

## **Application notes**





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

### Table of Contents

Introduction	. 5
1. Basic Configuration Parameters	. 6
2. Configuration Example	. 7
3. RipEX1-Base Configuration	. 8
4. RipEX2-Remote Configuration	10
5. RipEX3-Remote Configuration	12
6. RipEX4-Remote Configuration	13
7. Testing	15
A. Revision History	17

### Introduction

GRE (Generic Routing Encapsulation) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. The GRE Tunnel can be configured between any two devices that are compatible with this protocol.

- From the point of view of the traffic transferred, the GRE tunnel is one hop.
- There are 2 modes of GRE operation: TUN (Tunnel mode) or TAP (L2 transparent connection) with SW bridge. Implementation within RipEX only covers the TUN mode.
- Packets passing through the GRE tunnel are not protected against loss and are not encrypted.
- The GRE tunnel neither establishes nor maintains a connection with the peer. The GRE tunnel is created regardless of peer status (peer need not exist at all).
- The GRE tunnel has its own IP address and mask. Network defined by this address and mask contains only 2 nodes each end of the tunnel.
- As the GRE tunnel adds an additional header, a lower MTU is set (1476 B) to prevent GRE packet fragmentation. Incoming packets may be fragmented within the GRE interface.

### NOTE:

Packet acknowledgment and encryption (AES256) can be configured on the Radio channel. Both options are independent of GRE tunnels and apply to all the radio traffic.

### **1. Basic Configuration Parameters**

GRE Enables the whole GRE subsystem, the default value is "Off".

- GRE tunnels Each row/record corresponds to one GRE tunnel. There should not be more than 20 simultaneous GRE tunnels (recommendation). The Key/Primary Field of the table is "Peer address", which uniquely identifies each tunnel.
- Peer address The IP address of a remote GRE tunnel end-point. This end-point IP address must be unique and cannot be used for more than one tunnel. The local address (interface) is automatically selected based on the destination address type. Addresses on both ends must correspond to each other.
- Tunnel IP/MASK The tunnel IP address and mask. The network defined by this item must cover only the local tunnel address and remote end-point address. Both tunnel end-points must be within the same subnet, but IP addresses must be different. The remote end-point IP address is used as a "Gateway" for tunnel configuration. The network mask can even be /31 (255.255.255.254), because it is a p2p (no need for a network address and a broadcast address).
- Note The tunnel description.
- Active Enables or disables the particular tunnel.

Routing into the GRE tunnels can be configured in the Routing menu. The Gateway must be set as a remote end-point GRE tunnel IP address.



### 2. Configuration Example

Fig. 2.1: Topology

In this example, 4 RipEX units will be interconnected using a GRE tunnel. Routing will be configured for particular subnets and the communication will be verified.

RipEX1, acts as a centre for three remote units. Flexible Router mode will be utilized. Each RipEX is connected via Ethernet to its own local network and two remote RipEX units simulate using several subnets by "Alias" addresses (e.g. SLIP protocol). The Radio network subnet is 10.10.10.0/24. The GRE tunnel is not used on the radio channel. It is only utilized on the Ethernet network.

This example shows how a GRE tunnel can be used to route data via any L3 network without being able to alter the routing rules of this network – i.e. we cannot add RipEX subnets to the current routers, firewalls or other existing infrastructure. That's the reason to encapsulate all data to GRE, changing all packets to have IP headers from routable subnets – i.e. 192.168.131.0/24 and 192.168.141.0/24 in our example.

The RipEX configuration can be performed via Ethernet, USB/ETH or USB/WiFi access. Another option is to use the "Fast Remote Access" feature from any of the units to configure the rest of the network.

There is only one GRE tunnel. Both end-points are RipEX units; there is no need for any other external device.

RipEX1-Base <--> RipEX2-Remote: 10.2.2.0/31

## 3. RipEX1-Base Configuration

Status	Values from: RipE	X1-Base					Fast remot	e access	
Wizards									
Settings	Device								
Routing	Unit name F	RipEX1-Base	Time	Manual	Alarm management	Default	Neighbours&Statistics	Default	
VPN	Operating mode	Router	SNMP	Off	Power management	Always On	Graphs	Default	
IDaga	Hot Standby C	Dff	Firewall	Off	WiFi	On	Management	Default	_
IPSec	Padio		2	CTU	2	COM			
GRE	Radio		•	EIN	•	COM	COM 1	COM 2	
Diagnostic	Radio protocol	Flexible		IP	192.168.131.238	Туре	RS232 👻	RS232	
Neighbours	IP	10.10.10.	1	Mask	255.255.255.0	Baud rat	e [bps] 19200 💌	19200	
Statistic	Mask	255.255.2	:55.0	DHCP	Off	Data bits	8 💌	8	
Granhs	<ul> <li>TX frequency</li> </ul>	436.360.0	00	Shaping	Off	Parity	None 💌	None	
orupiis	RX frequency	436.360.0	00	Speed	Auto 💌	Stop bits	1 💌	1	
Ping	<ul> <li>Channel spacing [kH</li> </ul>	lz] 25.0	Ψ.	Modbus TCP	Off	Idle [byte	s] 5	5	
Monitoring	Modulation rate [kbp	s] 83.33   16	DEQAM	Terminal servers	011	MRU [by	tes] 1600	1600	
Maintenance	RF power [W]	0.5	Ψ.	TCP proxy	011	Flow cor	ntrol None 💌	None	
Maintenance	<ul> <li>Optimization</li> </ul>	Off	Ψ.	ARP proxy & VLA	N Off	Protocol	None	None	
	Encryption	Off							
	<ul> <li>MTU [bytes]</li> </ul>	1500							

Fig. 3.1: Centre configuration

In the Settings menu, change the Unit name to RipEX1-Base. The Operating mode is set to "Router" ("GRE" is not configurable in the Bridge mode).

Within the Radio parameters, "Flexible" mode is set. Configure the 10.10.10.1/255.255.255.0 IP address/netmask parameters. The frequency must be the same for all RipEX units, but otherwise is configurable as required. The channel spacing is set to 25 kHz and Modulation rate to 16DEQAM (83.33 kbps).

#### NOTE:

The parameters marked with a small red square must be the same within all RipEX units in network.

The last step is the Ethernet IP configuration – 192.168.131.238 / 255.255.255.0.

Status	Values from: RipEX1-Bas	se			Fast	remote access	?
Wizards							
Settings	GRE						
Routing	GRE	On 🔻					
VPN	GRE tunnels						
IPsec	Peer address		Tunnel IP/MASK	Note	Active	Modify	
0.05	192.168.141.239	10.2.2.0/31			~	Delete Add	
> GRE						Add	
Diagnostic							
Neighbours							
Statistic			Apply	Cancel			

Fig. 3.2: Centre station GRE configuration

GRE configuration is very straight-forward (all parameters are described at the beginning of this chapter). The Peer address is set to RipEX2-Remote Ethernet address – 192.168.141.239. The tunnel address should not overlap with any other subnet in the network.

**IMPORTANT:** 

The GRE tunnel only ever uses two IP addresses; thus the /31 mask is recommended.

Because the local GRE IP address was set as 10.2.2.0 the remote must be set to 10.2.2.1. The check box "Active" is enabled.

zarus												
ttings	Inter	aces										
uting	Radio	MAC	00:02:A9:BA:54:2B		IP 10.10.1	10.1	I	lask 255.2	55.255. <b>0</b>			
N	ETH	MAC	00:02:A9:BA:50:43		IP 192.16	8.131.238		lask 255.2	55.255.0		GR	E tunnels 👻
IPsec	Route	es										
GPE		Destination	Ma	ask	Gatewa	ay	Backup		Note		Active	Modify
UNL	192.168.	141.239/32	255.255.25	5.255	192.168.131.25	54	Off	R	oute to Remot	e2	~	Telete Add
gnostic	192.168.	141.0/24	255.255.25	5.0	10.2.2.1		Off	G	RE RipEX2 LA	AN .	~	≜ ▼ Delete Ad
Neighbours	172.20.2	0.0/30	255.255.25	5.252	10.2.2.1		Off	Ri	pEX2 Alias		~	* Telete Add
Heighbours	172.16.1	00.0/24	255.255.25	5.0	10.10.10.3		Off	Ri	pEX3 LAN		~	* Telete Add
Statistic	172.20.2	0.4/30	255.255.25	5.252	10.2.2.1		Off	Ri	pEX4 Alias		~	* Telete Add
Graphs	172.16.2	00.0/24	255.255.25	5.0	10.2.2.1		Off	Ri	pEX4 LAN		~	Delete Add
Ding	Default				0.0.0.0		Off					Add
Monitoring	Back	up										
ntenance	Name	Peer IP	Hysteresis [s]	SNMF	P Notification	HW A	larm Output	Alt	ernative pa	ths Active	Note	Modify
												- Add

Fig. 3.3: Centre station routing rules

The last menu to configure is "Routing". Together, 6 routes are configured in this example. You might configure different rules, but be consistent across all RipEX units.

- 192.168.141.239/32, Gateway 192.168.131.254
  - This route will probably be different in your network usually it is the nearest router that handles routing in your existing L3 network. For testing purposes, you can use our cellular router M!DGE.
  - The routing rule for RipEX2-Remote Ethernet subnet is required due to the accessibility of this remote RipEX unit -> correct GRE tunnel functionality.
- 192.168.141.0/24, Gateway 10.2.2.1
  - This route is used for all other units in 192.168.141.0/24 subnet and is routed to the RipEX2-Remote unit via GRE tunnel.
- 172.16.100.0/24, Gateway 10.10.10.3
  - Route to the RipEX3-Remote unit no GRE tunnel is used, common radio transmission.
- 172.20.20.0/30, 172.20.20.4/30 and 172.16.200.0/24, Gateway 10.2.2.1
  - Three routes to remote RipEX networks as a gateway, 10.2.2.1 Remote GRE IP address is used -> no need to add any routing rules in the existing L3 network.

## 4. RipEX2-Remote Configuration

Status	Values from: Rip	EX2-F	lemote								Fast	remote	access	
Wizards														
Settings	Device													?
Routing	Unit name	RipEX	2-Remote	Time		Manual	Alarm management	Defa	ault	Neig	hbours&Sta	tistics	Default	
VEN	Operating mode	Route	r 🔻	SNM	Р	Off	Power management	Alw	ays On	Gra	phs		Default	
VEN	Hot Standby	Off		Firev	vall	Off	WiFi	On		Man	agement		Default	
IPsec														
GRE	Radio			?		ETH	?		COM					?
Diagnostia											COM 1		COM 2	
Diagnostic	<ul> <li>Radio protocol</li> </ul>		Flexible			IP	192.168.141.239		Туре		RS232	-	RS232	-
Neighbours	IP		10.10.10.	2		Mask	255.255.255.0		Baud rat	e [bps]	19200	-	19200	-
Statistic	Mask		255.255.2	255.0		DHCP	Off		Data bits		8	-	8	-
Cranha	<ul> <li>TX frequency</li> </ul>	P	436.360.0	00		Shaping	Off		Parity		None	-	None	-
Graphs	RX frequency	Ľ	436.360.0	00		Speed	Auto 👻		Stop bits		1	-	1	-
Ping	Channel spacing [	kHz]	25.0	-		Modbus TCP	Off		Idle [byte	s]	5		5	
Monitoring	Modulation rate [kt	ops]	83.33   16	DEQAM		Terminal servers	Off		MRU (byt	es]	1600		1600	
-	RF power [W]		0.5	-		TCP proxy	Off		Flow cor	itrol	None	-	None	-
Maintenance	<ul> <li>Optimization</li> </ul>		Off	*		ARP proxy & VLA	N On		Protocol		None		None	
	Encryption		Off											
	<ul> <li>MTU [bytes]</li> </ul>		1500											

#### Fig. 4.1: RipEX2-Remote settings

The Settings menu is the same as on the Centre station except for the following:

- Unit name: RipEX2-Remote
- Radio IP: 10.10.10.2/24
- ETH IP: 192.168.141.239/24
- ARP Proxy & VLAN: On

ARP Proxy & VLAN menu must be opened and configured. Set the Alias IP address for the Ethernet interface. We simulate several subnets behind local RipEX's Ethernet (or SLIP protocol).

#### NOTE:

That is not necessary for GRE functionality; it is just used to show this configuration option.

ARP proxy & VI	LAN						
ARP proxy & VLAN	On 💌						
	ID/MA SK	Priority	Unit Manag	APD provid	Noto	Activo	Modify
Interface.VLAN ID	IP/MASK	Priority	Unit Manag.	ARP proxy	Note	Active	Modify
Interface.VLAN ID	IP/MASK	Priority	Unit Manag.	ARP proxy	Note Main interface	Active	Modify Add Subnet

Fig. 4.2: RipEX2-Remote ETH Alias/Subnet

To set and enable this alias, you need to click on the "Add Subnet" button and fill in the 172.20.20.1/30 subnet into the "IP/MASK" field.

Status	Values from: RipEX2-Ren	note		Fast	remote access
Vizards					
ettings	GRE				
outing	GRE	On 💌			
'PN	GRE tunnels				
IPsec	Peer address	Tunnel IP/MASK	Note	Active	Modify
	192.168.131.238	10.2.2.1/31		~	Delete Add
> GRE					Add
iagnostic					
Neighbours					
Statistic		Apply	Cancel		

Fig. 4.3: RipEX2-Remote GRE tunnel configuration

Set the Peer IP to the RipEX1-Base Ethernet IP address – 192.168.131.238. The GRE subnet must correspond to the Centre settings, i.e. choose the second IP address within a given subnet – 10.2.2.1/31.

Status	Values from: RipEX2-R	lemote				Fast remo	e access ?
Wizards							
Settings	Interfaces						?
Routing	Radio MAC 00:02	2:A9:BB:0F:AB	IP 10.10.10.2	Mask 25	5.255.255.0		
VPN	ETH MAC 00:02	2:A9:BB:0B:C3	IP 192.168.141.239	Mask 25	5.255.255.0	VLAN & GRE tunr	Subnets 🔻 Iels 🔻
IPsec							
GRE	Routes						?
UNL	Destination	Mask	Gateway	Backup	Note	Active	Modify
Diagnostic	192.168.131.0/24	255.255.255.0	192.168.141.254	Off	RipEX1-Base	✓	▼ Delete Add
Mainhhaunn	192.168.131.16/32	255.255.255.255	10.2.2.0	Off	Server GRE	~	▲ ▼ Delete Add
Neighbours	172.20.20.4/30	255.255.255.252	10.10.10.4	Off	RipEX4 Alias	~	▲ ▼ Delete Add
Statistic	172.16.200.0/24	255.255.255.0	10.10.10.4	Off	RipEX4 LAN	~	Delete Add
Graphs	Default		0.0.0.0	Off			Add

Fig. 4.4: RipEX2-Remote routing rules

The last step is to configure Routing rules.

- 192.168.131.0/24, Gateway 192.168.141.254
  - This rule depends on your L3 infrastructure, but in our example, we use the rule to route data for 192.168.131.0/24 network via local gateway.
- 192.168.131.16/32, Gateway 10.2.2.0
  - The route using the GRE tunnel packets for the Server (192.168.131.16) are encapsulated into the GRE. You might configure other destinations within this subnet if required, but not 192.168.131.238 (RipEX Ethernet – Peer IP, i.e. RipEX1-Base).
- 172.16.200.0/24 a 172.20.20.4/30, Gateway 10.10.10.4
  - Data for subnets behind RipEX4-Remote are routed to its 10.10.10.4 Radio IP address (i.e. not using GRE tunnel).

# 5. RipEX3-Remote Configuration

Status	Values from: RipE	X3-Remote	;						Fastre	mote	access	?
Wizards												
Settings	Device											?
Routing	Unit name	RipEX3-Remo	te T	ïme	Manual	Alarm management	Default	Ne	eighbours&Statis	tics	Default	
VPN	Operating mode	Router	× 5	NMP	Off	Power management	Always	On Gr	raphs		Default	
IPsec	Hot Standby	Off	F	irewall	Off	WiFi	On	Ma	anagement		Default	
GRE	Radio		?		ETH	?		COM's				?
Diagnostia									COM 1		COM 2	
Diagnostic	<ul> <li>Radio protocol</li> </ul>	Flexib	le		IP	172.16.100.200		Туре	RS232	•	RS232	-
Neighbours	IP	10.10	10.3		Mask	255.255.255.0		Baud rate [bps]	19200	•	19200	-
Statistic	Mask	255.25	55.255.0		DHCP	Off		Data bits	8	•	8	-
Granhe	<ul> <li>TX frequency</li> </ul>	436.36	60.000		Shaping	Off		Parity	None	-	None	-
Orapits	RX frequency	436.36	60.000		Speed	Auto 👻		Stop bits	1	•	1	-
Ping	Channel spacing [kł	Hz] 25.0		~	Modbus TCP	Off		Idle [bytes]	5		5	
Monitoring	Modulation rate [kbp	os] 83.33	16DEQA	м	Terminal servers	Off		MRU [bytes]	1600		1600	
	RF power [W]	0.5		-	TCP proxy	Off		Flow control	None	•	None	-
Maintenance	<ul> <li>Optimization</li> </ul>	Off	1		ARP proxy & VLA	AN Off		Protocol	None		None	
	Encryption	Off										
	<ul> <li>MTU [bytes]</li> </ul>	1500										

### Fig. 5.1: RipEX3-Remote unit settings

Configure a correct Unit name and ETH/Radio IP addresses. There is no Alias IP address.

Status	Values from: RipEX3-R	emote				Fast remote	access ?
Wizards							
Settings	Interfaces						?
Routing	Radio MAC 00	:02:A9:AC:0C:BD	IP 10	.10.10.3	Mask 255.25	5.255.0	
VPN	ETH MAC 00	:02:A9:AC:08:D5	IP 17	2.16.100.200	Mask 255.25	5.255.0	
IPsec	Routes						?
CPE	Destination	Mask	Gateway	Backup	Note	Active	Modify
UNL	192.168.131.0/24	255.255.255.0	10.10.10.1	Off	Base	~	Delete Add
Diagnostic	Default		0.0.0.0	Off			Add

Fig. 5.2: RipEX3-Remote routing rules

There is only one Routing rule – 192.168.131.0/24 is routed to the central RipEX radio in the centre - IP 10.10.10.1

• 192.168.131.0/24, Gateway 10.10.10.1

## 6. RipEX4-Remote Configuration

Wizards         Settings       Device         Routing       Unit name       RipEX4-Remote       Time       Manual       Alarm management       Default       Neighbours&Statistics       Default         VPN       • Operating mode       Router       SNMP       Off       Power management       Alarm Management       Default       Neighbours&Statistics       Default         IPsec       GRE       Radio       Off       WiFi       On       Management       Default         Neighbours       IP       10.10.4       Firewall       Off       WiFi       On       Management       Default         Neighbours       IP       10.10.10.4       Firewall       Off       YP       Mask       255.255.255.0       DHCP       Type       RS232       RS232 <td< th=""><th>Status</th><th>Values from: RipEX</th><th>4-Remote</th><th></th><th></th><th></th><th></th><th>Fast ren</th><th>note access</th><th>?</th></td<>	Status	Values from: RipEX	4-Remote					Fast ren	note access	?
Settings       Device         Routing       Unit name       RipEX4-Remote       Time       Manual       Alarm management       Default       Neighbours&Statistics       Default         UPN       Operating mode       Router       SNMP       Off       Power management       Always On       Graphs       Default         IPsec       GRE       Radio       Off       Firewall       Off       WiFi       Management       Default       Default       Default         Neighbours       P       10.10.10.4       Firewall       P       172.16.200.200       P       Baud rate [bps]       19200	Wizards									
Routing       Unit name       RipEX4-Remote       Time       Manual       Alarm management       Default       Neighbours&Statistics       Default         IPsec       GRE       0       Off       Firewall       Off       Power management       Alarm management       Default       Neighbours&Statistics       Default         Neighbours       Graphs       Off       Firewall       Off       W/Fi       On       Management       Default       Management       Default       Default       Nene       Statistic       Statistic       Statistic       Statistic       Statistic       Statistic       Statistic       Staping       Off       Stapi	Settings	Device								?
VPN       • Operating mode       Router       SNMP       Off       Power management       Always On       Graphs       Default         IPsec       GRE       Off       Off       WiFi       On       Management       Default         Diagnostic       Radio protocol       Flexible       P       10.10.10.4       P       172.16.200.200       Type       RS232       R	Routing	Unit name Rip	pEX4-Remote	Time	Manual	Alarm management	Default	Neighbours&Statisti	cs Default	
IPsec       On       Management       Default         GRE       Radio       ?       Firewall       Off       WiFi       On       Management       Default         Diagnostic       Radio protocol       Flexible       P       172.16.200.200       Type       RS232       RS232       RS232         Neighbours       IP       10.10.10.4       Mask       255.255.255.0       Mask       255.255.255.0       DHCP       Off       Data bits       8       9       9	VPN	Operating mode     Re	outer 👻	SNMP	Off	Power management	Always On	Graphs	Default	
GRE       Radio       ?       ETH       ?       COM         Diagnostic       -       -       Radio protocol       Flexible       p       172.16.200.200       Type       RS232       RS232         Meighbours       p       10.10.10.4       Mask       255.255.255.0       DHCP       Off         Statistic       -       TX frequency       436.360.000       Shaping       Off       Data bits       8       8         Ping       -       Channel spacing [kHz]       25.0       Modulation rate [kbps]       83.33   16DEQAIM       Modbus TCP       Off       Terminal servers       Off       MRU [bytes]       1600       1600         Maintenance       Optimization       Off       Flow control       None       None       None	IPsec	Hot Standby 01	ff	Firewall	Off	WiFi	On	Management	Default	
Diagnostic       Radio protocol       Flexible       IP       172.16.200.200       Type       RS232       RS232       RS232         Neighbours       IP       10.10.10.4       Mask       255.255.255.0       Mask       255.255.255.0       DHCP       Off       Data bits       8       8         Graphs       • TX frequency       436.360.000       Shaping       Off       DHCP       Off       Data bits       8       8       8       8       8       1	GRE	Radio		?	ETH	?	COM			?
Neighbours       - Radio protocol       Flexible       IP       172.16.200.200       Type       RS232       RS232         Neighbours       IP       10.10.10.4       Mask       255.255.255.0       Baud rate [bps]       19200       19200         Statistic       Mask       255.255.255.0       DHCP       Off       Data bits       8       8         Graphs       - TX frequency       436.360.000       Shaping       Off       Data bits       8       8         Nonitoring       - RX frequency       436.360.000       Speed       Auto       Stop bits       1       1         Modulation rate [kbps]       83.33   16DE0AM       Terminal servers       Off       MRU [bytes]       1600       1600         RF power [W]       0.5       TCP proxy       Off       None       None       None         - Optimization       Off       ARP proxy & VLAN       On       None       None       None	Diagnostio							COM 1	COM	2
Neighbours         IP         10.10.10.4         Mask         255.255.255.0         Baud rate [bps]         19200 <t< td=""><td>Diagnostic</td><td><ul> <li>Radio protocol</li> </ul></td><td>Flexible</td><td></td><td>IP</td><td>172.16.200.200</td><td>Туре</td><td>RS232</td><td>▼ RS232</td><td></td></t<>	Diagnostic	<ul> <li>Radio protocol</li> </ul>	Flexible		IP	172.16.200.200	Туре	RS232	▼ RS232	
Statistic       Mask       255.255.255.0       DHCP       Off       Data bits       8       8         Graphs       • TX frequency       436.360.000       Shaping       Off       Data bits       8       8         Ping       • Channel spacing [kHz]       25.0       • Modulation rate [kbps]       83.33   16DEQAM       Modulation rate [kbps]       83.33   16DEQAM       Modulation rate [kbps]       83.33   16DEQAM       TCP proxy       Off       Idle [bytes]       5       5         Maintenance       • Optimization       Off       ARP proxy & VLAN       On       None       None       None         Iterryption       Off       Iterryption       Off       ARP proxy & VLAN       On       None       None	Neighbours	IP	10.10.10.4	4	Mask	255.255.255.0	Baud rat	e [bps] 19200	▼ 19200	
Graphs       +TX frequency       436.360.000       Shaping       Off       Parity       None       None         Ping       -RX frequency       436.360.000       436.360.000       Speed       Auto       Stop bits       1       1         Monitoring       -Channel spacing [kHz]       25.0       Modulation rate [kbps]       83.33116DEQAM       Terminal servers       Off       Idel [bytes]       5       5         Maintenance       -Optimization       Off       ARP proxy & VLAN       On       None       None       None         It but to table       4500       0ff       ARP proxy & VLAN       On       None       None       None	Statistic	Mask	255.255.2	55.0	DHCP	Off	Data bits	8	▼ 8	-
Nonitoring     Nonitoring     Alto     Stop bits     1     1       Monitoring     Modulation rate [kbps]     83.33   16DEQAM     Speed     Auto     Stop bits     1     1       Monitoring     Modulation rate [kbps]     83.33   16DEQAM     Terminal servers     Off     MRU [bytes]     5     5       Maintenance     Optimization     Off     ARP proxy & VLAN     On     None     None	Graphs	<ul> <li>TX frequency</li> </ul>	436.360.0	00	Shaping	Off	Parity	None	▼ None	-
Ping     • Channel spacing [kHz]     25.0     Modbus TCP     Off       Monitoring     Modulation rate [kbps]     83.33   16DEQAM     Terminal servers     Off       Maintenance     0.5     TCP proxy     Off       • Optimization     Off     ARP proxy & VLAN     On       • Incryption     Off     None		RX frequency	436.360.0	00	Speed	Auto 💌	Stop bits	1	▼ 1	-
Monitoring     Modulation rate [kbps]     83.33   16DEQAM     Terminal servers     Off       Maintenance     RF power [W]     0.5     TCP proxy     Off       • Optimization     Off     ARP proxy & VLAN     On       • Encryption     Off     1500	Ping	Channel spacing [kHz	[] 25.0	-	Modbus TCP	Off	Idle [byte	s] 5	5	
Maintenance     RF power [W]     0.5     TCP proxy     Off     Flow control     None     None       • Optimization     Off     •     ARP proxy & VLAN     On     Protocol     None     None       • Encryption     Off     •     1500     1500     •     •     •	Monitoring	Modulation rate [kbps]	83.33   16	DEQAM	Terminal servers	Off	MRU (by	tes] 1600	1600	
Optimization     Off     ARP proxy & VLAN     On     Protocol     None     None     None	Maintonanco	RF power [W]	0.5	-	TCP proxy	Off	Flow co	ntrol None	<ul> <li>None</li> </ul>	-
Encryption     Off     1500	Maintenance	<ul> <li>Optimization</li> </ul>	Off	-	ARP proxy & VL	AN On	Protocol	None	None	
1500		<ul> <li>Encryption</li> </ul>	Off							
• MIU [bytes]		<ul> <li>MTU [bytes]</li> </ul>	1500							

### Fig. 6.1: RipEX4-Remote settings

Configure the correct Unit name and Radio/Ethernet IP addresses.

ARP proxy & VL	AN						?
ARP proxy & VLAN	On 💌						
Interface.VLAN ID	IP/MASK	Priority	Unit Manag.	ARP proxy	Note	Active	Modify
ETH0	172.16.200.200/24		~		Main interface		Add Subnet
	172.20.20.5/30					~	Delete
						A	Add VLAN
			ОКС	ancel			

Fig. 6.2: RipEX4-Remote ETH Alias/Subnet configuration

Click on the "Add Subnet" button to add the alias IP. Fill in the 172.20.20.5/30 and click on the "OK" button.

Status	Values	Values from: RipEX4-Remote							Fast remote access ?					
Wizards														
Settings	Interf	aces												7
louting	Radio MAC 00:02:A9:BA:73:6B				IP 10.10.10.4 Mask			255.255.255.	255.255.255.0					
/PN	ETH	MAC	00:02:A9:B	A:6F:83		IP 172.16.20	0.200	Masł	255.255.255.	0		VLAN & Su	ibnets 🔻	
IPsec	Route	es												1
CPE		Destination	ı	Mas	sk	Gatewa	ay	Backup		Note		Active	Modify	
URE	192.168.131.0/24		2	255.255.255.0		10.10.10.2		Off	RipEX	RipEX1-Base		~	Delete Add	d
Diagnostic	Default					0.0.0		Off					Ade	₫
Neighbours	Back	ar												
Statistic									Alteri	native pat	hs			
Granhs	Name	Peer IP	Hyster	esis [s]	SNMP	Notification	HW	Alarm Output	Gateway	Policy	Active	Note	Modify	
orapito													Add	
Ping	Logond	Lin D		nknown	Currenth	used.								
Monitoring	Legenu	OP L	Jown O		currenti	y ubeu								
laintonanao			Apply	Cane	el	Route for IP:		Find	Check rou	iting				

Fig. 6.3: RipEX4-Remote routing rules

There is only one routing rule – 192.168.131.0/24 is routed to the RipEX2-Remote Radio IP address. There is no GRE tunnel used. Data for 192.168.131.16/32 server will be encapsulated on RipEX2-Remote unit and routed via GRE tunnel over the Ethernet.

• 192.168.131.0/24, Gateway 10.10.10.2

### 7. Testing

The simplest way is to verify the connectivity via ICMP ping, e.g. a ping from RipEX4-Remote to the server connected to the RipEX radio in the centre - 192.168.131.16.

Go to the Diagnostic/Ping menu in the RipEX4-Remote unit. Choose the ICMP type and fill in the Destination IP (192.168.131.16). Other parameters might stay in default values.

Status	Values from: RipEX4-Remote	Fast remote access ?
Wizards		
Settings	Ping	?
Routing	Ping Type ICMP Length (bytes) 80 Period (ms)	1000
VPN	Destination 192.168.131.16 Count 5 Timeout [ms]	10000
IPsec	PING 192.168.131.16 (192.168.131.16) 80(108) bytes of data.	
GRE	88 bytes from 192.168.131.16: icmp_req=1 ttl=126 time=1466 ms 88 bytes from 192.168.131.16: icmp_req=2 ttl=126 time=862 ms	
Diagnostic	88 bytes from 192.168.131.16: icmp_req=3 ttl=126 time=703 ms 88 bytes from 192.168.131.16: icmp_req=4 ttl=126 time=665 ms	
Neighbours	88 bytes from 192.168.131.16: icmp_req=5 ttl=126 time=665 ms	
Statistic	192.168.131.16 ping statistics	
Graphs	<pre>5 packets transmitted, 5 received, 0% packet loss, time 4001ms rtt min/avg/max/mdev = 665.497/872.816/1466.733/305.750 ms, pipe 2</pre>	
> Ping		
Monitoring	Start   Shar	
Maintenance		

Fig. 7.1: Ping from RipEX4-Remote to the server connected to the radio in the centre

The ICMP ping proved the remote server accessibility. But how can we make sure the packets are encapsulated to GRE? Login to the RipEX1-Base unit and choose the Diagnostic/Monitoring menu. Set the parameters as depicted on Fig. 7.2 below and click on the "Start" button. Afterwards, execute the ping requests from RipEX4-Remote unit.

Status	Values from: RipEX1-Base ?
Wizards	
Settings	Monitoring ?
Routing	RADIO COM1 COM2 ETH V Internal hide params
VPN	ETH
IPsec	Rx V TX V Display HEX V Offset [bytes] 0 Length [bytes] 0
GRE	IP src 0.0.0.0/0 IP dst 0.0.0.0/0 Port src 0 Port dst 0 Include reverse
Diagnostic	Protocol type: all UDP TCP ICMP ARP Other
Neighbours	ETH Headers Off v Management traffic Off v
Statistic	Advanced parameters
Graphs	User rule <sup>r</sup> ip proto 47'
Pina	Tcpdump command tcpdump -n -i eth0 -tt -I -Z nobody ( ip proto 47 ) and ( not(udp or tcp or icmp or arp) ) and not(tcp port 22 or 80 or 443 or 8889)
> Monitoring	Show time diff. File period: 5 min 💌 File size: 100 kB 💌
Maintenance	15:53:09.178503 [ETH] IP 192.168.141.200 > 192.168.131.238: GREv0, length 112: IP 172.16.200.200 > 192.168.131.16 ICMP echo request, id 2997, seq 1, length 88
	ICMP echo reply id 2997, seq 1, length 88 15:53:10.156432 [ETH] IP 192.168.141.200 > 192.168.131.238: GREv0, length 112: IP 172.16.200.200 > 192.168.131.16: ICMP echo request id 2997, seq 2 length 88
	15:53:10.157681 [ETH] IP 192.168.131.238 > 192.168.141.200: GREv0, length 112: IP 192.168.131.16 > 172.16.200.200: ICMP echo reply, id 2997, seq 2, length 88
	15:53:11.168424 [ETH] IP 192.168.141.200 > 192.168.131.238: GREv0, length 112: IP 172.16.200.200 > 192.168.131.16: ICMP echo request, id 2997, seq 3, length 88
	15:53:11.169794 [ETH] IP 192.168.131.238 > 192.168.141.200: GREv0, length 112: IP 192.168.131.16 > 172.16.200.200: ICMP echo reply, id 2997, seq 3, length 88
	15:53:12.188484 [ETH] IP 192.168.141.200 > 192.168.131.238: GREv0, length 112: IP 172.16.200.200 > 192.168.131.16: ICMP echo request, id 2997, seg 4, length 88
	15:53:12.189544 [ETH] IP 192.168.131.238 > 192.168.141.200: GREv0, length 112: IP 192.168.131.16 > 172.16.200.200:
	15:53:13.156361 [ETH] IP 192.168.141.200 > 192.168.131.238: GREv0, length 112: IP 172.16.200.200 > 192.168.131.16: ICMP echo request, id 2997, seq 5, length 88
	15:53:13.157545 [ETH] IP 192.168.131.238 > 192.168.141.200: GREv0, length 112: IP 192.168.131.16 > 172.16.200.200: ICMP echo reply, id 2997, seq 5, length 88
	Start         Stop         Clear         File Start         File Status         Download

Fig. 7.2: Monitoring parameters and monitoring output

The packet length might be set to be 0 Bytes, because the payload is not important now. To display only GREv0 packets, define the advanced parameter as 'ip proto 47' (GRE protocol port).

#### NOTE:

The GRE interface might be monitored directly using the '-i gretun0' advanced parameter.

The ICMP packets are displayed in the output as GREv0 packets. There is no encryption and thus the packets are readable.

You can try to test accessibility of other units. The principle is the same.

Accessibility issues might be caused by:

- Missing routing rules (or default gateway, ...) on one of the computers
- Enabled firewall blocking the incoming ICMP requests
- · Misconfigured routing rules or GRE tunnels in RipEX units
- Etc...

# Appendix A. Revision History

Revision 1.0 First issue 2017-11-07