 (max. packet size)
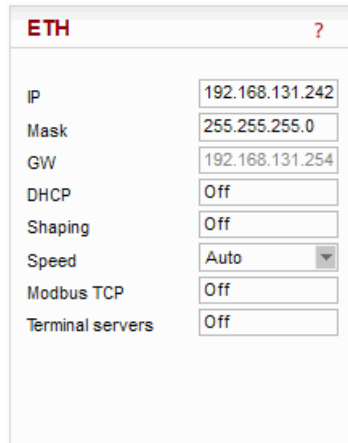
When packet to be transmitted from the Radio interface is longer than the MTU (Maximum Transmission Unit) set, the RipEX router performs standard IP fragmentation. A packet longer than the configured size is split into the needed number of fragments, which are then independently transmitted - the first 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.

6.3.3. ETH

* Active only when Router mode

Fig. 6.5: Menu Ethernet

IP

Default = 192.168.169.169
IP address of ETH interface

Mask

Default = 255.255.255.0
Mask of ETH interface

GW

Default = 0.0.0.0
The default gateway (applies to whole RipEX). It can be set also 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
  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 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 execute Apply and set DHCP server to On (+Apply) again.

- **Preferred IP's**
  It is possible to define which IP should be assigned by Server to 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. The next over-limit packets are discarded.

Modbus TCP*

For more information refer to Application note Modbus TCP.

** - 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
  TCP port used for Modbus TCP in RipEX.

- **TCP Keepalive [sec.]**
  Default = 120

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
      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, Manual.
      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 server*

Generally a Terminal Server (also referred to as 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 center should be connected to 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 the HW serial interface on the computer
- serial cable between 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 place of installation of RipEX already exists
- Modbus TCP with local TCP sesions on slave sites or when combination of Modbus RTU and Modbus TCP are used. For more information refer to Application note Modbus TCP/RTU

Note: The TCP (UDP) session operates only locally between RipEX and 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 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 has come from a COM port. When the data reaches the destination RipEX, it can be transffered 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 timeout in sec.for which the TCP socket in RipEX is kept active after a receipt of 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). **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

6.3.4. COM's

* Active only when Router mode

COM's			?
	COM 1		**COM 2**	
Type	RS232	▼	RS232	▼
Baud rate [bps]	19200	▼	19200	▼
Data bits	8	▼	8	▼
Parity	None	▼	None	▼
Stop bits	1	▼	1	▼
Idle [bytes]	5		5	
MRU [bytes]	1600		1600	
Flow control	None	▼	None	▼
Protocol	Modbus		None	

Fig. 6.6: Menu COM

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.

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.

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
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 (= maximum)
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.

6.3.5. Protocols

Fig. 6.7: 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 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 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 guaranties 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 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 like 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**
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.
- **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 DNP3 protocol has got source and destination addresses in its header, so there is no difference between Master and Slave in terms of RipEX configuration. DNP3 allows both, Master-Slave polling as well as spontaneous communication from remote units.
Broadcasts packets are not used, so only Address translation parameters are necessary to set.

Address translation

> *Table*

> *Mask*

UNI

UNI is the "Universal" protocol utility designed by RACOM. It is supposed to be used when "your" protocol is not on RipEX list. The only condition is that Master station generates only one type of frames and Protocol address is always on the same place (Address position).
Underlined parameters are described in *Common parameters*.

Mode of Connected device

> *Master*

- **Address mode**
  List box: Binary (1 B), Ascii (2 B)
  Default = Binary (1 B)
  RipEX reads the Protocol address in set format and length (Bytes).
  Ascii format is translated to binary one for the next Address translation.
  E.g. Ascii 6566 is translated to 0xAB
- **Address position**
  Specify the number of bytes from the beginning of the frame, where Protocol address starts.

> > *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 full duplex mode of DF1 is supported. Each frame in Allen-Bradley DF1 protocol has got source
and destination addresses in its header, so there is no difference between Master and Slave in Full
duplex mode in terms of RipEX configuration.
Broadcasts packets are not used, so only Address translation parameters are necessary to set.

- **Mode**
  List box: Full duplex, Half duplex
  Default = Full duplex

- **Block control mode**
  List box: BCC, CRC
  Default = Full duplex
  According DF1 specification, either BCC or CRC for Block control mode (data integrity) can be
  used.

- **Broadcast**
  List box: Off, On
  Default = Off

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.
    I.e. when RipEX receives the frame from connected device, it generates ACK frame (0x1006)
    locally. When RipEX receives the frame from the Radio channel, it sends this frame to connected
    device and waits for ACK. If ACK is not received within 1 sec. timeout, RipEX sends ENQ
    (0x1005) when Full duplex or repeats the frame when Half duplex. If ENQ (the frame) is not
    confirmed by ACK, it is once repeated from RipEX after 1 sec.

Profibus

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

Mode of Connected device

Master

    Broadcast

    Address translation

        Table

        Mask

Slave

    Broadcast accept

6.4. 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 got its own MAC address, IP address and Mask. IP packets are processed according the Routing table then.

The COM ports are treated in 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.

6.4.1. Menu Routing

Fig. 6.8: 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 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 baloon tip while cursor is in specific line on Mask. It shows which IP addreses are included in the network which is routed to respective Gateway.

Interface

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

When Auto is selected, 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.

6.5. Diagnostic

6.5.1. Neighbours and Statistic

Fig. 6.9: Menu Neighbours

Neighbours and Statistic follow the same pattern.

Most importantly, they share 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 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, 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 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 - the log is manually saved, stored in history file and cleared. This is equal to situation when Log save period expires.
Note: Remember that both Neighbours and Statistic logs are saved.

• **Difference**
  Clear - when executed, 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 - displays values of the Difference log, i.e. the values accumulated from time when the Set button has been executed.

  Notice, that Log start, Last upd. and Log uptime labels at the top has been changed to Diff. start, Diff. upd. and Diff. uptime when 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. Refresh 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 executed 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. Judging DQ requires experience, rule-of-thumb values: below 100 means the link is unusable, at 125 short packets should get through, 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. In case of PoE supplying the characters PoE appears instead.
- **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. 6.10: 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 PRO-TOCOL 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.

6.5.2. Graphs

Graphs functionalities as well as meanings of **Overview**, **Detail**, **Sampling period** are described in the help Settings/Device.
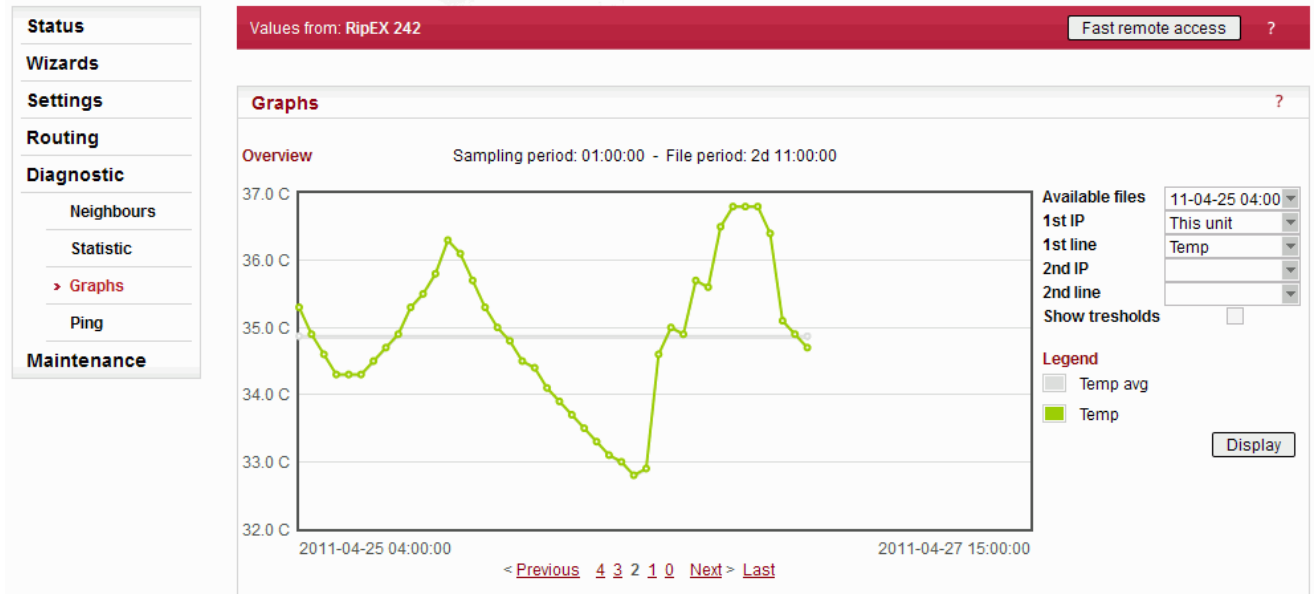
Fig. 6.11: Menu Graphs

- **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.
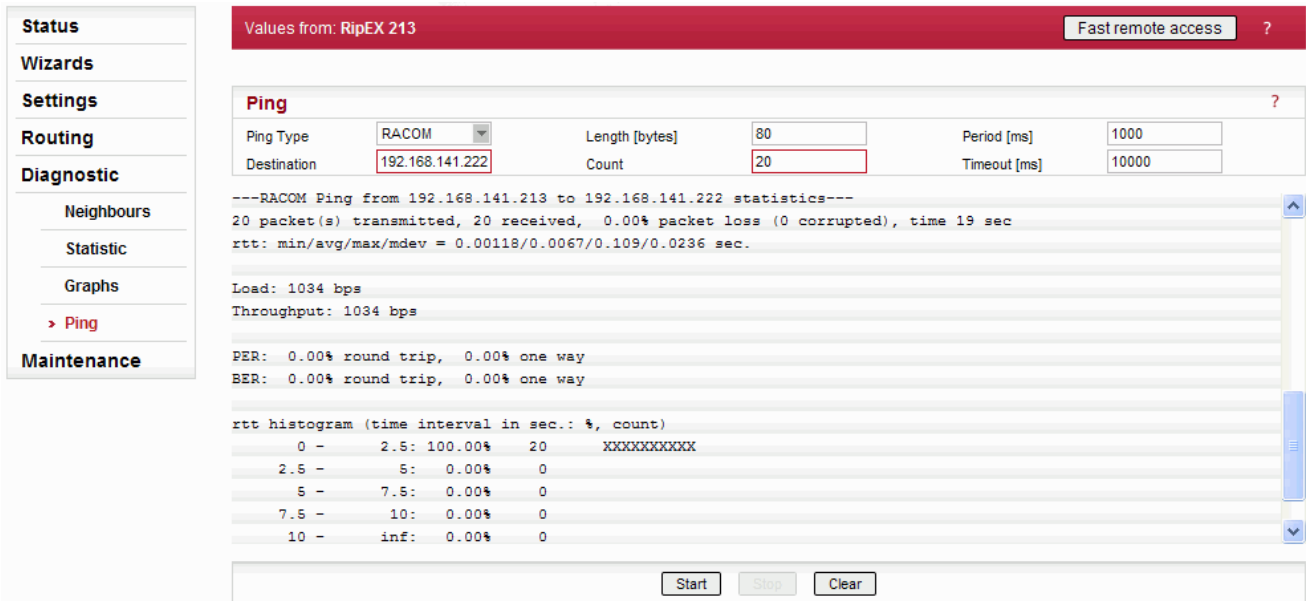
6.5.3. Tools

Ping

Fig. 6.12: 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, RACOM
  Default = RACOM
  - **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.
  - **RACOM**
    RACOM 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
  RACOM - 43 bytes for IP+UDP+RACOM header + 8 bytes (Trace-RSS and DQ) per each radio hop + 4 bytes (marking in server)
  RACOM ping can not be longer than 3/4 MTU.

- **Count**
  Default = 10
  Number of pings to be transmitted. The allowed range is from 1 to 1024.

- **Period [ms]**
  Default = 5000
  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 10.10.10.223: icmp_req=4 ttl=64 time=74.8 ms"
      88 bytes = total packet lenght
      10.10.10.223 = 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:**
      "10 packets transmitted, 10 received, 0% packet loss, time 45000ms"
      "rtt min/avg/max/mdev = 74.891/695.531/2025.624/560.579 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
  - **RACOM**
    - **Run-time report:**
      "131 bytes from 192.168.2.3: req=4 rtt=0.720s"

"192.168.2.1-->10.10.10.2 :36/95[RSS/DQ]-->10.10.10.3 :45/63[RSS/DQ]-->192.168.2.3"
"192.168.2.3-->10.10.10.2 :39/68[RSS/DQ]-->10.10.10.1 :45/77[RSS/DQ]-->192.168.2.1"
131 bytes = RACOM packet size (RACOM header + data + trace)
192.168.2.3 = 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 4.671 sec."
"rtt min/avg/max/mdev = 74.891/695.531/2025.624/560.579 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: 1053 bps"
"Throughput: 1053 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: 45.0/45.2/46.0/5 min/avg/max/hom"
"DQ : 55.0/62.6/72.0/4 min/avg/max/hom"

"Radio hop with lowest RSS – direction from Destination"
"RSS: 45.0/45.0/45.0/8 min/avg/max/hom"
"DQ : 59.0/67.6/81.0/3 min/avg/max/hom"
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 "Homogenity" shows the jitter of RSS values from individual pings.

"rtt histogram (time interval in sec.: %, count)"
" 0.000 - 2.500: 100.00% 5" XXXXXXXXX
" 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

6.6. Maintenance

6.6.1. SW feature keys

Fig. 6.13: Menu SW feature keys

Certain advanced RipEX features are activated with software keys. One may see the list of possible keys and their status. Possible status values:

- **Uploaded –** uploaded in RipEX, but not active
- **Not present**
- **Active**
- **Time limited –** the key can be time limited. For such a type, the remaining time is displayed (1d 07:33:20). Time is calculated as the run time of the unit.
- **Master –** when Master key (unlocks all keys) is active.

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

- **Upload** – when executed, SW key is uploaded into the RipEX, however it is not active yet. You can subsequently upload more keys.
- **Activate** – when executed, uploaded keys (see key status) are activated. Afterwards the unit automatically reboots.

6.6.2. Configuration

Fig. 6.14: Menu Maintenance Configuration
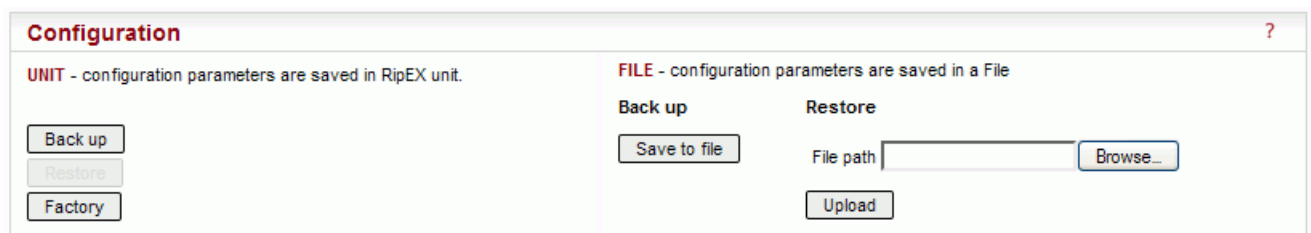
- **UNIT**
    - **Back up** – Back up saves the active configuration into a backup file in the unit.
    - **Restore** – configuration saved in the backup file in the unit is activated and the unit reboots.
    - **Default** – sets factory defaults and activates them. The unit reboots afterwards.
- **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.

6.6.3. Firmware

Fig. 6.15: Menu Maintenance Firmware

The firmware in the unit consists of several parts, however they come in one firmware package. Their names and versions can be seen. There can be two versions of firmware package 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.

- **Upload to Archive** – Fill in the file path, or browse your disk in order to find the file. When file is selected, it is uploaded and becomes the Archive firmware.
- **Archive to Active** – when executed, the Active firmware is substituted by the Archive firmware. 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 execute the button.

6.6.4. Password

Fig. 6.16: Menu Maintenance Password

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

6.6.5. Miscellaneous

- **Reboot** – when executed, the unit correctly shuts down and starts again. The reboot time is approx. 25 sec.

6.6.6. Technical support package

Fig. 6.17: 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 history can 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.

7. 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.

8. Troubleshooting

- **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 3.2.6, "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.

- **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.

- **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.

- **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.

- **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.

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

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

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

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

- **The RACOM 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 disturbing signals come from different directions, changing the direction of the antena may solve the problem. A unidirectional antenna should be used in the first place. Metallic objects in close vicnity of the antenna may cause harmful reflections, relocating the antena by few meters may help. Change of polarization at both ends of the link could be the solution as well.

- **The RACOM Ping test shows bad homogeneity.**

  - Quite often the bad homogeneity comes together with a low DQ. In that case follow the advices given in the previous paragraph. If rather the DQ corresponds to the RSS level, you should look for unstable elements along the signal route - 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 strong enough to cope with it.

9. Safety, environment, licensing

9.1. Frequency

The radio modem must be operated only in accordance with the valid frequency license issued by national frequency authority and all radio parametres has 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.

9.2. 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.

Tab. 9.1: Minimum Safety Distance

	Antenna Gain		
	5 dBi	10 dBi	15 dBi
160 MHz	1 m	2 m	4 m
300 and 400 MHz	1 m	2 m	4 m
900 MHz	0.7 m	1 m	2 m

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

9.4. 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.

9.5. Important Notifications

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

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. Under any circumstances the author or another company or person is not responsible for secondary, accidental or related damages resulting from application of this product.

The producer does not provide the user of 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 does not provide of guarantees if the company product has been used in these aforementioned devices.

RACOM Open Software License

Version 1.0, November 2009
Copyright (c) 2001, RACOM s.r.o., Mírová 1283, Nové Město na Moravě, 592 31

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

The program (binary version) is available for free on the contacts listed on 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.

A. Revision History

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

Revision 1.0   2011-05-16
First issue