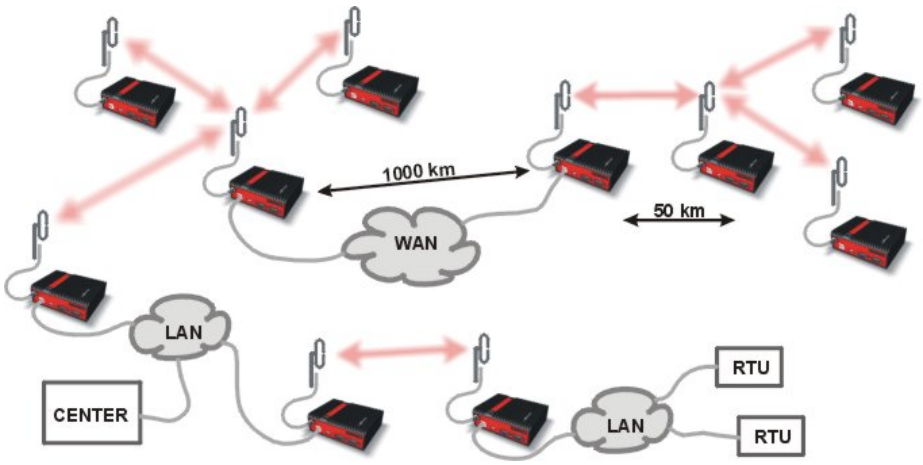
RACOM
RADIO DATA NETWORKS

Application notes



RipEX
IPsec

version 1.1
1/11/2018
fw 1.7.x.0

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

www.racom.eu

Table of Contents

1. Configuration of IPsec Tunnels in RipEX Units

- The IPsec tunnel can be established among all devices compatible with IPsec protocol (RipEX, CISCO, etc.). The following IPsec Basic Description is also available *in the RipEX manual*[1].

- **IPsec Basic Description**

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

  Although there are 2 modes of operation RipEX only offers Tunnel mode. In Tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet (ESP - Encapsulating Security Payloads) with a new IP header.

  Symmetrical cryptography is used to encrypt the packets. The symmetric keys must be safely delivered to the peer. In order to maintain a secure connection, symmetric keys must be regularly exchanged. The protocol used for secure key exchange is IKE (Internet Key Exchange). Both IKE version 1 and the newer version 2 are available in RipEX.

  IKE protocol communication with the peer is established using UDP frames on port 500. However, if NAT-T (NAT Traversal) or MOBIKE (MOBile IKE) are active, the UDP port 4500 is used instead.

  NOTE:
  NAT-T is automatically recognized by IPsec implementation in RipEX.

  The IPsec tunnel is provided by Security Association (SA). There are 2 types of SA:
  IKE SA: IKE Security Association providing SA keys exchange with the peer.
  CHILD SA: IPsec Security Association providing packet encryption.

  Every IPsec tunnel contains 1 IKE SA and at least 1 CHILD SA.

  Link partner (peer) secure authentication is assured using Pre-Shared Key (PSK) authentication method: Both link partners share the same key (password).

  As and when the CHILD SA expires, new keys are generated and exchanged using IKE SA.

  As and when the IKE SA version IKEv1 expires - new authentication and key exchange occurs and a new IKE SA is created. Any CHILD SA belonging to this IKE SA is re-created as well.

  As and when the IKE SA version IKEv2 expires one of two different scenarios might occur:
  If the re-authentication is required - the behavior is similar to IKEv1 (see above).
  It the re-authentication is not required - only new IKE SA keys are generated and exchanged.

For more details and parameters description, check the *RipEX manual*[2].

[1] http://www.racom.eu/eng/products/m/ripex/h-menu.html#IPsec
[2] http://www.racom.eu/eng/products/m/ripex/h-menu.html#IPsec

2. Configuration Example

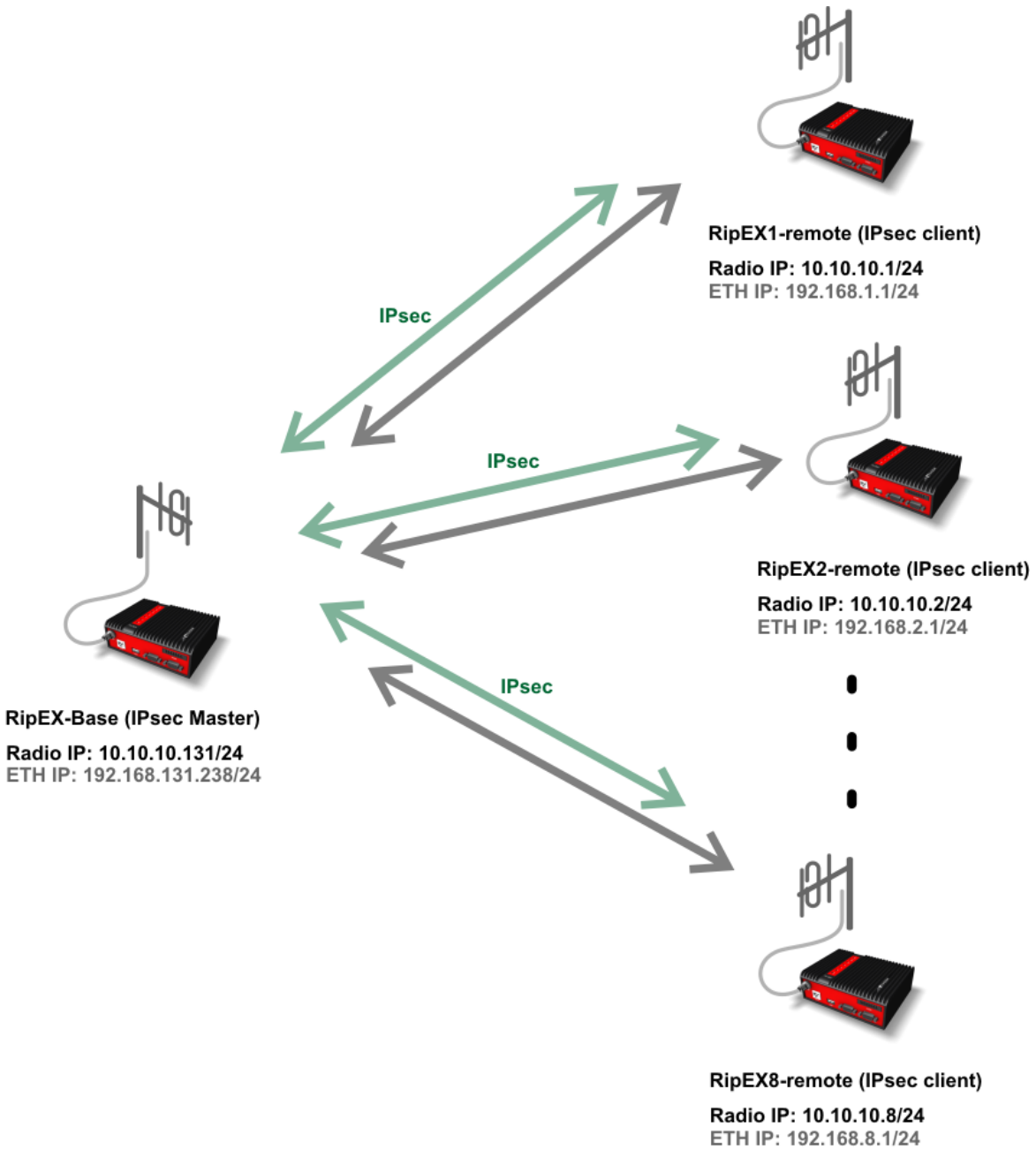


Fig. 2.1: Topology

RipEX supports up to 8 simultaneous IPsec tunnels, i.e. up to 8 tunnels can be established in a single RipEX unit; This is a hardware restriction. If you need more tunnels established in one unit, choose a different VPN concentrator such as Cisco, Fortigate etc.

In this example, one RipEX unit is configured as a 'Master / concentrator' with 8 tunnels to remote units. As there are only 3 RipEX units in a DEMO case, only 3 configurations of selected units will be described – the central RipEX (RipEX-Base) and two remote units (RipEX1-remote and RipEX8-remote). Configuration of other radios follows the same principles.

The configuration example shows IPsec connectivity between the Master station and both remote units, as well as IPsec communication between both remote units via this Master station.

3. RipEX-Base Configuration

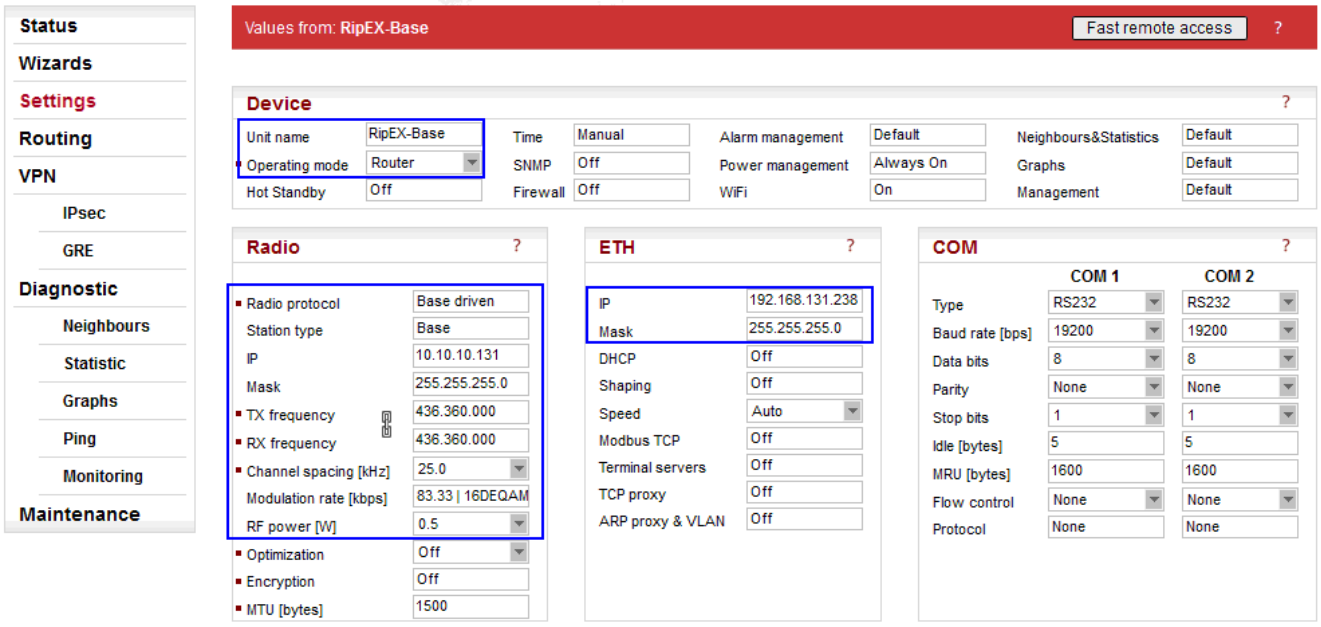


Fig. 3.1: RipEX-Base Settings

Parameters:

Unit name	“RipEX-Base”
Operating mode	“Router“ (IPsec cannot be used in the Bridge mode)
Radio protocol	“Base Driven“ (The protocol can also be set as “Flexible”, but this example utilizes the Base Driven Protocol, BDP)
Station type	“Base” (detailed configuration in Fig. 3.2 *RipEX-Base Radio protocol settings*)
IP/Mask	“10.10.10.131/24” (common subnet for all RipEX units in this example)
TX/RX frequency	“436.360.000 MHz” (configure any frequency, but the same among all RipEX units – simplex or duplex scenarios are both possible)
Channel spacing	“25 kHz” (configure any spacing, but this must be the same for all units)
Modulation rate	“83.33 | 16DEQAM” (use the same “type” for all units, but otherwise, configure as preferred)
RF power (W)	“0.5 W” (set the minimum possible RF power for tests using dummy loads on your desk – laboratory tests)
ETH IP/Mask	“192.168.131.238/24” (set the Ethernet IP/Mask)

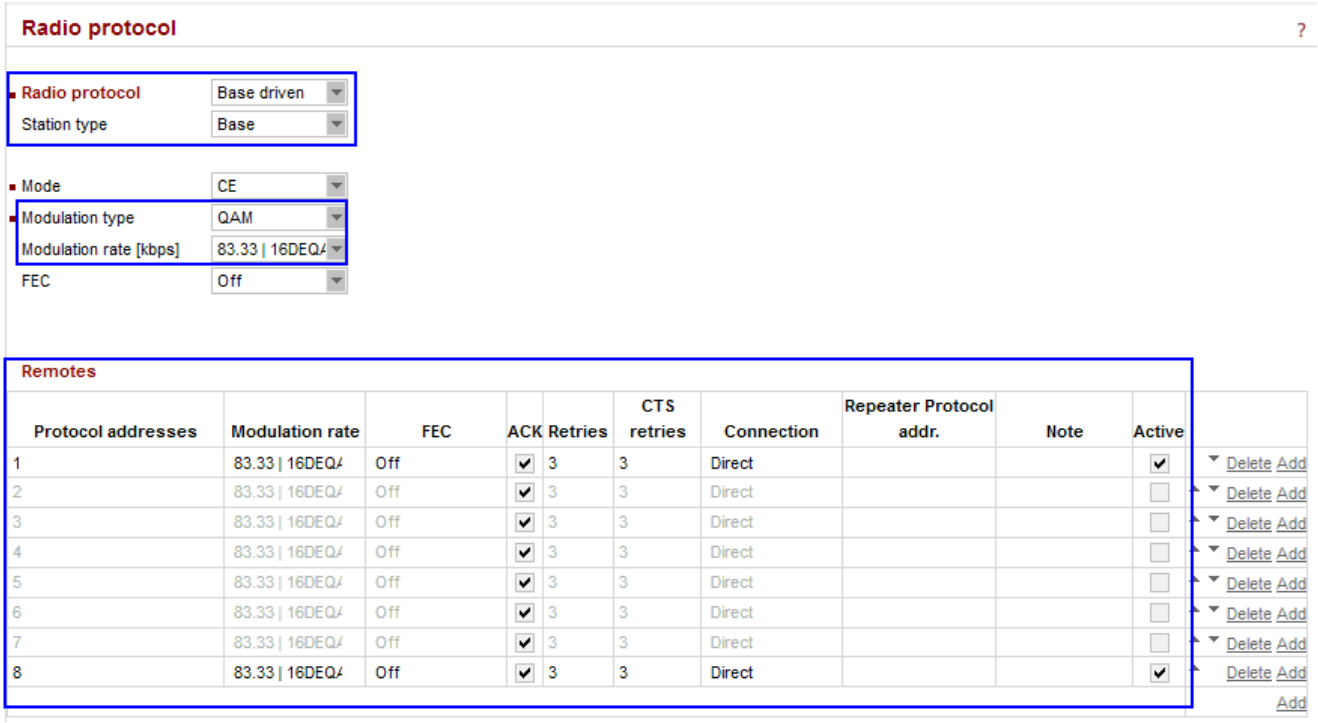


Fig. 3.2: RipEX-Base Radio protocol settings

Parameters:

Radio protocol	“Base driven”
Station type	“Base”
Modulation type	“QAM” (must be the same among all RipEX units)
Modulation rate	“83.33 kbps | 16DEQAM” (the default modulation rate)
Remotes	8 remote units are configured, but only 2 of them are activated due to the simplicity of this example. The Modulation rate can be set for each link individually, as well as FEC, ACK, Retries or CTS retries. The connection is “Direct” for all units.

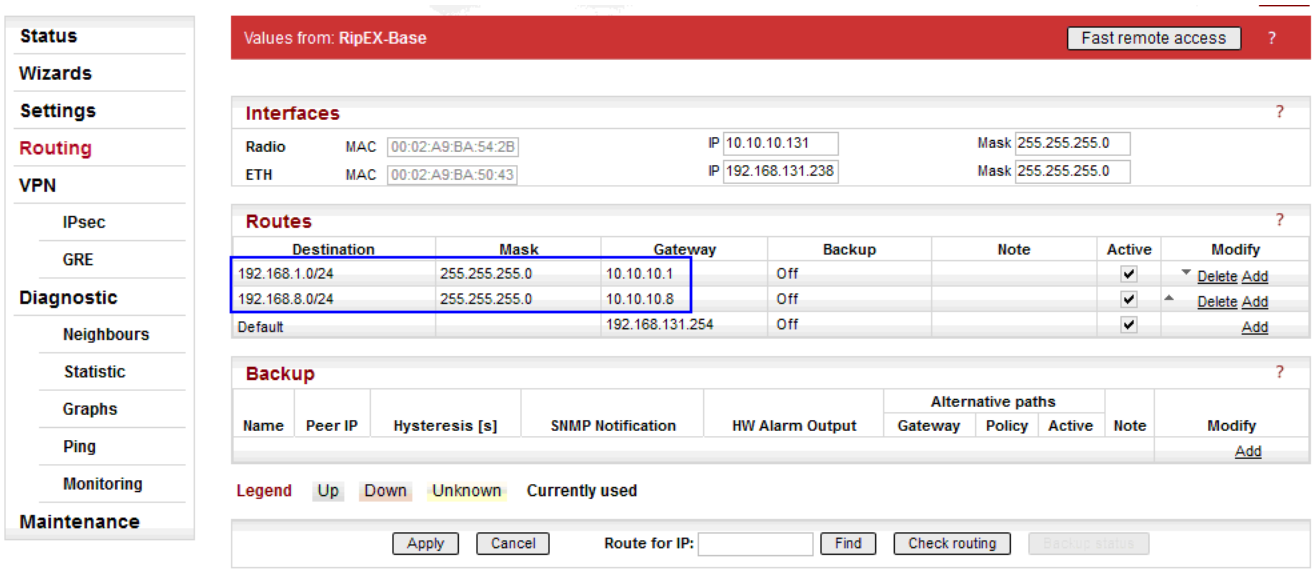


Fig. 3.3: RipEX-Base Routing

The Peer IP address can either be the Radio IP or Ethernet IP (if the remote end-point is RipEX). Correct routing rules must be configured for remote end-point accessibility, i.e. 192.168.1.1/32 and 192.168.2.1/32. Otherwise, RipEX-Base does not know a route to the other RipEX's Ethernet IPs.

In the following step (IPsec configuration), interconnection of local and remote subnets via IPsec tunnels will be configured. Correct routing MUST be configured, otherwise, the traffic between remote Ethernet subnets will be filtered and discarded. I.e. for each planned remote subnet which should be reachable via IPsec, a correct routing must be set.

If the IPsec is down, there are automatic firewall rules blocking such traffic to avoid unencrypted data being sent from the RipEX unit. In our example, if the tunnel is down, RipEX-Base blocks all the traffic coming from the 192.168.131.0/24 network to 192.168.1.0/24 and/or 192.168.8.0/24 networks. This traffic can only be forwarded if an IPsec tunnel is used (so it's up and running).

- 192.168.1.0/24 via 10.10.10.1 (connection to RipEX1-remote)
- 192.168.8.0/24 via 10.10.10.8 (connection to RipEX8-remote)

Once correct routing rules are connected on remote units, Ethernet-to-Ethernet connectivity is ready.

There is also a Default gateway configured (192.168.131.254). This route can be omitted completely if not required for any other purpose (e.g. accessibility of this unit via Ethernet from other subnets).

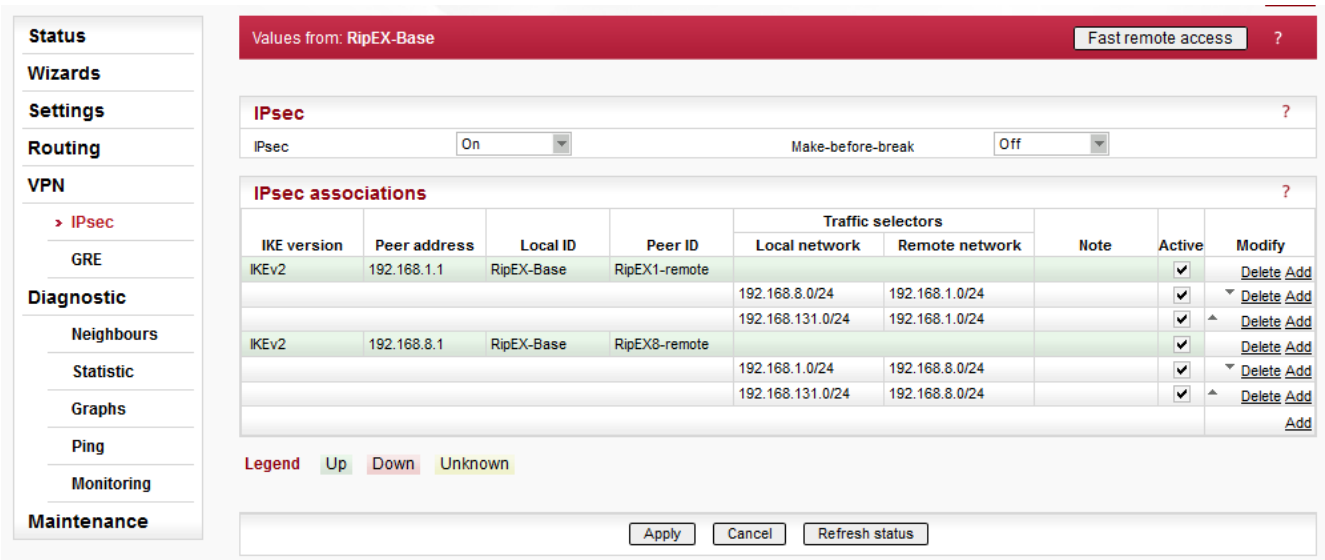


Fig. 3.4: RipEX-Base IPsec configuration summary

In Fig. 3.4, two IPsec associations are already configured and running. See Fig. 3.5 for the tunnel configuration. Both tunnels are configured in the same way.

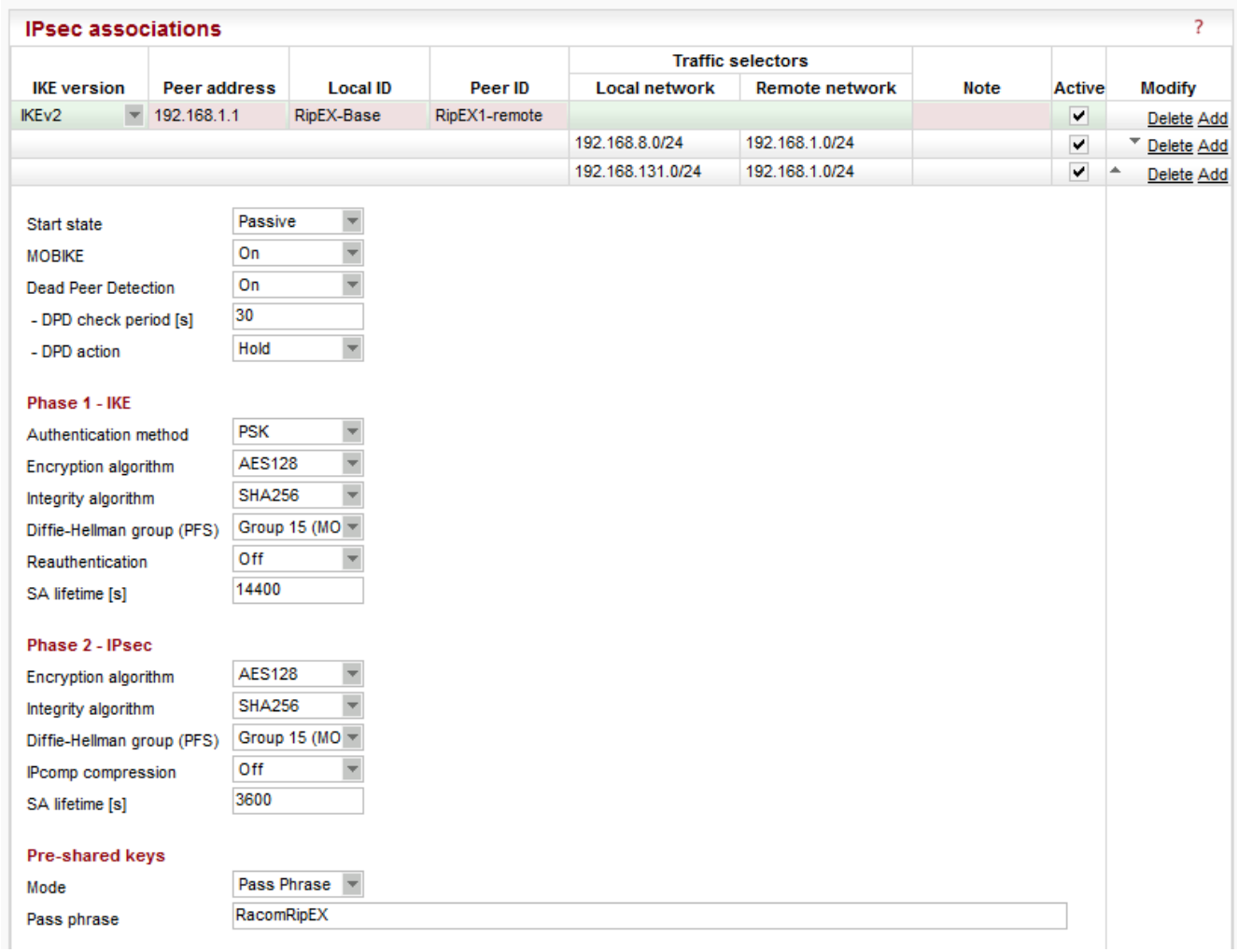


Fig. 3.5: RipEX-Base IPsec association configuration #1

Parameters:

IKE version	“IKEv2” (IKEv1 is also implemented)
Peer address	“192.168.1.1” (Ethernet IP address of "RipEX1-remote")
Local ID	“RipEX-Base”
Remote ID	“RipEX1-remote”
Traffic selectors	“192.168.8.0/24 (local) <-> 192.168.1.0/24” (a selector for RipEX1-remote and RipEX2-remote connectivity over IPsec) “192.168.131.0/24 (local) <-> 192.168.1.0/24” (a basic selector for Ethernet to Ethernet accessibility over IPsec)
Start state	“Passive” (it waits for incoming connections from remote units)
MOBIKE	“On” (default)

Dead Peer Detection	“On” (check every 30 seconds and if there is no accessibility of remote end-point, close the connection and wait for re-establishment, i.e. “Hold” option)

Phase 1 – IKE

Authentication method	“PSK”
Encryption algorithm	“AES128” (default)
Integrity algorithm	“SHA256” (default)
PFS	“Group 15” (default)
Reauthentication	“Off” (default)
SA lifetime [s]	“14400” (default)

Phase 2 – IPsec

Encryption algorithm	“AES128” (default)
Integrity algorithm	“SHA256” (default)
PFS	“Group 15” (default)
IPcomp compression	“Off” (default)
SA lifetime [s]	“3600” (default)

Pre-shared keys

Mode	“Pass phrase” (default)
Pass phrase	“RacomRipEX” (can be configured as required, but must be the same on both units)

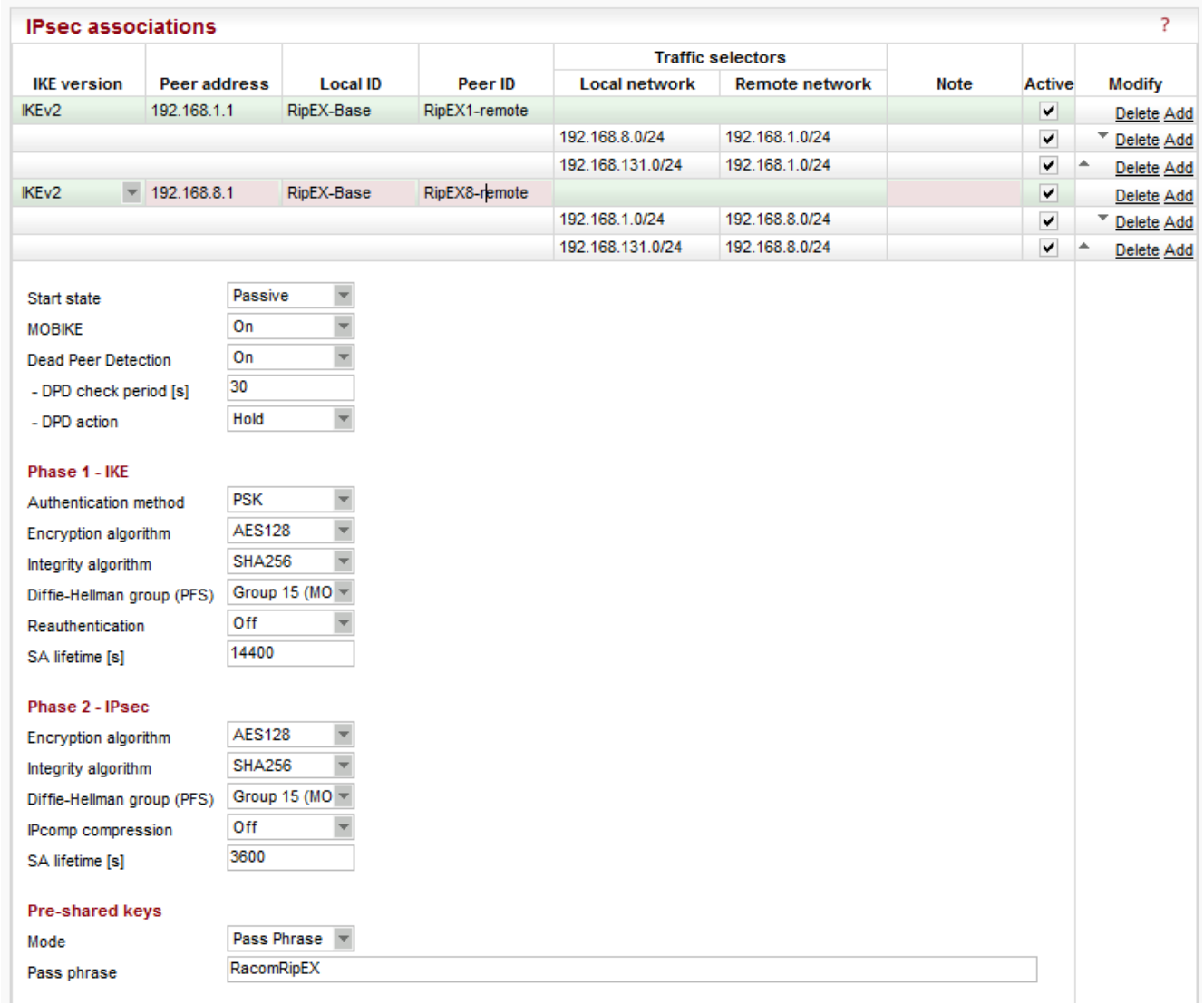


Fig. 3.6: RipEX-Base IPsec association configuration #2

The second tunnel has the same parameters except for:

Peer address	“192.168.8.1” ("RipEX8-remote" Ethernet IP)
Peer ID	“RipEX8-remote”
Traffic selectors	“192.168.1.0/24 (local) <-> 192.168.8.0/24” (a selector for RipEX1-remote and RipEX2-remote connectivity over IPsec)
	“192.168.131.0/24 (local) <-> 192.168.8.0/24” (a basic selector for Ethernet to Ethernet reachability over IPsec)

NOTE: The start states should not be “Start” at both tunnel end-points, because it might happen that both end-points will try to initiate the connection at the same time and thus create and delete SAs until resolved. Do not use a “Passive” mode at both end-points – no tunnel would be initiated at all.

Once configured and applied, the tunnels need the remote units to be configured as well, otherwise the tunnels cannot be established.

4. RipEX1-remote Configuration

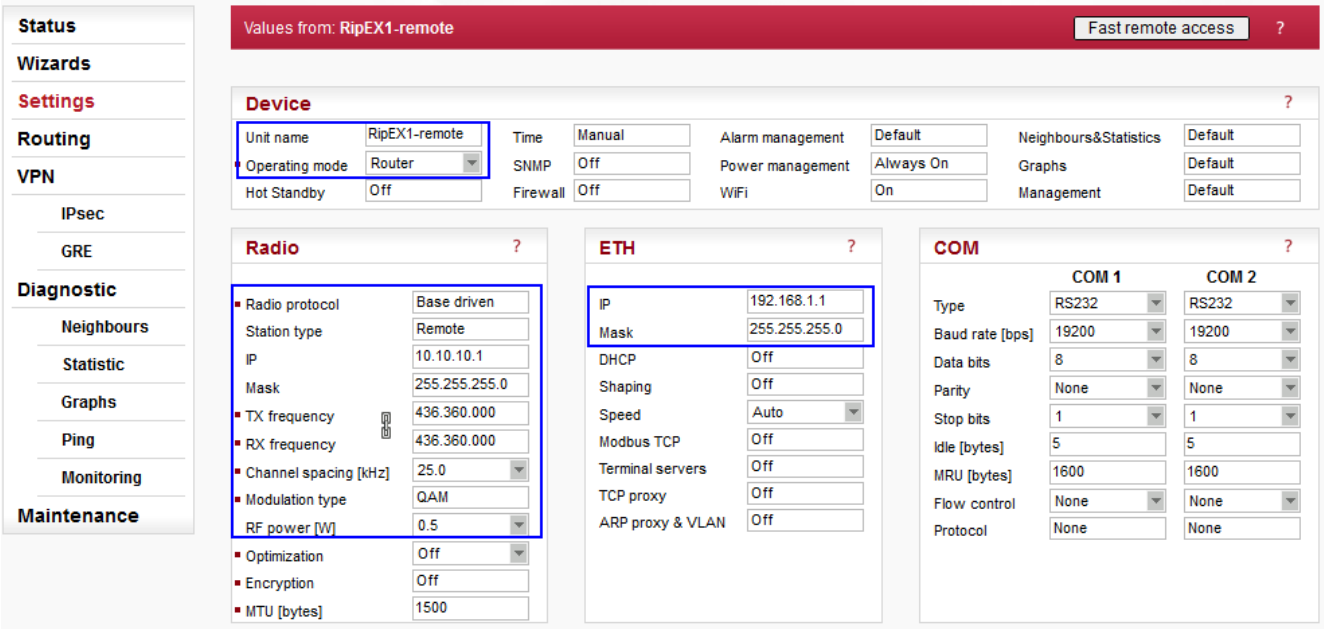


Fig. 4.1: RipEX-Base IPsec association configuration #2

Parameters:

Unit name	“RipEX1-remote”
Operating mode	“Router“ (IPsec cannot be used in the Bridge mode)
Radio protocol	“Base Driven“ (The protocol can also be set as “Flexible”, but this example utilizes the Base Driven Protocol, BDP)
Station type	“Remote” (detailed configuration in Fig. 4.2)
IP/Mask	“10.10.10.1/24” (common subnet for all RipEX units in this example)
TX/RX frequency	“436.360.000 MHz” (configure any frequency, but the same among all RipEX units – the simplex or duplex scenarios are possible)
Channel spacing	“25 kHz” (configure any spacing, but this must be the same for all units)
Modulation type	“QAM” (use the same “type” for all units, otherwise configure as preferred)
RF power (W)	“0.5 W” (set the minimum possible RF power for tests using dummy loads on your desk – laboratory tests)
ETH IP/Mask	“192.168.1.1/24” (set the Ethernet IP/Mask)

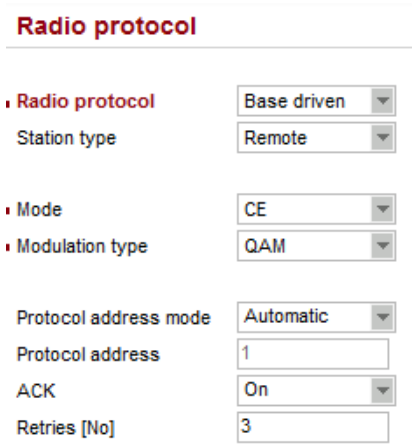


Fig. 4.2: RipEX1-remote BDP configuration

Parameters:

Radio protocol	“Base driven”
Station type	“Remote”
Modulation type	“QAM” (must be the same among all RipEX units)
Protocol address mode	“Automatic” (protocol address equals to the last Radio IP digit, i.e. “1”)
ACK	“On”
Retries	“3”

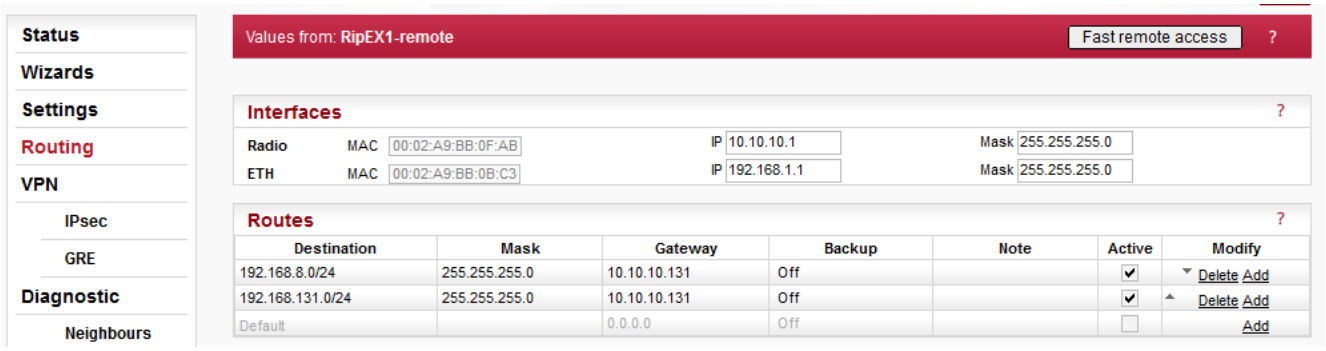


Fig. 4.3: RipEX1-remote Routing

Two routing rules must be added – both remote Ethernet subnets are accessible via the Master radio IP. Without correct routing rules, IPsec will not function properly.

- 192.168.8.0/24 via 10.10.10.131
- 192.168.131.0/24 via 10.10.10.131

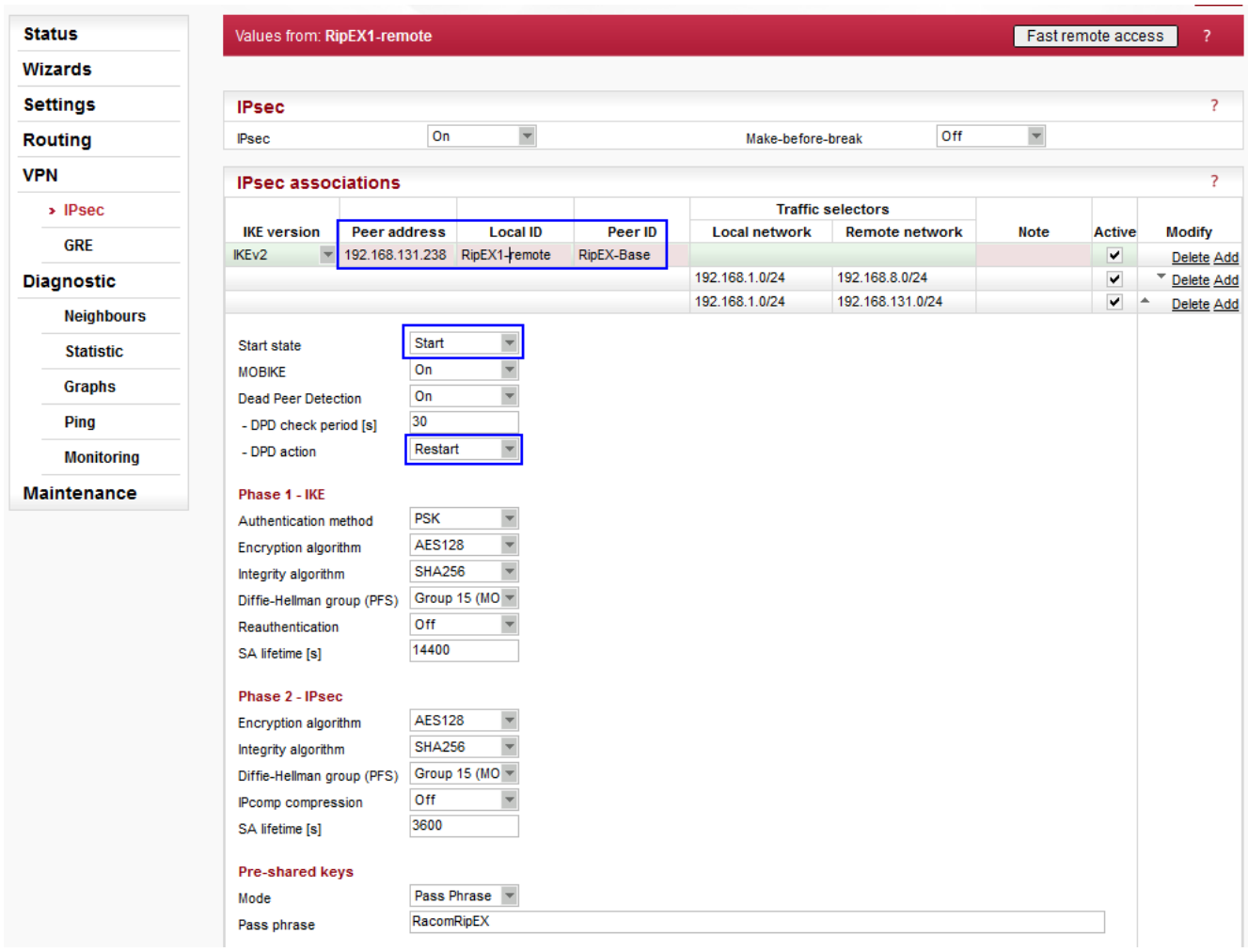


Fig. 4.4: RipEX1-remote IPsec configuration

Parameters:
The IKE, IPsec and PSK parameters are the same as on the Master station. Remember the following differences:

Peer address	“192.168.131.238” ("RipEX-Base" Ethernet IP)
Local ID	“RipEX1-remote”
Peer ID	“RipEX-Base” (both IDs must correspond to those used on the Master station)
Traffic selectors	“192.168.1.0/24 (local) <-> 192.168.8.0/24” (a selector for RipEX1-remote and RipEX2-remote connectivity over IPsec) “192.168.1.0/24 (local) <-> 192.168.131.0/24” (a basic selector for Ethernet to Ethernet accessibility over IPsec)
Start state	“Start” (Connection is established immediately)
DPD action	“Restart” (Connection is established immediately)

The “Start state” might either be “Start” or “On demand”, but cannot be “Passive”, because this state is already configured on the Master station and no end-point would initiate the VPN tunnel.

5. RipEX8-remote Configuration

RipEX8-remote configuration is the same as RipEX1-remote, only a different IP addresses are used. See the following setup with highlighted differences only.

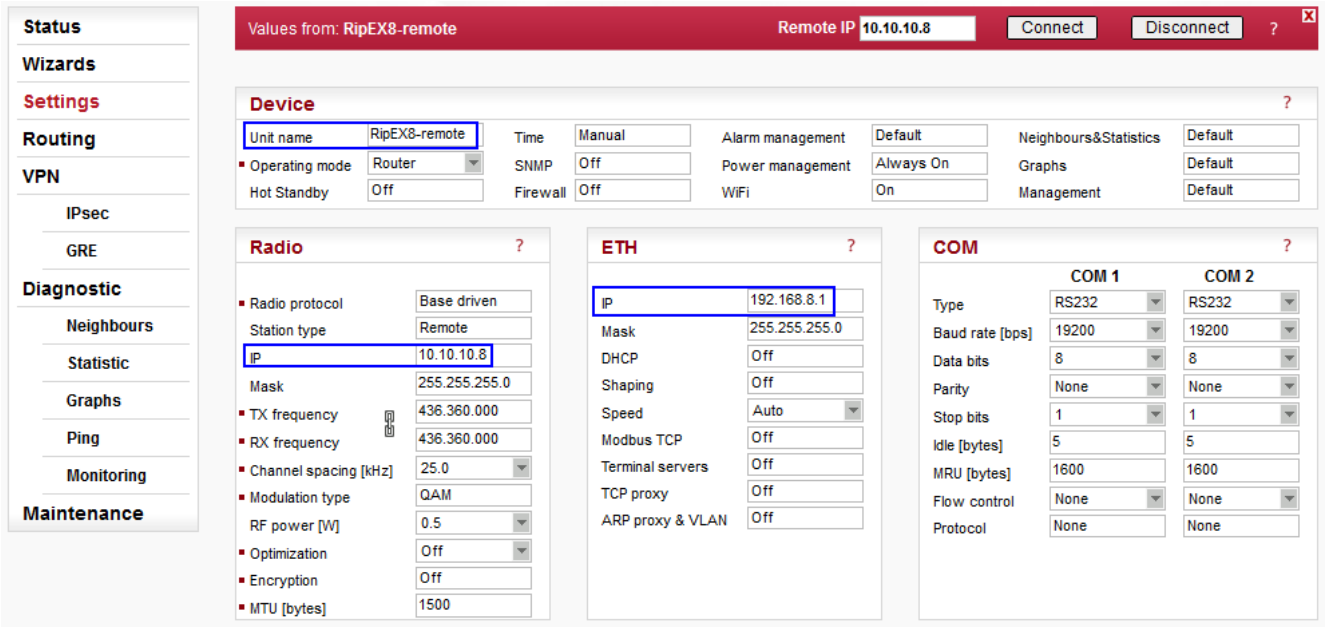


Fig. 5.1: RipEX8-remote Settings

Parameters different from RipEX1-remote Settings:

Unit name	“RipEX8-remote”
Radio IP address	“10.10.10.8”
Ethernet IP address	“192.168.8.1”

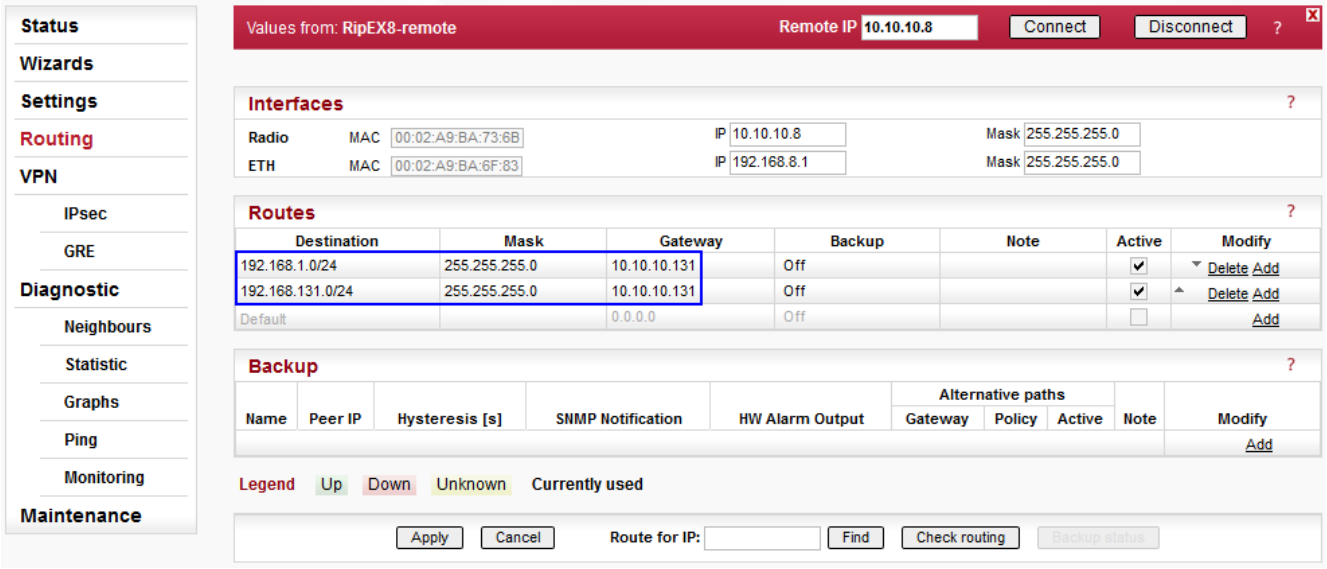


Fig. 5.2: RipEX8-remote Settings

The routes are the same as on RipEX1-remote with one exception – 192.168.1.0/24 is used as a Destination route, because 192.168.8.0/24 is the local network for this unit.

- 192.168.1.0/24 via 10.10.10.131
- 192.168.131.0/24 via 10.10.10.131

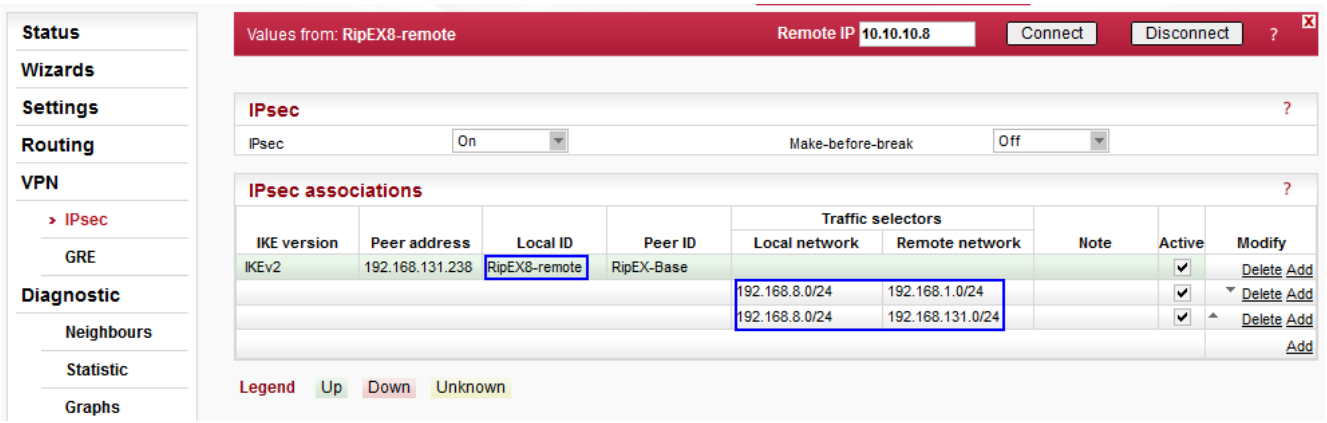


Fig. 5.3: RipEX8-remote Settings

Follow the RipEX1-remote configuration, change the local ID to RipEX8-remote and configure correct Traffic Selectors.

Traffic selectors:

- “192.168.8.0/24 (local) <-> 192.168.1.0/24”
- “192.168.8.0/24 (local) <-> 192.168.131.0/24”

6. IPsec Recommendations

The number of IPsec parameters is very high and it can be hard to optimize their settings to suit the network performance. The following section provides explanation and several recommendations to optimize the configuration when utilizing it on the Radio channel.

Parameter	Recommendation
Make-before-break	A temporary connection break during IKE_SA re-authentication is suppressed by this parameter. It is supported in IKEv2 only. Set it to “On” for a higher tunnel reliability and availability, because the connection is not interrupted during re-authentication.
IKE version	Use the “IKEv2” if possible. One of the main reasons is a lower bandwidth consumption compared to IKEv1, always helpful for the Radio channel.
Start state	One possible approach is to set “Passive” mode in the central site (IPsec concentrator) and “Start” in all Peers. In such a configuration, if the Peer is turned off, the Master does not try to establish the connection. Only if the Peer is alive, will it automatically establish the connection itself and the Master station will be ready to answer. Do NOT use the “Passive” mode on both end-points. In such configuration, no tunnel will be established. Neither is it recommended to configure a “Start” mode on both peers, because establishment can be initiated from both peers simultaneously and two SAs can be created which might result in dropping the tunnel and re-establishment. Eventually, a correct tunnel is established, but it may take a while in a cycle before the tunnel is established correctly.
MOBIKE	In static RipEX networks, mobility support is not required – turn it “Off”.
Dead Peer Detection	It is set in our example and is used to keep the tunnel up and running. If keep-alive packets are lost, the tunnel is closed and “action” is performed. Turn this option “On” for faster communication loss recovery. This can be very useful if the SA lifetime periods are long and/or RipEX HotStandby is used. The “DPD Action” might be any of the available options, one possible option is to use “Hold” in the Master station and “Restart” in remote units.
Encryption algorithm	Use the default AES128 which provides a sufficient level of security while keeping CPU usage at low values.
Integrity algorithm	Use the default SHA256 for a sufficient level of packet integrity.
Diffie-Hellman group	With default Encryption and Integrity settings, we suggest using Group19 or Group20. Both are within the so called “Elliptic Curve” group. They provide the same or better security, but consume less CPU than typical “Modulo Prime” groups. Nevertheless, “Modulo Prime” groups are widely used and a default group is MODP3072 (Group15).

Reauthentication	We recommend you to turn this option “Off” (default), because it consumes less bandwidth when the IKEv2 SA expires and negotiation is required. On the other hand, enabled reauthentication is more secure.
SA lifetime	If these values are too low, this leads to high CPU usage for reauthentication which will also occur too often. The default values are 14400 seconds (2 days) for IKE phase I and 3600 seconds (1 hour) for IKE phase II. These are the minimal recommended values for the Radio channel while maintaining a sufficiently high security level.
IPcomp compression	Where possible turn this useful option “On”, because this feature might save precious bandwidth using the compression. If using IPsec, the default radio compression does not have any effect on packet sizes. By default, it is “Off”, because the Peer might not support this feature.
Pre-shared keys	Choose a pass phrase length as required, but 30 or more characters are more than secure enough and no special characters are required. Consider a different PSK for every IPsec tunnel. You can also use a “Key” mode and generate a secure and unique key for a particular tunnel. Copy and paste the key to the Peer unit.

7. IPsec Bandwidth Consumption

Each IPsec tunnel needs several packets to be exchanged for:

- Tunnel establishment
- Re-keying procedures
- Closing the tunnel

The exact overhead is different for all possible combinations of Encryption, Integrity algorithms, IP compression and other parameters.

One example configuration: PSK, IPcomp enabled, aes128-sha256-modp2048

- Tunnel establishment: 4 packets, 1528 B
- Re-keying: 4 packets, 1248 B
- Closing the tunnel: 2 packets, 216 B

Transferring 5120 B of random data (5 packets) results in 5580 B of transferred data on the Radio channel, i.e. 8.98 % overhead for each packet.

Keep in mind that by percentage, the overhead is higher if the packet size is lower, e.g. the overhead will be higher for 100B packet than for 1300B packets.

Another example: Sending non-compressible 1000B UDP frame results in:

- Sending 1102B IPsec packet on the Radio channel,
- while 1030 B packet if IPsec is not used.

That means +72B of overhead (for 1000B packet, it is 7.2% overhead).

8. Configuration Example with CISCO router

The IPsec tunnel can be established among all devices compatible with IPsec protocol (RipEX, CISCO, etc.). This chapter explains and shows the RipEX and CISCO ASA configuration steps and IPsec interconnectivity over the Ethernet infrastructure.

CISCO router/firewall can be used as a powerful IPsec concentrator utilizing tens, hundreds or thousands of IPsec tunnels. If you already have a company infrastructure and VPN connectivity and you need to have remote access to the whole RipEX network in a secure way, CISCO IPsec concentrator (or any other similar supplier) is one of the solutions.

Note

You can use RipEX instead of a CISCO router, but keep in mind the limitation of 8 simultaneous IPsec tunnels.

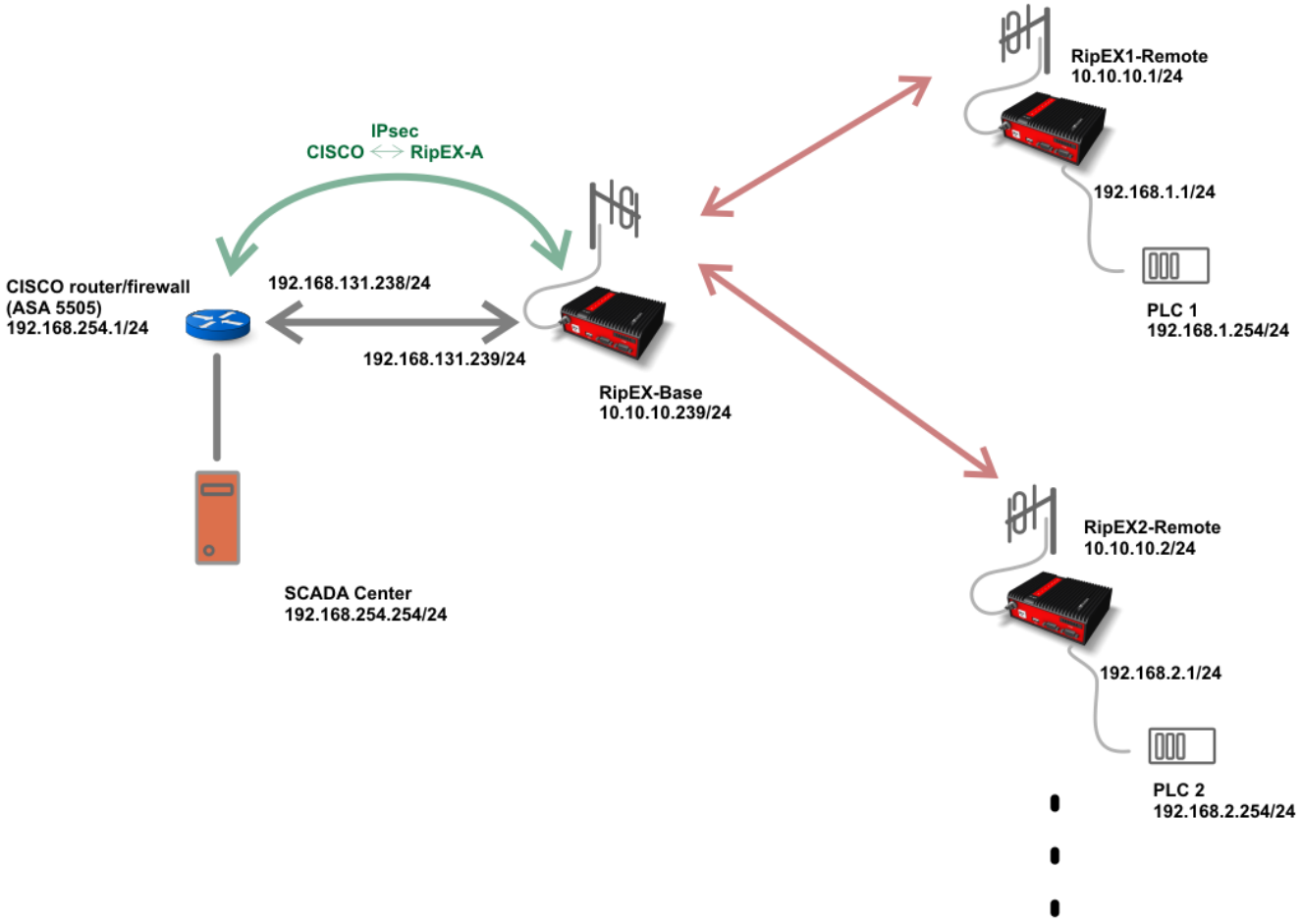


Fig. 8.1: Topology

The connection between CISCO and RipEX routers can go over any infrastructure, including other routers, switches or firewalls via any connectivity type (cellular network, p2p microwave links, …). For this simple example, only the “direct” or “switched” connection is used, i.e. both are within one Layer2 subnet: 192.168.131.0/24.

The central location behind the CISCO ASA router is configured with 192.168.254.0/24 network. This SCADA center monitors all remote PLC units. The PLCs can either be connected via Ethernet, or via RS232 links (RTUs).

Configuration of the central CISCO router and RipEX-Base will be explained in detail. Other RipEX units' configurations are straight-forward and will be explained briefly.

8.1. RipEX-Base General Configuration

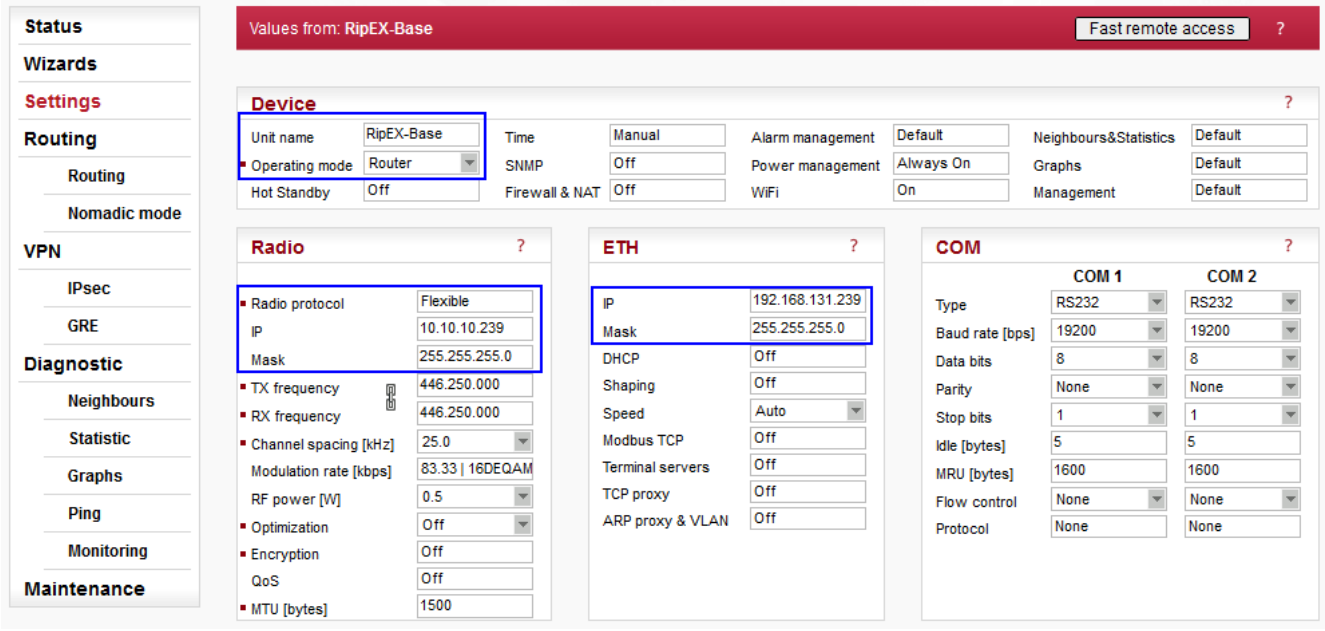


Fig. 8.2: RipEX-Base Settings

Parameters:

Unit name	RipEX-Base
Operating mode	Router (IPsec can only be configured in Router mode)
Radio protocol	Flexible (you can choose either of the two supported protocols – Flexible or Base driven)
Radio IP/Mask	10.10.10.239/24
ETH IP/Mask	192.168.131.239/24

Note

See previous chapters, the manual or web interface help on other parameters.

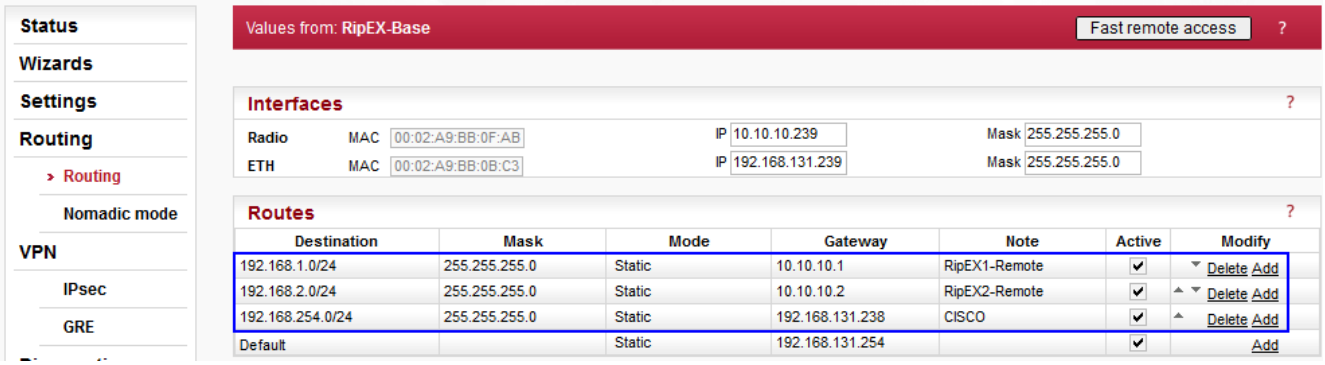


Fig. 8.3: RipEX-Base Routing

Three static routes are configured to meet the topology being used:

- 192.168.1.0/24 via 10.10.10.1 (connection to RipEX1-Remote Ethernet subnet)
- 192.168.2.0/24 via 10.10.10.2 (connection to RipEX2-Remote Ethernet subnet)
- 192.168.254.0/24 via 192.168.131.238 (connection to CISCO subnet)

The first two routes are necessary to access remote subnets via the Radio channel and there is no IPsec configured. The third route to 192.168.254.0/24 network is also necessary and once IPsec is established, packets sent to this remote network will be encapsulated (following the IPsec selectors' configuration).

8.2. CISCO General Configuration

CISCO ASA is configured via CLI commands.

Note

A Windows "putty" application can be used to access CISCO CLI environment (e.g. via Console port / RS232). Once logged in, type "enable" and "conf t" to access configuration menu. See the CISCO documentation for more details.

Parameters:

```
hostname ciscoasa
```

- The CISCO ASA hostname (hostname can be used as a Peer ID for IPsec if required)

```
interface Ethernet0/0
 switchport access vlan 2
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.254.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.131.238 255.255.255.0
```

- Ethernet interface IP configuration. The internal (inside) LAN is configured with 192.168.254.1/24 subnet. The external (outside) interface is set to 192.168.131.238/24 and it's set for the Ethernet0/0 interface.

```
object network vpn-local-192.168.254.0
 subnet 192.168.254.0 255.255.255.0
object network vpn-remote-192.168.1.0
 subnet 192.168.1.0 255.255.255.0
object network vpn-remote-192.168.2.0
 subnet 192.168.2.0 255.255.255.0

nat (inside,outside) source static vpn-local-192.168.254.0 vpn-local-192.168.254.0 ▶
destination static vpn-remote-192.168.2.0 vpn-remote-192.168.2.0
nat (inside,outside) source static vpn-local-192.168.254.0 vpn-local-192.168.254.0 ▶
destination static vpn-remote-192.168.1.0 vpn-remote-192.168.1.0
```

- The "object" settings define three objects with their network and mask. Objects are used to simplify other configuration steps.
- NAT (Network Address Translation) rules are created to forward the communication between local and remote subnets.

Note

Different approaches are possible.

8.3. Remote RipEX Units Configuration

Remote RipEX units must also be set in Router mode with correct Radio parameters applied. The only routing rule required is a "Default gateway" to the central RipEX-Base unit's radio IP (10.10.10.239).

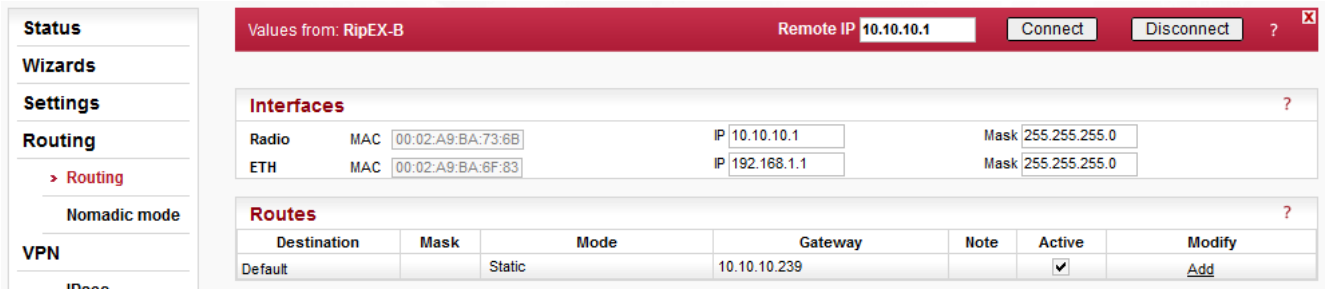


Fig. 8.4: Remote RipEX units' Routing menu

8.4. IPsec Configuration

The complete RipEX IPsec configuration used in this example is:

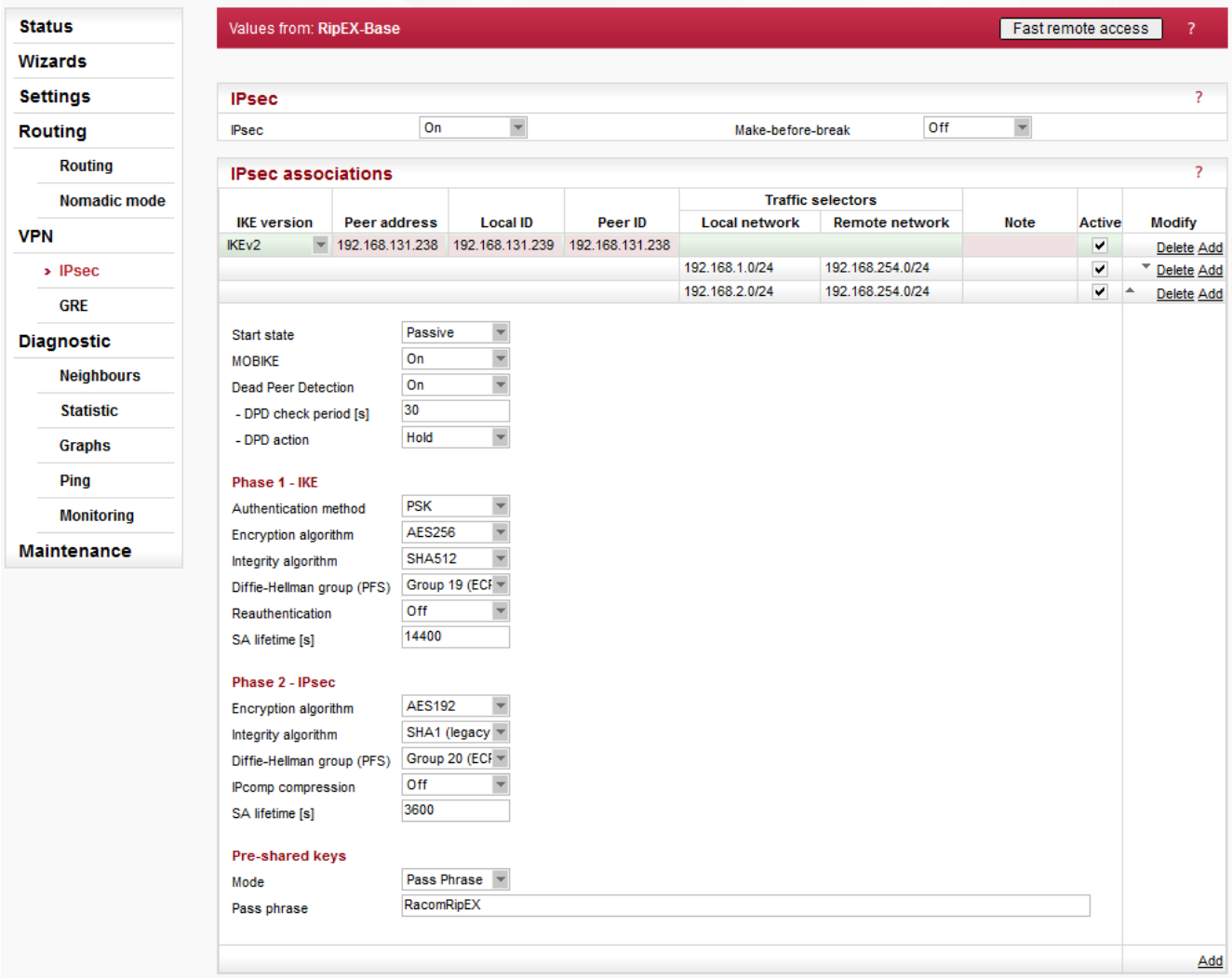


Fig. 8.5: RipEX-Base IPsec configuration

CISCO configuration:

```
access-list l2l-list extended permit ip object vpn-local-192.168.254.0 object ▶
vpn-remote-192.168.1.0
access-list l2l-list extended permit ip object vpn-local-192.168.254.0 object ▶
vpn-remote-192.168.2.0

crypto ipsec ikev2 ipsec-proposal ikev2proposal
 protocol esp encryption aes-192
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto map ikev2map 1 match address l2l-list
crypto map ikev2map 1 set pfs group20
crypto map ikev2map 1 set peer 192.168.131.239
crypto map ikev2map 1 set ikev2 ipsec-proposal ikev2proposal
crypto map ikev2map 1 set security-association lifetime seconds 3600
```

```
crypto map ikev2map interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 19
 prf sha512
 lifetime seconds 14400
crypto ikev2 enable outside

group-policy ripexTrialPol internal
group-policy ripexTrialPol attributes
 vpn-tunnel-protocol ikev2
 ipsec-udp enable
tunnel-group 192.168.131.239 type ipsec-l2l
tunnel-group 192.168.131.239 general-attributes
 default-group-policy ripexTrialPol
tunnel-group 192.168.131.239 ipsec-attributes
 ikev2 remote-authentication pre-shared-key RacomRipEX
 ikev2 local-authentication pre-shared-key RacomRipEX
```

Selected RipEX-CISCO IPsec parameters

IKE version	Peer address	Local ID	Peer ID	Traffic selectors		Note	Active	Modify
				Local network	Remote network			
IKEv2	192.168.131.238	192.168.131.239	192.168.131.238				☑	Delete Add
				192.168.1.0/24	192.168.254.0/24		☑	Delete Add
				192.168.2.0/24	192.168.254.0/24		☑	Delete Add

Fig. 8.6: RipEX-Base Peer address, IDs and Traffic selectors

CISCO commands:

CISCO defines “Peer address” via a command

```
crypto map ikev2map 1 set peer 192.168.131.239
```

Tunnel type must be configured using a “tunnel-group” command:

```
tunnel-group 192.168.131.239 type ipsec-l2l

tunnel-group 192.168.131.239 general-attributes
 default-group-policy ripexTrialPol
```

A policy for using IKEv2 is created and named “ripexTrialPol”.

```
group-policy ripexTrialPol internal
group-policy ripexTrialPol attributes
 vpn-tunnel-protocol ikev2
 ipsec-udp enable
```

The policy states that IKEv2 is allowed (IKEv1 is NOT allowed) and IPsec traffic via UDP datagrams.

The Local and Peer IDs are configured as IP addresses automatically in CISCO. If a different ID is required, enter the IPsec attributes tunnel configuration and choose the required identity.

```
ciscoasa(config)# tunnel-group 192.168.131.239 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# isakmp identity <option>
```

For example, the hostname can be used as the CISCO ID using:

```
ciscoasa(config-tunnel-ipsec)# isakmp identity hostname
```

In such a case, change the Peer ID to “ciscoasa” in the RipEX-Base IPsec configuration.

The traffic selectors in RipEX correspond to the following CISCO parameters:

```
access-list l2l-list extended permit ip object vpn-local-192.168.254.0 object ▶
vpn-remote-192.168.1.0
access-list l2l-list extended permit ip object vpn-local-192.168.254.0 object ▶
vpn-remote-192.168.2.0
```

These commands specify the “interesting traffic” which will be encrypted. Notice its name “l2l-list” which is also used in other parameters/commands.

RipEX parameters:

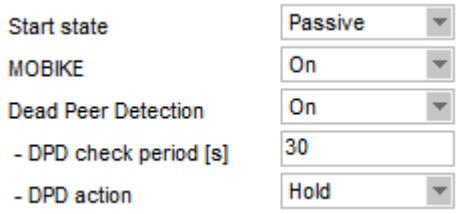


Fig. 8.7: RipEX-Base IPsec parameters

CISCO commands:

Check your CISCO device manual if parameters in Fig. 7 are or are not supported. The tested CISCO ASA automatically starts the IPsec tunnel and thus, RipEX is set to the “Passive” mode. MOBIKE and DPD were not configurable, but could be enabled in RipEX. DPD takes care of the tunnel “health” and can force tunnel re-establishment. The MOBIKE parameter is “on” by default, but if the topology is static, it can be turned off.

Note

In newer CISCO iOS, the DPD mechanism should be supported using the tunnel-group ipsec-attributes “`isakmp keepalive {disable | threshold <threshold> retry <retry-interval> | threshold infinite}`” command.

RipEX parameters:

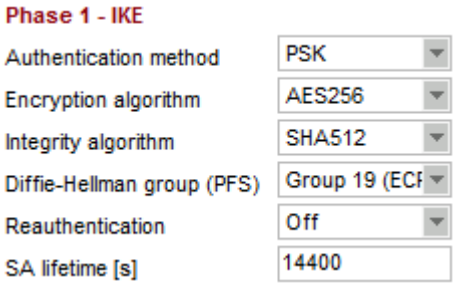


Fig. 8.8: RipEX-Base IPsec Phase 1 parameters

RipEX only supports the PSK authentication method.

CISCO commands:

CISCO PSK configuration is shown later in the PSK pass-phrase settings.

Other parameters can be configured via the IKEv2 policy:

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha512
 group 19
 prf sha512
 lifetime seconds 14400
```

The PRF is not configurable in RipEX and it's always the same as integrity algorithm. The SA lifetimes do not need to be the same on both IPsec tunnel end-points. Once the CISCO or RipEX SA lifetime is reached, the re-keying (re-authentication) is started and lifetime values are reset at both end-points.

Note

Reauthentication was not configurable in a tested CISCO ASA iOS version. Reauthentication is useful as the authentication method if certificates are being used.

RipEX parameters:

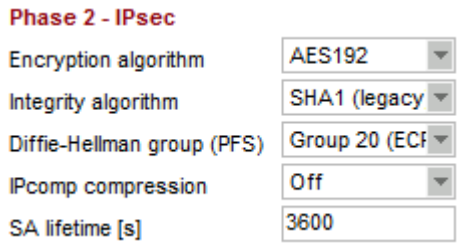


Fig. 8.9: RipEX-Base IPsec Phase 2 parameters

```
crypto ipsec ikev2 ipsec-proposal ikev2proposal
 protocol esp encryption aes-192
 protocol esp integrity sha-1
crypto map ikev2map 1 set pfs group20
```

```
crypto map ikev2map 1 set ikev2 ipsec-proposal ikev2proposal
crypto map ikev2map 1 set security-association lifetime seconds 3600
```

Note

IPcomp was not implemented in tested CISCO ASA iOS.

RipEX parameters:

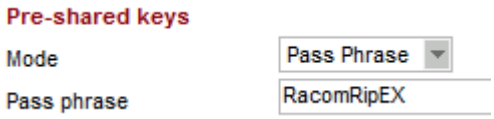


Fig. 8.10: RipEX-Base IPsec PSK

CISCO commands:

```
tunnel-group 192.168.131.239 ipsec-attributes
 ikev2 remote-authentication pre-shared-key RacomRipEX
 ikev2 local-authentication pre-shared-key RacomRipEX
```

Note

If you run the “show run” command to see the configured parameters, the PSK is displayed as *****.

Other important CISCO parameters:

```
crypto map ikev2map 1 match address l2l-list
```

Create a crypto map and match it to the previously create ACL rules named “l2l-list”

```
crypto map ikev2map interface outside
```

Apply the crypto map to the correct interface

```
crypto ikev2 enable outside
```

Enable IKEv2 on a correct interface

Note

Check the IPsec/IKEv2 details with respective manuals.

8.5. CISCO Troubleshooting

CISCO devices have several ways to debug issues with IPsec, here are some of them:

```
ciscoasa(config)# show crypto ikev2 sa detail
```

Detailed information about active IKEv2 Security Associations

```
ciscoasa(config)# show crypto ipsec sa
```

Information about active IPsec Security Associations

```
ciscoasa(config)# deb crypto ikev2 protocol
ciscoasa(config)# deb crypto ikev2 platform
```

Debug output for IKEv2

9. IPsec Testing and Functionality Verification

The most important and basic functionality overview can be displayed in the Web interface in the VPN / IPsec menu. Click on the “Refresh status” to see current IPsec tunnels’ states.

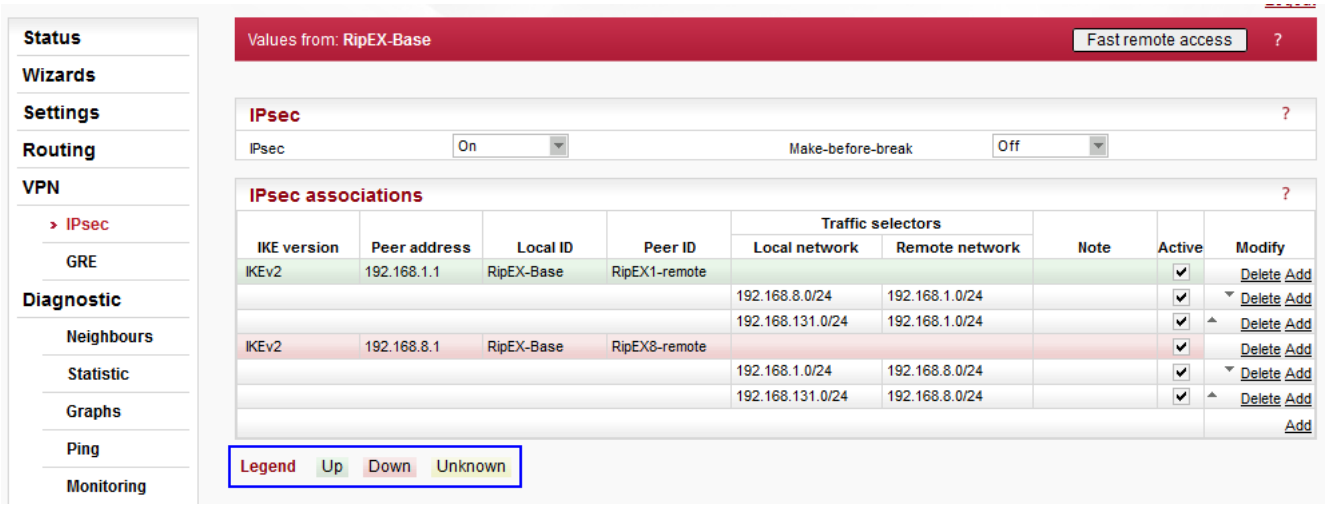


Fig. 9.1: RipEX8-remote Settings

Possible states:

- Green (“Up”): The corresponding IKE SA and all corresponding CHILD SAs are created.
- Red (“Down”): The IKE SA is not created and the tunnel is not established.
- Yellow (“Unknown”): The IKE SA status is not available.
- Gray: The individual CHILD SA line can be gray if:
  it is not marked as Active, or
  its configuration was not accepted.

A quick overview can be also checked via CLI command “cli_status_ipsec_show”. This command prints the IKE SA states identified by the Peer IDs.

```
CLI(admin):~$ cli_status_ipsec_show

Status of active IPsec associations:

Peer ID: RipEX1-remote Status: up

Peer ID: RipEX8-remote Status: up
```

Another option is to check the packets in the Monitoring menu. IKE uses UDP packets on ports 500 or 4500. ESP is the IP protocol 50. A filter can be specified as UDP and “Other”. An example of received ESP packet:

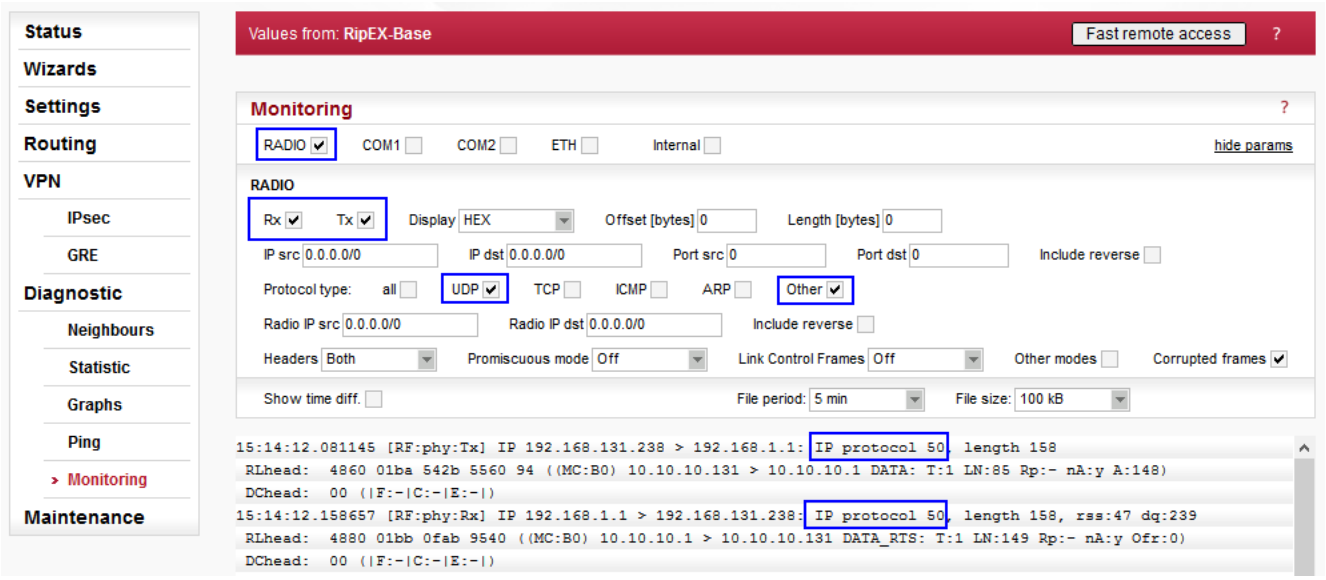


Fig. 9.2: RipEX-Base IPsec Monitoring on the Radio channel

10. Troubleshooting

- User data packets are dropped until the IPsec connection is established. ICMP “admin prohibited” packets are sent back to the source address. The ping response is “Packet filtered”.
- There is only one instance of the SA under normal conditions. When the key exchange is in process, two instances may exist at the same moment. The connection can be duplicated in certain circumstances. It should not cause any problems for user traffic. On the other hand, it consumes system resources and increases network overhead.
- When the “SA lifetime” expires and the connection is broken, the “Diffie-Hellman group” is probably set up incorrectly.
- Is the IKE version the same on both tunnel end-points?
- Did you configure a correct “Peer address” on both end-points?
- Are the “Local ID” and “Peer ID” correct on both end-points and do they correspond to each other? I.e. On the second unit, the values must be the same, but switched.
- Are the “Traffic selectors” correct on both end-points and do they correspond to each other? The selectors must always be paired – via switching the “Local” and “Remote” networks.
- Are all the IKE parameters the same on both end-points? (Encryption algorithm, Integrity algorithm, Diffie-Hellman group)
- Are all the IPsec parameters the same on both end-points (child SA)?
- Are you really sure the parameters are the same? Might be difficult to spot some parameters in other vendors’ routers such as CISCO, Mikrotik, Fortigate and others…
- Is the PSK configured the same on both end-points? Did you fill the hexadecimal number (“Key”) instead of text (“Pass phrase”)?

Appendix A. Revision History

Revision 1.0 2017-11-07
First issue

Revision 1.1 2018-01-10
CISCO example added