

Application notes



version 1.1 2024-03-12

Table of Contents

1. RipEX2 - GRE TAP tunneling	. 5
1.1. Configuration	. 5
1.1.1. RipEX A	. 5
1.1.2. RipEX B	. 8
1.1.3. Diagnostics and tests	. 8
1.1.4. L2 Forward Firewall	11
Revision History	15

1. RipEX2 - GRE TAP tunneling

GRE L2 tunnel captures Ethernet frames of the bridge and sends them to the other end of the tunnel. It is linked up to the RipEX2 internal bridge (LAN interface) as one of the bridge's ports. It enables to build bridges via the complex routed infrastructured networks and combines the local partial segments into one network segment.

We had a so-called ARP proxy functionality in RipEX radios. Proxy ARP is a technique by which a proxy server (local RipEX) at given network answers via the Address Resolution Protocol (ARP) queries for an IP address that is not on that local network segment. This functionality is not implemented in RipEX2, but with the GRE TAP tunnelling feature, advanced native full transparent Layer2 (Ethernet) connectivity over the Layer3 Radio network can be achieved.

GRE L2 tunnel can be used to natively transport IPv6 traffic, GOOSE messaging, multicast, VLAN double-tagged packets – QinQ 802.1ad or single tagged 802.1q over the RipEX2 IPv4 network.



1.1. Configuration

Fig. 1.1: GRE TAP tunnel diagram

1.1.1. RipEX_A

Start with RipEX2 units in factory settings. From this point, do the following changes. Go to the Device – Unit menu and set the Unit name. You can also update time in the device so that debugging is easier afterwards (time synchronization).

RipEX2 - GRE TAP tunneling

RipEX2 NoName @10.9.8.7	1 ⁰⁴ 1 Remote access	
Unit time: 2021-12-28 07:37:22 (UTC+0)	General Service US	GB Time Hot standby
 STATUS SETTINGS Interfaces Routing 	Unit name RipEX_A Unit note Unit location Unit contact	
Firewall VPN Security Device	3 All infor	mation above is used in SNMP device info.

Fig. 1.2: RipEX_A Device unit

RipEX2 NoName @192.168.169.169	I ⁰ I Remote access	UNIT
Unit time: 2021-10-13 13:28:04 (UTC+0)	General Service USB Time Hot standby	
Ø STATUS	Status NTP state not synced Texture of former	
hterfaces	Stratum 16 Delay [ms] 0.000 Dispersion [ms] 1.770	
Routing Firewall	Time Change device time manually 2021-10-13 13:28:05 Update in device Vse bro	wser time
Security	NTP client synchronization source NTP server	
Device	NTP server minimum polling time 1 min. v	
Unit	Time zone Europe/Prague 👻	
Configuration Events SNMP Software keys	Table does not contain any data. Add NTP server	
Firmware	T ADD IVIT Server	

Fig. 1.3: RipEX_A Device – Unit – Time

Go to the SETTINGS – Interfaces – Ethernet and set the 192.168.1.1/24 IP address.

RipEX2 NoName @192.168.1	169.169 I ^{lly} I Remote access
Unit time: 2021-10-13 13:37:26 (UTC+0)	ETH1 • ETH2 • ETH3 • ETH4 • ETH5 •
⊘ STATUS	Status
🍫 SETTINGS	ETH1: • - Attached - Router mode
Interfaces	Network interface
Ethernet	Name bridge bridges: ETH 1, ETH 2, ETH 3, ETH 4
Radio COM	Allow unit management
Terminal servers	LAN
Routing	IP / Mask 192.168.1.1/24 Note

Fig. 1.4: RipEX_A – Interfaces – Ethernet

Change the Radio interface configuration.

• Mode	Router
Radio protocol	Flexible (can be BDP as well)
Radio / IP mask	10.10.1/24
TX / RX frequencies	Set to any value appropriate to you
Modulation type	QAM (you can use FSK as well, but set the same in RipEX_B)
Modulation	64QAM (choose to suit your needs)

	1 ⁹ 1 Remote access	RADIC		🔍 🔳 Chang	ges 💌 Notific	ations
Unit time: 2021-12-28 07:38:21 (UTC+0)	Status					<
	Radio interface			Radio parameter	s	
STATUS	Mode	Router	*	TX frequency [Hz]	415500000	0
🗘 🖧 SETTINGS	IP / Mask	10.10.10.1/24		RX frequency [Hz]	415500000	\$
Interfaces	Allow unit management	On	*	Antenna configuration	Single (Tx/Rx)	*
Ethernet	Radio protocol			RF power PEP [dBm]	20	*
Radio	Radio protocol	Flexible	*	Channel spacing [kHz]	25	*
COM	ACK	On	*	Occupied bandwidth limit [kHz]	16	*
Terminal servers	Retries [No]	3	\$	Modulation type	QAM	*
Routing	Foreign packets RSS threshold [-dBm]	120	0	Modulation	64QAM	*
Firewall	Repeat COM broadcast	Off	*	FEC	Off	*

Fig. 1.5: RipEX_A Interfaces - Radio

Go to the VPN – GRE menu and set the L2 GRE TAP tunnel. The only parameter is the Peer address equal to 10.10.10.9 (RipEX_B radio IP).

Add		×
I	Active	
Peer address	10.10.10.9	
Interface	bridge	*
MTU	1462	\diamond
Note	Key enabled	
Confirm a	and close Close	

Fig. 1.6: RipEX_A GRE TAP configuration

Save all the changes and do similar steps in RipEX_B.

1.1.2. RipEX_B

RipEX_B configuration is the same as in RipEX_A so you can upload the saved configuration from RipEX_A to RipEX_B and then change the following parameters:

Unit name	RipEX_B
Ethernet IP	192.168.1.9/24
• Radio / IP mask	10.10.10.9/24
GRE TAP Peer IP	10.10.10.1

1.1.3. Diagnostics and tests

The most basic example is to run ICMP ping from RipEX2 GUI, or you can run an ICMP from connected devices as well.

Go to the RipEX_A or RipEX_B Diagnostics – Tools menu and select ICMP ping tab. Fill in the Destination IP. In this example, local accessed unit is RipEX_B and ping is run against 192.168.1.1 IP address.

	ote access	TOOLS		■ Changes 🕫 No	tifications
Unit time: 2021-12-21 14:58:35 (UTC+1)	ICMP ping	RSS ping Routing	RF transmission test	Antenna detection	
STATUS SETTINGS US DIAGNOSTICS	Parameters Destination IP 1 Period [ms] 100 Count 5	92.168.1.1 🔅 Leng	th [8] 200 t (ms] 10000 anual V Source	e IP	
Overview Events	Controls Start			🛓 Download	1 Clear
Statistics Monitoring Routing	Output No received	data yet.			
Tools					

Fig. 1.7: RipEX_B ICMP ping to RipEX_A 192.168.1.1

Click on the Start button and you should see a similar output.

PING 192.168.1.1 (192.168.1.1) from 192.168.1.9 : 200(228) bytes of data.

208 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=110 ms

208 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=82.2 ms

208 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=119 ms

208 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=101 ms

208 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=119 ms

--- 192.168.1.1 ping statistics ----

5 packets transmitted, 5 received, 0% packet loss, time 4005ms

rtt min/avg/max/mdev = 82.299/106.792/119.951/14.101 ms

In a Diagnostics – Monitoring menu, you can verify that packets are encapsulated to GRE. Enable Radio interface monitoring for all on the Radio channel. You can set the Length parameter to 0 Bytes so that more lines fit into one console output.

You should see similar GRE traffic in your output (you can run another ICMP ping from a 2nd window).

14:55:59.565152 [RF:phy:tx] IP 10.10.10.9 > 10.10.10.1 GRE, length:284

14:55:59.619935 [RF:phy:rx] IP 10.10.10.1 > 10.10.10.9 GRE, length:284, rss:74 mse:36

14:56:04.624331 [RF:phy:tx] IP 10.10.10.9 > 10.10.10.1 GRE, length:84

14:56:04.877228 [RF:phy:rx] IP 10.10.10.1 > 10.10.10.9 GRE, length:84, rss:74 mse:36

14:56:04.913019 [RF:phy:tx] IP 10.10.10.9 > 10.10.10.1 GRE, length:83

14:56:04.977027 [RF:phy:rx] IP 10.10.10.1 > 10.10.10.9 GRE, length:83, rss:74 mse:37

Once all of this is working fine, you can test traffic which is most important for you - such as

- VLAN double-tagged packets
- IPv6
- Multicast
- GOOSE
- ...

1.1.4. L2 Forward Firewall

Every single packet is now being transferred over the Radio channel which has a limited bandwidth. Very often, you may need to limit forwarded traffic - e.g. allowing multicast and ARPs, but disabling IPv6.

Since the 2.1.6.0 firmware, you can configure the L2 forward firewall so it e.g. denies all the multicast data, IPv6 etc.

Within this example, L2 Forward firewall will block the traffic coming to the RipEX2 via any of its ETH ports and being forwarded to 'any' interface (especially the 'radio' interface). The denied traffic is going to be IPv6 and multicast. ARP data are also multicast packets, for a proper L2 functionality, the 1st rule enables ARP data.

Go to the SETTINGS >	Firewall > L2 > For	ward menu. Add the	1 st rule enabling	ARP data.
			J	

Edit forward rule	×
Enable rule	 ✓
Only VLAN	Off 🖌
Ethernet protocol	ARP 🖌
Source MAC filter	All 🖌
Destination MAC filter	All
Input port	All ETH 🗸
Output port	All 🗸
Select bridge	Off 🖌
Activation limit	Off 🖌
ARP OpCode	All
ARP source IP/mask	0.0.0/0
ARP destination IP/mask	0.0.0/0
Action	Allow 🗸
Note	Allow ARP
Confirm and close	Close

Fig. 1.8: Enabling ARP data

Add two other rules. Deny IPv6 data:

Edit forward rule		×
Enable rule	~	
Only VLAN	Off	~
Ethernet protocol	IPv6	~
Source MAC filter	All	~
Destination MAC filter	All	~
Input port	All ETH	~
Output port	All	~
Select bridge	Off	~
Activation limit	Off	~
Action	Deny	~
Note	Deny IPv6	
Confirm and close	Clo	ose

Fig. 1.9: Denying IPv6 data

Deny Multicast data:

Edit forward rule		×
Enable rule	~	
Only VLAN	Off	~
Ethernet protocol	All	~
Source MAC filter	All	~
Destination MAC filter	Multicasts	~
Input port	All ETH	~
Output port	All	~
Select bridge	Off	~
Activation limit	Off	~
Action	Deny	~
Note	Deny multicast	
Confirm and close	Clo	se

Fig. 1.10: Denying multicast data

Send the changes to the unit and do the same in 2nd unit. Open the L2 firewall status and keep it being refreshed. Try some PING data being sent (allowed ARP packets). Try to do some Internet access from your laptop via the default gateway set to our RipEX2 Ethernet Network Interface. You should see the counters being increased.

RipEX2 - GRE TAP tunneling

RipEX2 RipEX_A @192.168.1.1) ^y I Remote access	L2
Unit time: 2024-02-26 11:06:13 (UTC+0)	Blocklist/Allowlist Forward	
😝 STATUS	Status	
🕨 🍫 SETTINGS	Firewall L2 tables Bridge table: filter	
Interfaces	Bridge chain: INPUT, entries: 0, policy: ACCEPT	
Routing	Bridge chain: FORWARD, entries: 1, policy: ACCEPT 1j forward_user, pcnt = 105 bcnt = 6598	
Firewall	Bridge chain: OUTPUT, entries: 0, policy: ACCEPT	
L2	Bridge chain: forward_user, entries: 3, policy: ACCEPT 1p ARP -i FTH+ -i RFTURN , pont = 4 bont = 184	
L3	2p IPv6 -i ETH+ -j DROP , pcnt = 12 bcnt = 912 3d Multicast -i ETH+ -i DROP , pcnt = 12 bcnt = 480	
NAT	,	

Fig. 1.11: L2 Forward Firewall status

Revision History

Revision 1.0 2022-01-17 First issue

Revision 1.1 2024-02-29 Added Section 1.1.4, "L2 Forward Firewall"