RACOM
RADIO DATA NETWORKS

Návod k použití

RipEX
Radiomodem & Router

verze 1.10
15. března 2019

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

Obsah

Nepřehlédněte

Tento manuál obsahuje pouze výběr kapitol dostačující pro nastavení a pro práci se zařízením se zaměřením na českého zákazníka.
Kompletní manuál v angličtině je dostupný na *www.racom.eu*[1].

Copyright

Zřeknutí se odpovědnosti

Přestože dokumentace byla vytvářena s velkou péčí, RACOM nenese žádnou odpovědnost za chyby nebo opomenutí, ani za škody vyplývající z použití těchto informací. Tento dokument a/nebo zařízení může být měněno, s cílem jeho vylepšení, bez upozornění.

Obchodní značky

Všechny obchodní značky a názvy výrobků, použité v tomto návodu, jsou ve vlastnictví jejich případných vlastníků.

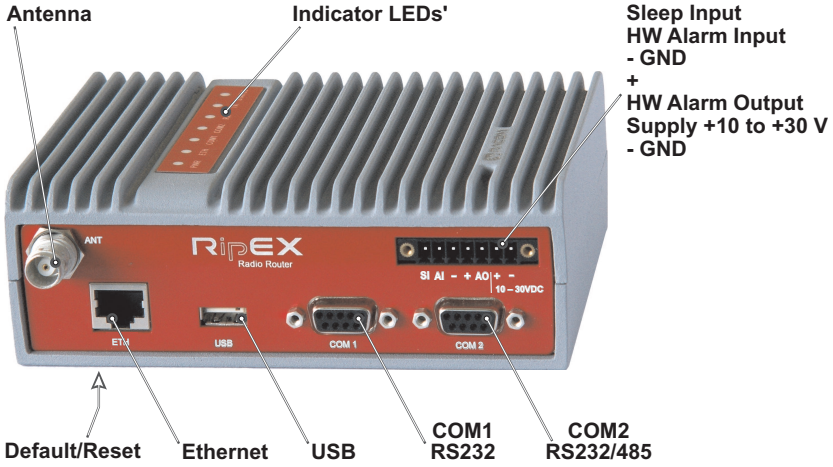
Důležité poznámky

- Vysílání a příjem dat v rádiovém kanále nemůže být, vzhledem k vlastnostem bezdrátové komunikace, zaručeno. Data mohou být zpožděna, poškozena (t.j. obsahovat chyby) nebo dokonce i úplně ztracena. Významná zpoždění nebo ztráty jsou však, při použití takových rádiových zařízení jako jsou výrobky společnosti RACOM a ve správně navržených sítích, velmi vzácné. Zařízení vyráběné společností RACOM nesmí být použito v situaci, kdy výpadek při vysílání nebo příjmu dat může způsobit škodu, ať už uživateli nebo třetím stranám, a to včetně (ale ne výhradně) zranění nebo smrti osob nebo ztrátám na majetku. RACOM neručí za škody jakéhokoliv druhu vzniklé při příjmu nebo vysílání dat a/nebo chybou nebo poruchou tohoto výrobku při přenosu dat.
- Za žádných okolností RACOM, ani jakákoliv jiná společnost nebo osoba, nenese odpovědnost za náhodné, neúmyslné nebo podobné škody vzniklé používáním výrobků společnosti RACOM. RACOM neposkytuje uživatelům žádnou záruku vhodnosti a použitelnosti výrobků pro jejich konkrétní aplikaci.
- Výrobky společnosti RACOM nejsou vyvíjeny, navrženy a testovány pro použití v aplikacích, které mohou přímo ovlivňovat zdraví nebo životní funkce osob nebo zvířat, ani jako součást podobně důležitých systémů. RACOM nedává žádnou záruku, pokud jeho výrobky budou v takových aplikacích použity.

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

Uvedení do provozu

RipEX je rádiový modem, přesněji rádiový IP router, se širokými možnostmi konfigurace. Pro uvedení do provozu stačí připojit anténu, napájení a nastavit konfiguraci pomocí PC s webovým prohlížečem.



Obr. 1: Rádiový router RipEX

Defaultní přístupové parametry: IP 192.168.169.169/24, username: admin, password: admin

Nastavte na svém PC statickou IP adresu 192.168.169.x/24, zapněte RipEX a vyčkejte 25 sekund na rozběh OS v RipEXu. Připojte vaše PC k ETH interface RipEXu, spusťte váš prohlížeč a do adresového řádku napište https://192.168.169.169. Při prvním připojení k RipEXu akceptujte bezpečnostní certifikát https vydaný firmou Racom.

Ujistěte se před začátkem konfigurace, že váš RipEX je jediným v okolí, který je zapnutý. Z výroby vycházejí všechny RipEXy se shodnou defaultní konfigurací, mohlo by se tedy stát, že se připojíte bez upozornění k jinému RipEXu v rádiovém dosahu.

Pokud se připojujete přes volitelný adaptér USB/ETH "X5", pak vaše PC dostane IP adresu z vestavěného serveru DHCP. V prohlížeči pak použijte adresu https://10.9.8.7. Další postup je shodný a okolních RipEXů se nemusíte obávat, budete připojeni vždy jen k lokálnímu radiomodemu.

Rádiová síť SCADA krok za krokem

Stavba spolehlivé rádiové sítě pro systém SCADA nemusí být zcela jednoduchá, i když použijete tak univerzální a snadno konfigurovatelné zařízení, jako je rádiový modem RipEX. Následující přehled vám může pomoci v rychlém a účelném postupu.

1. Navrhněte vaši síť tak, aby úroveň RF signálů splňovala požadavky systému.
2. Vypočtěte a odhadněte průchodnost sítě a dobu odezvy při požadovaném zatížení vaší aplikací.
3. Proveďte test na stole s 3–5 soupravami RipEX a zařízením SCADA.
4. Navrhněte adresové a routingové schéma sítě.
5. Nakonfigurujte RipEXy.
6. Instalujte jednotlivé stanice
   a. Namontujte RipEX do rozvaděče
   b. Instalujte anténu
   c. Instalujte napájecí kabel antény
   d. Proveďte správné uzemnění
   e. Propojte kabely a připojte konektory. SCADA zařízení nepřipojujte.

f. Zapněte napájení RipEXu
g. Otestujte rádiovou linku
h. Ověřte pingem dostupnost všech IP adres, se kterými bude tato jednotka komunikovat.
i. Připojte zařízeni SCADA

7. Proveďte test vaší aplikace

POZNÁMKA:
Z bezpečnostních důvodů je při komunikaci mezi PC a RipEXem použito SSL kryptování pro http protokol. Protokol https vyžaduje bezpečnostní certifikát. Tento certifikát je nutno instalovat do vašeho prohlížeče (Mozilla Firefox, Internet Explorer). Při prvním připojení k RipEXu Vás požádá PC o potvrzení importu certifikátu do PC. Certifikát je podepsán certifikační autoritou Racom s.r.o. Splňuje všechny bezpečnostní předpisy a nemusíte se obávat vložit jej do počítače. Potvrďte import včetně všech varování a výjimek, které Váš počítač může při instalaci zobrazovat.

Je možno stáhnout si do RipEXu vlastní SSL certifikát pro https komunikaci použitou při konfiguraci přes web. Je doporučen a podporován 2048 bitový certifikát, ale může být použit i 512 nebo 1024 bitový certifikát. SSL certifikát může obsahovat jeden nebo dva soubory. Obě možnosti lze použít.

Podrobný popis v angličtině naleznete na *www racom.eu (html)*[1] nebo *www.racom.eu (pdf)*[2] a v Helpech ovládacího menu.

[1] http://www.racom.eu/eng/products/m/ripex/index.html
[2] http://www.racom.eu/download/hw/ripex/free/eng/ripex-m-en.pdf

1. RipEX podrobně

1.1. Provozní režimy

Radiomodem RipEX se nejlépe hodí pro přenos velkého počtu krátkých zpráv, kdy je požadováno jejich zaručené dodání.

Základní použití radiomodemu RipEx je následující:

Polling (obvolávání)
V sítích s obvoláváním centrální řídící jednotka obvolává všechny vzdálené radiomodemy jeden po druhém. Řídící jednotka vyměňuje data s aktuálně připojenou vzdálenou rádiovou stanicí a když skončí, vytvoří nové spojení s další vzdálenou stanicí podle pořadí dotazování.

Report-by-exception (spontánní přístup)
V sítích se spontánním přístupem lze vzdálené jednotky rovněž obvolávat. Kromě toho jakákoliv vzdálená jednotka může spontánně posílat data do řídící jednotky (typicky u alarmové zprávy).

Mesh
V uspořádání "síť" může kterýkoli radiomodem komunikovat spontánně s libovolným jiným radiomodemem. V tomto uspořádání je možno používat i aplikace s přístupem pooling nebo report-by-exception.

Pro komunikaci s různými typy aplikací poskytuje RipEX více možností pro vytvoření rádiové sítě. Jsou to dva různé operační módy, Bridge a Router a tři protokoly na rádiovém kanálu:

- *Transparent* používaný v Bridge módu
- *Base driven* používaný v Router módu
- *Flexible* používaný v Router módu

1.2. Transparent protokol v režimu Bridge

Paket přijatý přes jakékoliv rozhraní je vysílán broadcastem do odpovídajících rozhraní všech jednotek v rámci sítě. Pakety přijaté na COM jsou na vzdálených místech vyslány na COM1 i na COM2.

Kterákoliv jednotka může být nakonfigurována jako repeater (opakovač). Repeater předává všechny pakety, které dostává rádiovým kanálem. Síť z jednotek RipEX má bezpečnostní mechanismy, které zabraňují zacyklení paketů v rádiovém kanálu (např. když repeater přijme paket z jiného repeateru) nebo duplicitnímu příjmu paketů posílaných do uživatelského rozhraní (např. když RipEX přijme paket přímo a pak stejný z repeateru).

Vedle standardního ukončení paketu „Idle“ periodou na sériovém portu (pauza za obdrženými bajty) bridge mode také nabízí "streaming". V režimu streaming začne přenos na rádiovém kanálu okamžitě, bez čekání na konec přijatého rámce na COM => nulové zpoždění.

Režim „bridge mode“ je vhodný pro všechny systémy s obvoláváním.

Poznámka

Limited broadcast 255.255.255.255 a Direct broadcast např. 192.168.255.255 stejně jako Multicast (224.0.0.0 až 239.255.255.255) na Ethernetu jsou podporovány a přenášeny rádiovou sítí.

Návodné video vysvětlující funkci režimu bridge je k vidění zde: *http://www.racom.eu/ripex-bridge-mode*.

Podrobnější popis Transparentního protokolu viz *User manual RipEX*[1].

1.3. Base driven protokol v režimu Router

Provoz na rádiovém kanálu je řízen centrální jednotkou Base station. Přístup na rádiový kanál je přidělován deterministickým algoritmem a tím je dosaženo bezkolizního provozu bez ohledu na zatížení sítě. Rovnoměrným rozložením kapacity rádiového kanálu mezi všechny jednotky Remote je dosaženo stabilní doby odezvy s minimálními výkyvy.

Veškerá komunikace na rádiovém kanálu je řízena z Base station a všechny rámce uvnitř rádiové sítě musí být směrovány přes Base station. Je třeba nastavit příslušný routing.

Base station může komunikovat s různými rychlostmi Modulation data speeds a různým nastavením FEC.

Každá jednotka Remote může pracovat jako Repeater pro jinou Remote. Mezi Base station a Remote může být jen jeden Repeater ale jeden Repeater může být používán více jednotkami Remote.

Pro jednotky Remote umístěné za Repeatrem není třeba nastavovat cesty v Routingových tabulkách. Odesílání rámců přes Repeatry je v obou směrech transparentně řízeno protokolem Base driven.

Je-li požadována komunikace mezi dvěma Remote, pak je třeba v jednotkách Remote v Routing tables nastavit příslušné cesty přes Base station.

Potvrzování rámců ACK, opakované vysílání a kontrola CRC zaručují doručení dat a jejich správnost i při nepříznivých podmínkách na rádiovém kanálu.

Podrobnější popis Base driven protokolu viz *User manual RipEX*[2].

1.4. Flexible protokol v režimu Router

Radiomodem RipEX funguje jako standardní IP router s dvěma rozhraními (rádiové a Ethernetové) a dvěma COM porty. Na rádiovém kanálu je sofistikovaný antikolizní protokol, který kontroluje a ověřuje každý jednotlivý paket. V režimu IP router může každá jednotka současně pracovat jako store-and-forward (uložit a předat) repeater a přitom předávat pakety do připojeného zařízení.

Režim „router mode“ je vhodný pro všechna použití. Na rozdíl od režimu „bridge mode“ je přijetí paketu potvrzeno přes rádiový kanál i ve velmi jednoduchých typech obvolávání a paket je v případě potřeby zopakován.

[1] http://www.racom.eu/eng/products/m/ripex/ripex-detail.html#bridge_mode
[2] http://www.racom.eu/eng/products/m/ripex/ripex-detail.html#base-driven

Poznámka

V režimu Router nejsou v rádiové síti podporovány Ethernet broadcasty a multicasty. Broadcasty jsou podporovány jen jako součást sériových SCADA protokolů.

Návodné video vysvětlující funkci router mode je k vidění zde: *http://www.racom.eu/ripex-router-mode*.

1.4.1. Detailní popis

Režim router je vhodný pro sítě typu multipoint (vícebodové), kde mohou být použity multi-master aplikace s různými kombinacemi obvolávání a/nebo spontánní datové protokoly. Proprietární protokol linkové vrstvy na rádiovém kanálu je velmi sofistikovaný, může přenášet jak unicast, tak i broadcast rámce, je schopný vyhnout se kolizím, používá potvrzovací rámce přenosu dat a kontrolou CRC, zajišťuje přenos a integritu dat i v nepříznivém prostředí s rušením na rádiovém kanále.

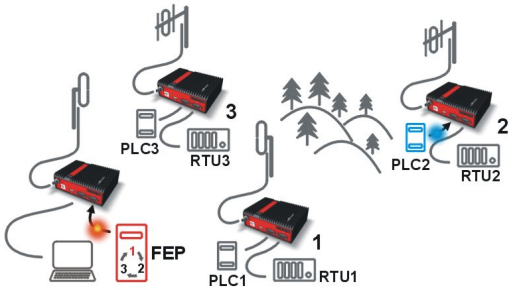
RipEX pracuje jako standardní IP router se dvěma nezávislými rozhraními: Rádiové rozhraní a ETH. Každé rozhraní má svojí vlastní MAC adresu, IP adresu a masku.

IP pakety jsou zpracovávány podle pravidel routingové (směrovací) tabulky. V routingové tabulce můžete také nastavit default gateway (výchozí bránu) routeru (platí pro obě rozhraní).

COM porty jsou považovány za standardní zařízení typu host, zprávy k nim mohou být doručeny do určených čísel portů jako UDP datagramy. Cílová IP adresa COM portu je buď ethernetová IP adresa nebo IP adresa rádiového rozhraní. Zdrojová IP adresa paketů odchozích z COM portů je vždy IP adresa ETH rozhraní.

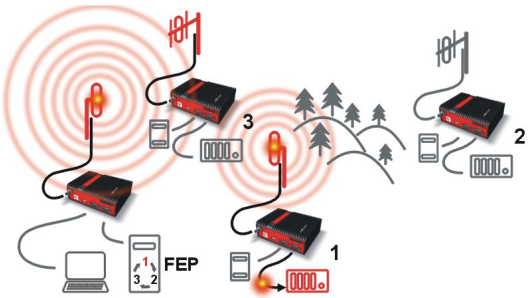
1.4.2. Příklad funkce

V následujícím příkladu jsou dvě nezávislá zařízení SCADA připojená k dvěma COM portům RipEXu 1. Jedno z nich je označené jako RTU (Remote Telemetry Unit) a předpokládá se obvolávání z centra (FEP – Front End Processor). Druhé je označeno jako PLC (Programmable Logic Controller) a předpokládá se spontánní komunikace s libovolně zvolenými vzdálenými PLC.



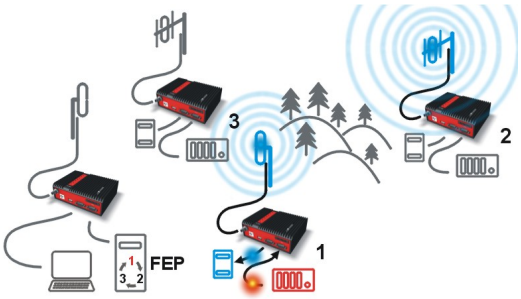
Krok 1

FEP vyšle pro RTU1 paket s žádostí přes COM2 na připojený RipEX.
Současně PLC2 odešle na RipEX paket pro PLC1 přes COM1.



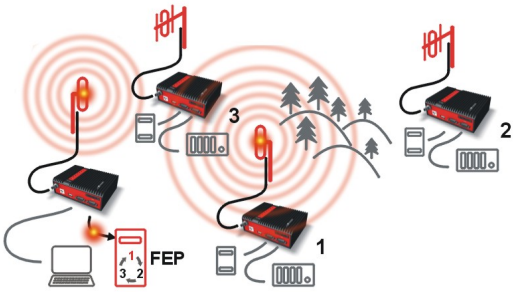
Krok 2

RipEX vysílá paket z FEP adresovaný pro RTU1 do rádiového kanálu.
RipEX1 obdrží tento paket, zkontroluje správnost dat a odešle potvrzení (ACK – acknowledgement).
Současně je paket poslán do RTU1 přes COM2.
RipEX3 sice obdrží tento paket také, ale nereaguje, protože tento paket je adresován pouze pro RipEX1.



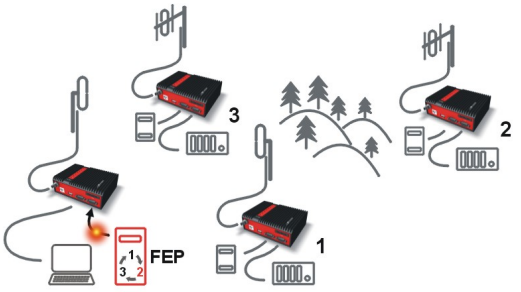
Krok 3

RipEX2 čeká, až je ukončena předchozí operace na rádiovém kanálu (antikolizní mechanismus).
Potom RipEX2 vysílá na rádiovém kanálu adresovaný paket pro PLC1.
RipEX1 obdrží tento paket, zkontroluje správnost dat a odešle potvrzení (ACK).
Ve stejný čas je odeslán paket do PLC1 přes COM1. Souběžně je paket s odpovědí z RTU1 pro FEP přijat na COM2.



Krok 4

RipEX1 přenáší paket s odpovědí od RTU1 pro FEP v rádiovém kanálu.
Tento paket obdrží všechny RipEXy. Paket je určen pro RipEX u FEP, takže jen tento RipEX reaguje. Zkontroluje integritu dat a vyšle potvrzení na RipEX1.
Současně je odeslán paket RipEXu do FEP přes COM2.



Krok 5

FEP obdrží odpověď od RTU1 a dotazování cyklus (polling) pokračuje ...

Nicméně jakýkoliv PLC nebo RTU může kdykoliv spontánně odeslat paket na jakékoliv jiné místo.

1.4.3. Příklady konfigurace

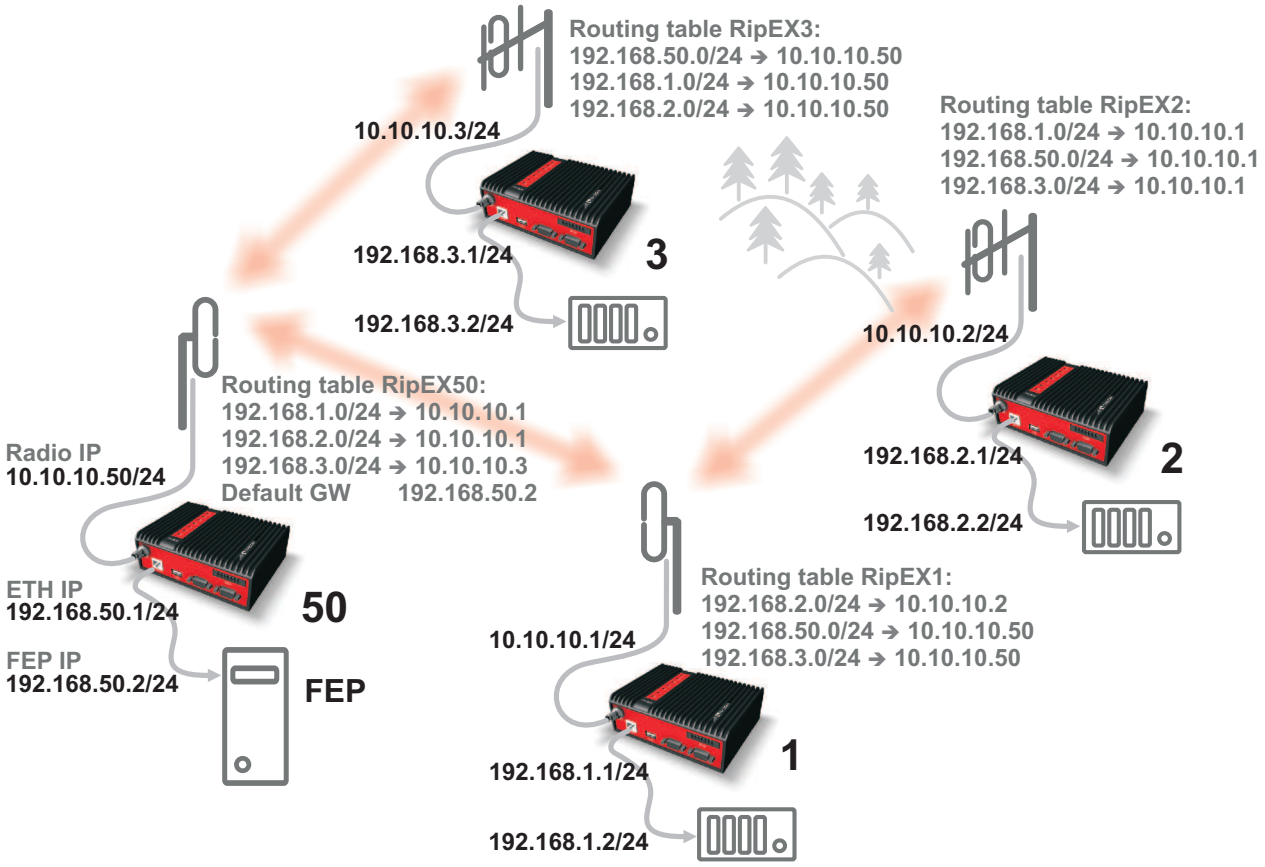
Jak již bylo uvedeno výše, rádiový modem RipEX funguje jako standardní IP router se dvěma samostatnými rozhraními: Rádiové a ETH. Každé rozhraní má svou vlastní MAC adresu, IP adresu a masku.

Operační zásady IP routeru stanoví, že každá jednotka může sloužit jako opakovač. Pouze je nutné správně nakonfigurovat routingové tabulky.

Rádiové IP adresy RipEXu musí komunikovat přes rádiový kanál a také musí sdílet stejnou IP síť. Doporučujeme plánovat vaší IP síť tak, aby každý RipEX byl připojený k samostatnému ethernetovému portu dílčí sítě. To pomáhá udržovat routingové tabulky jasné a jednoduché.

Poznámka

I když IP adresy všech RipEXů sdílejí rádiový kanál jedné IP sítě, nemohou spolu přímo komunikovat jako ve společné IP síti. Pouze RipEXy, které jsou ve vzájemném rádiovém dosahu, (navzájem se slyší) mohou komunikovat přímo. Je-li požadována komunikace s rádiovými IP adresami, musí routingové tabulky zahrnovat i ty trasy, které jsou ve stejné síti (přes retranslace), ale jsou odlišné od běžných IP sítí. Konfigurace v níže uvedeném příkladě pro jednoduchost nemá taková routingová pravidla (nejsou potřebné ve většině případů).



Obr. 1.1: Adresování

Formální soulad mezi posledním bajtem rádiové IP adresy a předposledním bajtem ethernetové adresy není nutný, ale usnadňuje orientaci. Obrázek „Adresování“ ukazuje routingovou tabulku vedle každého RipEXu. Routingová tabulka definuje novou gateway (bránu) pro každou cílovou IP adresu (destination). Při rádiovém přenosu dat rádiová IP adresa dalšího rádiově připojeného RipEXu slouží jako gateway.

Příklad trasy z FEP (RipEX 50) do RTU 2:

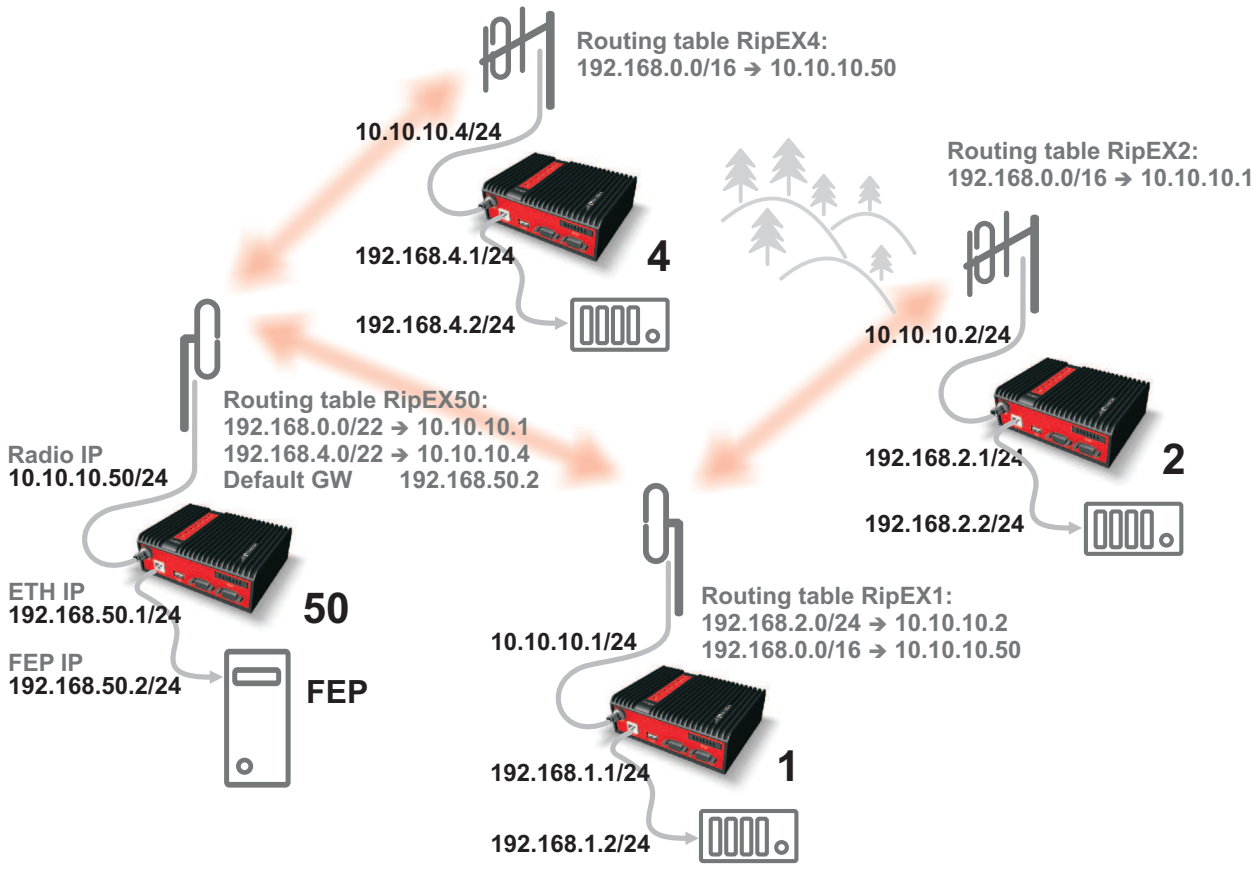
- Destination (cílová adresa) je 192.168.2.2
- Routingová tabulka na RipEXu 50 obsahuje tento záznam:
  Destination 192.168.2.0/24 Gateway 10.10.10.1
- Na základě tohoto zápisu, jsou všechny pakety s adresou v rozsahu od 192.168.2.1 až 192.168.2.254 směrovány do 10.10.10.1
- Vzhledem k tomu, že rádiová IP adresa RipEXu 50 je 10.10.10.50/24, může router říct, že IP 10.10.10.1 patří do rádiového kanálu a odešle paket na tuto adresu přes rádiový kanál
- Paket je přijat RipEXem 1 s adresou 10.10.10.1, na vstupu do routeru
- Routingová tabulka RipEXu 1 obsahuje záznam:
  Destination 192.168.2.0/24 Gateway 10.10.10.2
  na jehož základě je paket směrován do 10.10.10.2 přes rádiový kanál
- Paket je přijat RipEXem 2
- Router porovnává cílovou IP 192.168.2.2 s vlastní ethernetovou adresou 192.168.2.1/24
  a určí, že cíl paketu je ve vlastní ETH síti a pošle paket přes ethernetové rozhraní - nakonec paket obdrží RTU 2.

1.4.4. Rady pro adresování

Ve velkých a složitých sítích s četnými repeatery jednotlivé routingové tabulky mohou být dlouhé a obtížné k porozumění. Chcete-li zachovat jednoduché routingové tabulky, režim adresování by měl sledovat rozvržení rádiové sítě.

Přesněji řečeno, každá skupina IP adres zařízení (RipEXu i SCADA), která je přístupná přes repeater, by se měla pohybovat v rozmezí, které může být definováno maskou a žádná adresa definovaná maskou neexistuje v jiné části sítě.

Typická síť se skládá z jednoho centra a několika vzdálených stanic. Má stromové uspořádání, které může být snadno napodobeno schématem adres - viz příklad na obrázku „Optimalizované adresování“ níže.



Obr. 1.2: Optimalizované adresování

Výchozí brána (default gateway) je také velmi mocný nástroj routingu. Buďte však při jejím použití velmi opatrní, kdykoli výchozí cesta půjde do rádiového rozhraní, tj. do rádiového kanálu. Pokud by přišel do routeru paket k neexistující IP adrese, byl by přenášen přes rádiový kanál. Takové pakety zvyšují zatížení sítě, nebo přinejmenším způsobují nadměrné kolize paketů, mohou vytvářet smyčky atd. V důsledku toho by výchozí brána měla vždy vést k ETH rozhraní, pokud si nejste naprosto jisti, že se nikdy nemůže vyskytnout paket k neexistující IP destination (pamatujte, že máte co do činění s komplexním softwarem psaným a nakonfigurovaným lidmi).

1.5. Kryptování

AES 256 (Advanced Encryption Standard) může být použit pro ochranu proti průniku do rádiového kanálu. Je-li AES 256 zapnut (On), pak je ke každému rámci na rádiovém kanálu připojen 16 Bytový kontrolní blok. AES vyžaduje kryptovací klíč. Délka klíče je 256 bit (32 Byte, 64 hexadecimálních znaků). Shodný klíč musí být uložen ve všech jednotkách v síti.

Klíč se dá zadat ve formě **klíčového slov**a (Pass phrase). Pro vložení klíče není třeba vyplňovat 32 Byte hexa znaků. Klíč lze generovat automaticky podle klíčového slova (Pass phrase). Vložte klíčové slovo (libovolné tisknutelné znaky ASCII, min. 1 znak, max. 128 znaků). Shodné klíčové slovo musí být vloženo do všech jednotek v síti.

Klíč je možné zadat i **manuálně**. Vložte 32 Byte nebo 64 hexa znaků nebo použijte generátor náhodných čísel (tlačítko Generate). Shodné slovo musí být ve všech jednotkách v síti. Tedy musí být vygenerováno v jedné z nich a zkopírováno do ostatních.

1.6. Firewall

1.6.1. Firewall IP (L3)

K dispozici je standardní linuxový IP L3 firewall, a to jak pro Router, tak i pro Bridge mód. Kromě IP adres (L3 funkcionalita) je možné zadat i seznam Eth portů (L4 funkcionalita), které budou FW blokovány.

POZNÁMKA 1:
Nastavení Firewall L2/L3 nemá vliv na ETH přístup. Tedy Firewall neovlivní přístup do lokálně připojeného RipEXu (přístup přes web, ping...).

POZNÁMKA 2:
Porty 443 a 8889 jsou interně použity pro servisní přístup. Dbejte opatrnosti při vytváření pravidel pro L3 Firewall, která ovlivní průchod datagramů přes tyto porty. Přístup managementu na vzdálený RipEX může být ztracen, jestliže jiný RipEX je routerem na trase managentu a jeho port 443 (nebo 8889) je ve Firewallu zakázán (RipEX používá IP tabulku "forward"). Pokud to nastane, použijte na chybně konfigurovaném RipEXu tlačítko RESET na spodní straně (podržte 15 sekund) a tak přejděte na defaultní nastavení přístupu. Tím se obnoví defaultní IP adresa Ethernetu, defaultní heslo, vypne se L3 Firewall (Off), nastaví se ARP proxy&VLAN settings na OFF a rychlost Ethernetu na Auto.

POZNÁMKA 3:
Nastavení Firewall L3 nemá vliv na pakety přijímané a předávané z / na Rádiový kanál. Problém popsaný v Poznámce 2 nemůže nastat, pokud je router RipEX rádiovou retranslací, tedy používá pouze rádiový kanál pro vstup i výstup.

1.6.2. Firewall MAC (L2)

K dispozici je také linuxový L2 firewall, který pracuje se zakázanými (blacklist) nebo povolenými (whitelist) MAC adresami.

Blacklist - zakázané adresy
MAC adresy uvedené v této tabulce jsou blokovány, tedy pakety od / na ně jsou zahozeny. Provoz z jiných MAC adress je povolen.

Whitelist - povolené adresy

Pouze MAC adresy uvedené v této tabulce jsou povoleny, tedy pakety od / na ně jsou povoleny. Provoz z jiných MAC adress je blokován.

1.7. Řízení spotřeby

RipEX umožňuje, kromě standardního režimu spotřeby, přepnutí do dvou zvláštních šetřících režimů - šetřící (SAVE) mód a uspaný (SLEEP) mód.

SAVE mód

Pokud je RipEX přepnut do SAVE módu, pak může být v jednom ze dvou stavů - stav SAVE nebo stav ACTIVE. Ve stavu SAVE je funkce RipEXu omezena na rádiový kanál, aby byla zmenšena spotřeba (přibližně 2 W). Ve stavu ACTIVE pracuje RipEX normálně, poskytuje všechny funkce a má normální spotřebu. Přechod mezi těmito stavy je ovládán pinem SI na napájecím konektoru, přijetím paketu na rádiovém kanálu a hodnotou parametru SAVE mode. Přechod ze stavu SAVE do ACTIVE vyžaduje vnitřní spuštění systému a trvá přibližně 48 sec, přechod z ACTIVE do SAVE proběhne za 4 sec.

RipEX je probuzen, jestliže přijme paket určený pro jeho IP adresu. Za tuto je považována kterákoli IP adresa konfigurovaná v RipEXu (Radio, ETH, ETH Subnet, SLIP) nebo adresa směrovaná přes tento RipEX. Tedy RipEX je probuzen nejen paketem, který směřuje do něj, ale i paketem, který směřuje do zařízení připojeného za tímto RipEXem nebo které je připojeno přes retranslaci rádiovým kanálem tohoto RipEXu.

POZNÁMKA:
Manuální zrušení úsporného režimu.
Při firmware 1.2.1.0 a vyšším můžeme uvést RipEX do stavu SAVE, pak vypnout a zapnout napájení a během nabíhacího času (přibližně 48 sec) začne LED Status rychle blikat po dobu cca 10 sec. Pokud během tohoto blikání stiskneme tlačítko Reset po dobu cca 1 sec, pak se režim napájení přepne na Always On (trvalé napájení) a jednotka je přístupná běžným způsobem (Ethernetem nebo USB/ETH adaptéram "X5").

SLEEP mód

SLEEP mód je řízen digitálním vstupem na napájecím konektoru. Je-li příslušný pin (SI) uzemněn, pak je RipEX přepnut do spánku a má spotřebu pouze 0,07 W. Čas potřebný pro úplné probuzení stanice ze stavu SLEEP je přibližně 48 sekund.

1.8. Diagnostika a správa sítě

Rádiový modem RipEX nabízí širokou škálu možností vestavěné diagnostiky a nástrojů pro správu sítě.

1.8.1. Logy

V RipEXu jsou k dispozici statistické logy a logy ze sousedních stanic (neighbours). Oba logy mají dostupnou historii 20 souborů logů, takže celková historie uložených hodnot je 20 dní (výchozí hodnota “Log save period“ – perioda ukládání dat – se používá 1440 min.).

Neighbours

Log „Neighbours“ obsahuje informace o sousedních jednotkách (RipEXy, které jsou přístupné přímo přes rádiový kanál, tj. bez retranslace). Každý RipEX na síti pravidelně vysílá svůj stav, sadu takzvaných "Watched values" (sledovaných hodnot): pravděpodobnost ztráty paketů při přenosu dat přes rádiový kanál, aktuální napájecí napětí, vnitřní teplotu, měřený RF výstupní výkon, poměr stojatých vln (PSV) na anténním napáječi a celkový počet přijatých paketů přijatých / předaných z rozhraní ETH, COM1 nebo COM2. Kromě toho RipEX, který zaznamenává tato data ve svém logu také udržuje informace o tom, kolikrát poslouchal jeho sousední jednotky a stejně zaznamenává i RSS a DQ. Pro další informace viz manuál – *http://www.racom.eu/eng/products/m/ripex/h-menu.html#diag*.

Statistiky

Log „Statistic“ obsahuje informace o objemu datového provozu na všech rozhraních: rádiovém, ETH, COM1 a COM2. Nabízí podrobné informace o počtu přenášených paketů, o jejich velikosti a jejich počtu za sekundu. Kromě toho je pro rádiové kanály k dispozici podrobné rozdělení do uživatelských a servisních paketů. Pro další informace viz manuál – *http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-statistic*.

1.8.2. Grafy

Nezávislá databáze periodicky ukládá sledované hodnoty (viz „Neighbours“ log výše) až z pěti sousedních RipEXů i z lokálního RipEXu, kde jsou nejdůležitější hodnoty statistického logu. Všechny tyto hodnoty lze zobrazit formou grafů.

Grafy mohou zobrazit souhrn dat nebo podrobnosti v detailu. Detailní logování je aktivováno při dosažení mezní hodnoty specifické položky umožnující podrobnější rozbor provozu jednotky, když dojde k vyhlášení alarmu. Každý graf může zobrazit dva různé prvky najednou, včetně jejich nastavených prahových hodnot. Každá z těchto zobrazených hodnot může být z jiné jednotky RipEX.

Pro další informace viz manuál, kapitolu *http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-graphs*.

1.8.3. SNMP

RipEX má implementovány SNMPv1/v2c a SNMPv3. Hodnoty poskytnuté RipEXem jsou uvedeny v MIB tabulce. RipEX také umožňuje generování SNMP Notification, když bylo dosaženo mezní hodnoty sledovaných hodnot: RSSI com, DQcom, TXLost [%], Ucc, Temp, PWR, PSV, ETH [Rx / Tx], COM1 [Rx / Tx], COM2 [Rx / Tx], HW Alarmový vstup a / nebo pro některá vnitřní varování a chyby.

Tabulku MIB pro RipEX najdete v dokumentu Application notes na odkazu *http://www.racom.eu/eng/products/m/ripex/app/snmp/MIB.html*, nebo na webu Racom na odkazu *http://www.racom.eu/download/hw/ripex/free/eng/3_fw/RACOM-RipEX-MIB.zip*.

1.8.4. Ping

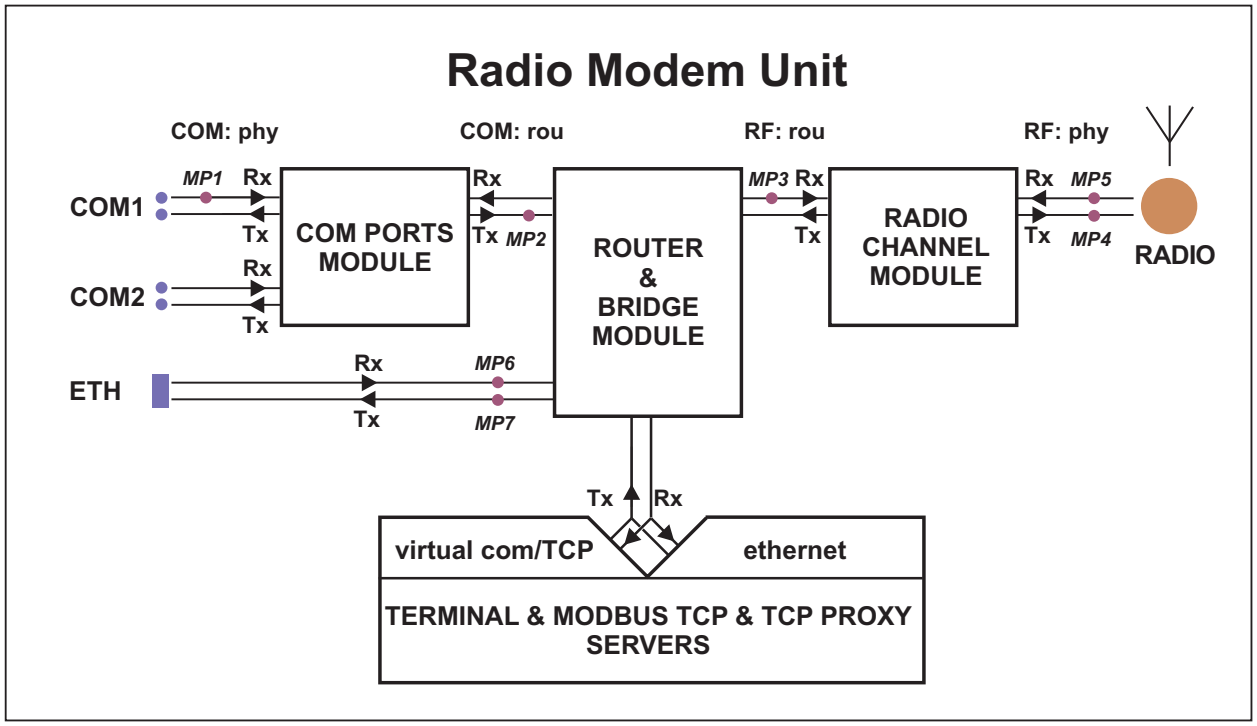
Pro diagnostiku jednotlivých rádiových linek je RipEX vybaven modifikovaným nástrojem Ping. Kromě standardních informací, jako je například počet odeslaných a přijatých paketů nebo doba odezvy, poskytuje celkovou zátěž, BER, PER a konkrétní údaje o kvalitě rádiového přenosu, RSS a DQ pro rádiové spojení na trase přenosu.

Podrobněji v kapitole *10.1 – „Ping“* .

1.8.5. Monitoring

Monitoring je moderní diagnostický nástroj, který umožňuje podrobnou on-line analýzu komunikace přes některá rozhraní routeru RipEX. Když je potřeba takové pokročilé diagnostiky, mohou být monitorována kromě všech fyzických rozhraní (RADIO, ETH, COM1, COM2) i některá vnitřní rozhraní mezi softwarovými moduly (například terminálové servery Modus TCP serveru atd.).

Výstup monitoringu lze prohlížet on-line, nebo jde uložit do souboru v RipEXu (i vzdáleném) a později jej stáhnout.



Obr. 1.3: Monitorovaná rozhraní

Podrobněji v kapitole *10.2 – „Monitoring“* .

1.9. Update a upgrade firmware

V nepravidelných časových intervalech jsou uvolňovány aktualizace firmware RipEXu (update nebo upgrade), které zlepšují funkčnost a/nebo opravují chyby. Tyto aktualizace lze stáhnout zdarma z internetových stránek *http://www.racom.eu*.

Aktualizace firmware přináší významná vylepšení a nové funkce, které posouvají produkt firmy Racom na novou úroveň. Stažení a použití upgrade firmwaru je stejné jako u update firmwaru. Pro aktivaci nové funkce nebo samotné aktualizace však bude možná muset být zakoupen softwarový klíč (viz další kapitolu).

Další informace viz kapitolu *http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-fw*.

1.10. Softwarové klíče

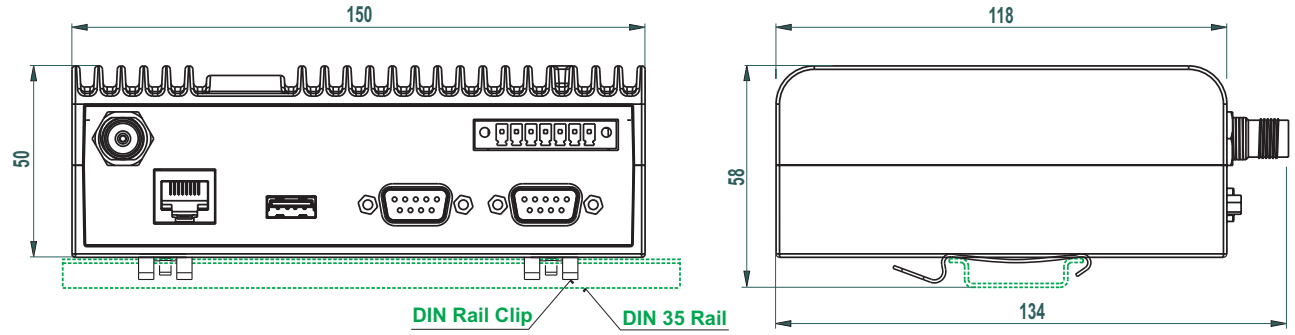
Některé pokročilé funkce RipEXu jsou aktivovány softwarovými klíči. Softwarové klíče umožňují uživatelům nejprve koupit pouze funkčnost, kterou potřebují, a později dokoupit další funkce s tím, jak jeho požadavky a očekávání porostou. A podobně, když některé funkce (např. COM2) jsou vyžadované jen na určitých místech, odpovídající klíč může být aktivován pouze v případě potřeby.

- Klíče ochraňují investice do hardwaru. Díky SDR na bázi hardwaru návrženého přímo pro RipEX není nutná fyzická výměna – uživatel si jednoduše koupí klíč a aktivuje funkci.
- Na zkoušky a testování mohou být dodány časově omezené klíče. Tyto klíče aktivují funkci pomocí kódu jednou na omezenou provozní dobu (po zapnutí). Zdarma je v každém RipEX Master-key na zkušební dobu 30 dnů .
- Všechny softwarové klíče jsou vždy vázány na konkrétní RipEX výrobním kódem.

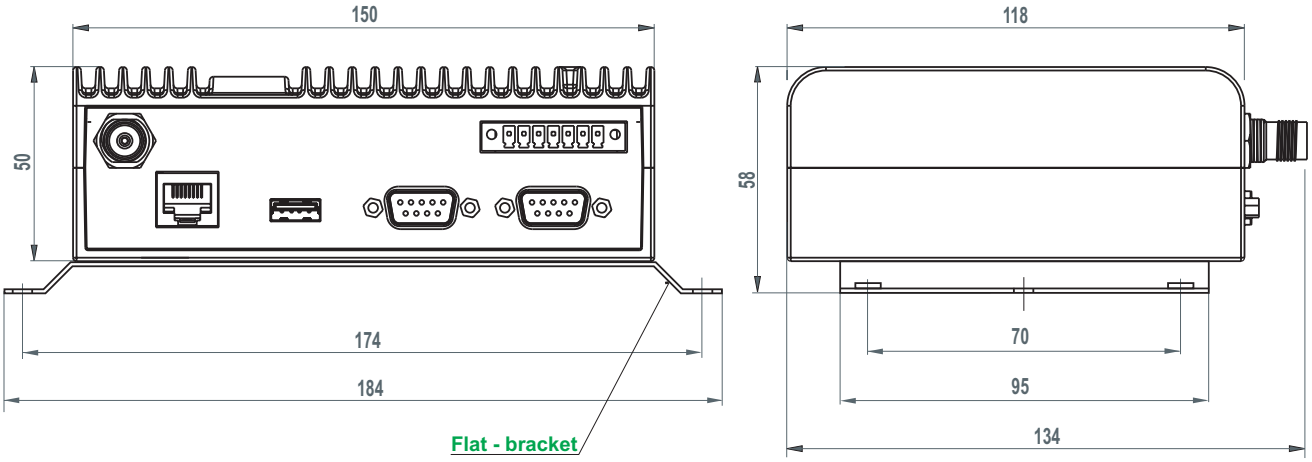
Podrobnosti najdete v kapitole *http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-sw-keys*.

2. Popis

Rozměry



Obr. 2.1: Rozměry RipEXu



Obr. 2.2: Plochý montážní držák

Indikační LED

Tab. 2.1: Funkce LED

Obr. 2.3: Indikační LED

	Barva	**Popis**
STATUS	Zelená	OS RipEXu (Linux) správně pracuje
	Zhasnuto	tlačítko Reset bylo stisknuto
	Zelená pomalu bliká	reset po 5 s stisku tlačítka
	Zelená rychle bliká	defaultní přístupové parametry po 15 s stisku tlačítka
	Červená rychle bliká	Emergency
	Červená	alarmový stav
TX	Zelená bliká s periodou 1 s	GPS modul synchronizován, pouze pro model RipEX-xxxG
	Červená	vysílání na rádiový kanál
RX	Zelená	přijímač se synchronizoval na paket
	Žlutá	na rádiovém kanálu je signál silnější než −80 dBm
COM2	Zelená	příjem dat

	Barva	**Popis**
	Žlutá	vysílání dat
COM1	Zelená	příjem dat
	Žlutá	vysílání dat
ETH	Žlutá ON	rychlost 100 Mb/s
	Žlutá OFF	rychlost 10 Mb/s
	Zelená ON	připojeno
	Zelená bliká	ethernet data
PWR	Zelená	napájení zapnuto
	Bliká s periodou 1 s	Save mód
	Bliká jednou za 3 s	Sleep mód

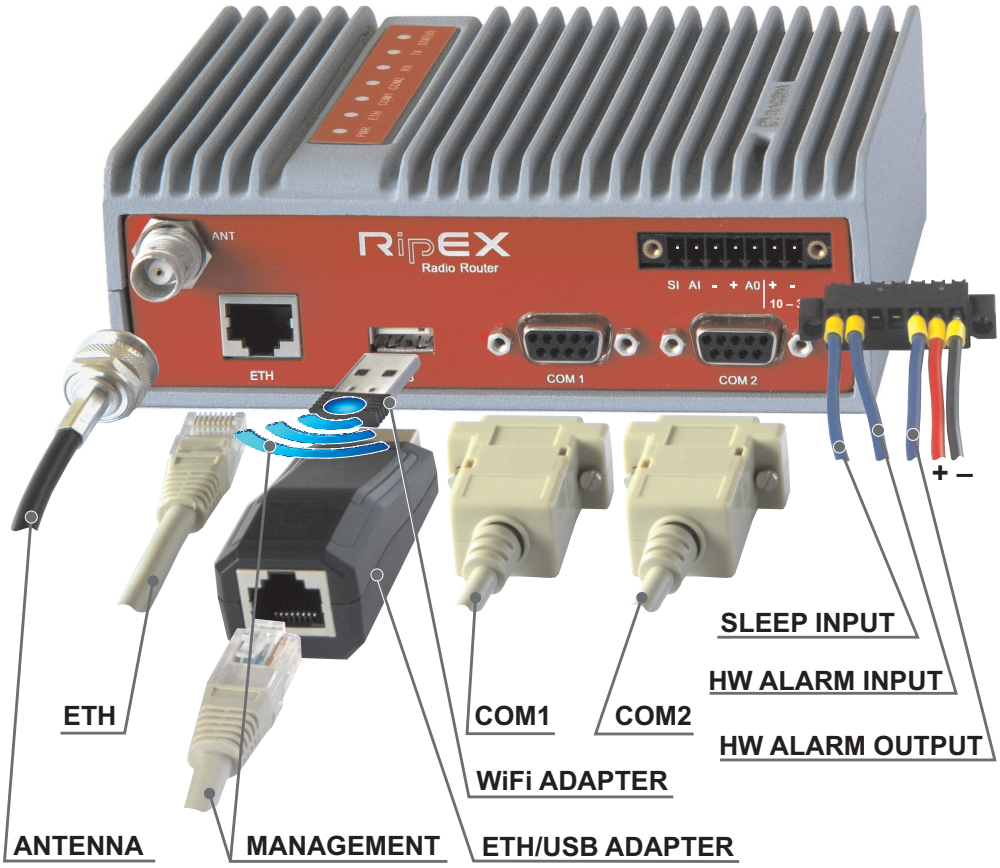
Alarmový stav – je zapnutý, když jakákoliv ovládaná položka v menu „Alarm management“ (viz RipEX manual, Adv. config., *Settings / Alarm management*[1]) je ve stavu alarmu (mimo mezní hodnoty) a jsou zkontrolovány "SNMP Notification", "HW Alarm Output" nebo "Detail graphs start" pro každou řádku v Alarm configuration table.

Stav nouze – Nouzový stav je nedefinovaný stav RipEXu buďto z důvodu SW nebo HW problému, když RipEX nepracuje správně. Funkce webové stránky jsou většinou k dispozici i v havarijním stavu. V případě, že problém nelze odstranit vypnutím a zapnutím zařízení, zašlete jej na firmu RACOM k opravě.

2.1. Konektory

Všechny konektory rádiového routeru RipEX jsou umístěny na předním panelu. Vrchní strana je vybavena panelem s LED. Tlačítko RESET je umístěno v otvoru na spodní straně routeru.

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



Obr. 2.4: Konektory routeru RipEX

Varování – prostředí s nebezpečím výbuchu

Nemanipuluje zařízením RipEX (neodpojujte napájení ani jiné konektory), pokud není vypnuté nebo pokud je v prostředí s nebezpečím výbuchu.

2.1.1. Anténa

Anténa se připojí k radiomodemu RipEX přes 50Ω konektor TNC female.

Na objednávku může být dodáván model se dvěma anténními konektory. Toto řešení se obvykle používá na komunikačních stožárech, kde je jedna Rx a jedna Tx anténa společná pro všechna zařízení.

Obr. 2.5: Anténní konektor TNC

Poznámka

Frekvenční odstup (rozdílná Rx a Tx frekvence) je nezávislý na přítomnosti dvou anténních konektorů. Rozdílnou frekvenci Rx a Tx lze nastavit i na standardním RipEXu s jedním anténním konektorem.

Varování – prostředí s nebezpečím výbuchu

Anténa musí být nainstalována mimo zónu s nebezpečím výbuchu.

Obr. 2.6: Oddělené antény Rx a Tx

Varování: Při provozu bez antény nebo umělé zátěže může dojít k poškození rádiového modemu RipEX.

2.1.2. Napájecí konektor

Tento odolný konektor slouží k přivedení napájecího napětí do RipEXu a k připojení řídicích signálů. Konektor se šroubovými svorkami a upevňovacími šrouby pro napájení je dodáván s každým routerem RipEX. Pro připojení se používá konektor Tyco 7 pin terminal block plug, part No. 1776192-7, rozteč 3,81 mm. Konektor je určen pro elektrické vodiče o průřezu 0,5 až 1,5 mm^2. Odizolovaný konec vodiče by měl být dlouhý 6 mm. Tyto konce by měly být před vložením do svorky opatřeny koncovkami PKC 108. Po vložení vodičů do svorek bezpečně utáhněte šroubky.

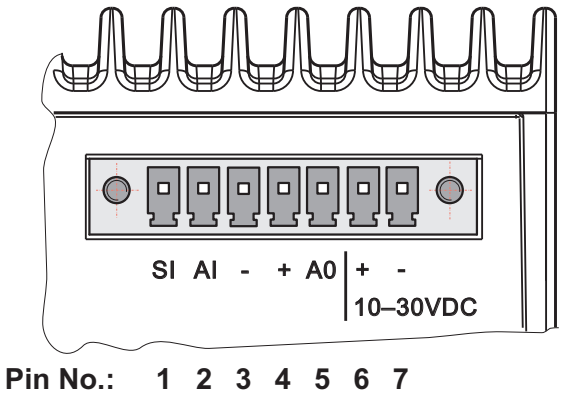
Tab. 2.2: Funkce pinů napájecího konektoru

Pin	Označeno	Signál
1	SI	SLEEP INPUT
2	AI	HW ALARM INPUT
3	−	−(GND) – for SLEEP IN, HW ALARM INPUT
4	+	+(POWER) – for HW ALARM OUTPUT
5	AO	HW ALARM OUTPUT
6	+ 10−30VDC	+ POWER (10 to 30 V)
7	− 10−30VDC	− POWER (GND)

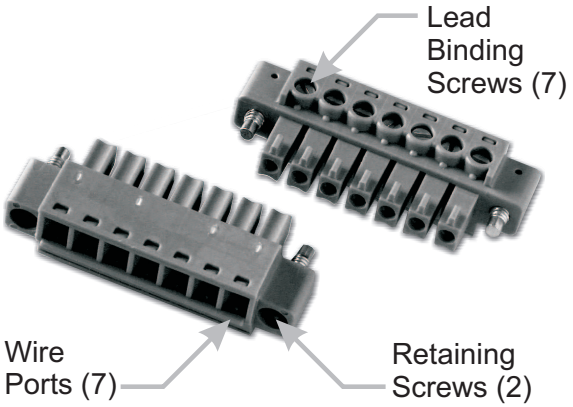
Piny 3 a 7 a piny 4 a 6 jsou uvnitř propojeny.

Varování – prostředí s nebezpečím výbuchu

Při použití v prostředí s nebezpečím výbuchu musí být zařízení napájeno jiskrově bezpečným zdrojem.



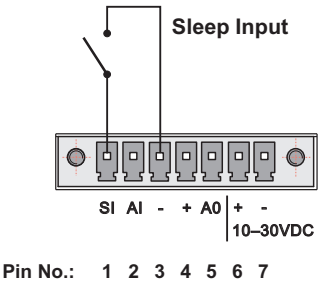
Obr. 2.7: Napájecí konektor



Obr. 2.8: Šroubové svorky pro napájecí konektor

SLEEP INPUT (vstup signálu SLEEP)

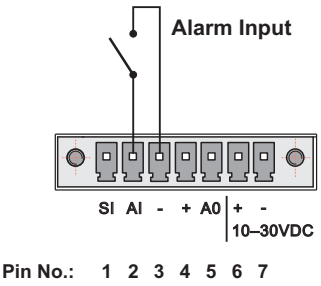
SLEEP INPUT je digitální vstup pro aktivaci režimu spánku. Je-li tento pin uzemněný (např. připojením k pinu 3), RipEX se přepne do režimu spánku. Při použití „Power managementu“ (*Advanced Configuration*[2]) může být přechod do režimu spánku zpožděn o nastavený čas. Odpojení SLEEP vstupu z GND (-) režim spánku ukončí. RipEXu trvá probuzení z režimu spánku 48 sekund.



SLEEP INPUT lze použít také pro probuzení ze stavu save módu. Podrobnosti viz kapitola (*Advanced Configuration*[3], Power management – řízení spotřeby).

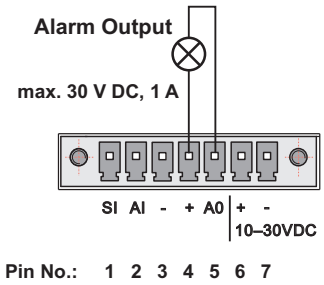
HW ALARM INPUT (Alarmový vstup)

HW ALARM INPUT je digitální vstup. Pokud je uzemněný (např. připojením k pinu 3), spustí se externí alarm. Tento alarm může být použit například pro přenos informace pomocí SNMP Notification, informuje třeba o výpadku proudu nebo problému zařízení RTU. Další informace o řízení alarmů viz kapitola *Advanced Configuration*[4].



[2] http://www.racom.eu/eng/products/m/ripex/h-menu.html
[3] http://www.racom.eu/eng/products/m/ripex/h-menu.html
[4] http://www.racom.eu/eng/products/m/ripex/h-menu.html

HW ALARM OUTPUT (Alarmový výstup)



HW ALARM OUTPUT je digitální výstup. Může být aktivován v menu Alarm management settings, kapitola *Advanced Configuration*[5]. Funkce může být použita například pro informování připojené RTU o alarmu RipEXu nebo o tom, že jednotka je v připraveném stavu. Pokud se spustí alarm, HW ALARM OUTPUT je vnitřně spojen s GND. Pokud externí zařízení vyžaduje připojení ke kladnému pólu napájení, měl by být použit PIN 4.

NAPÁJENÍ

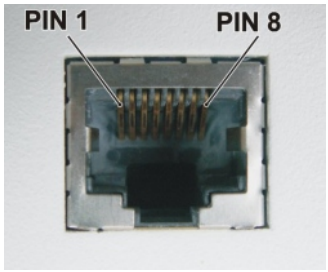
Napájecí piny označené + a - slouží k připojení napájení 10–30 VDC. Požadavky na napájení jsou definovány v kapitolách *4.6 – „Napájení“* a *3 – „Technické parametry“*.

2.1.3. ETH

Pro připojení Ethernetu je používán standardní konektor RJ45. RipEX má rozhraní 10/100 BaseT Auto MDI/MDIX, takže lze připojit k ethernetové síti až10 Mb/s nebo 100 Mb/s. Rychlost lze zvolit buďto ručně nebo ji automaticky rozpozná RipEX. RipEX je vybaven funkcí Auto MDI/MDIX, která mu umožňuje připojení přes standardní i křížové kabely, automaticky se přizpůsobí použitému kabelu.

Zapojení pinů na konektoru

Tab. 2.3: Připojení kabelu ETH ke konektoru



Obr. 2.9: RJ-45F

Pin	Signál	Přímý kabel	Křížený kabel
1	TX+	oranžová – bílá	zelená – bílá
2	TX−	oranžová	zelená
3	RX+	zelená – bílá	oranžová – bílá
4	—	modrá	modrá
5	—	modrá – bílá	modrá – bílá
6	Rx−	zelená	oranžová
7	—	hnědá – bílá	hnědá – bílá
8	—	hnědá	hnědá

[5] http://www.racom.eu/eng/products/m/ripex/h-menu.html

2.1.4. COM1 a COM2

U rádiového routeru RipEX lze využít dvě sériová rozhraní COM1 a COM2 ukončená DB9F konektorem. COM1 je vždy RS232, COM2 může být nakonfigurován jako RS232 nebo RS485 (více v anglickém manuálu *http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-com*).

Sériové rozhraní RipEXu RS232 je zapojeno jako zařízení DCE (Data Communications Equipment). Zařízení připojená k sériovým portům RipEXu by měla být typu DTE (Data Terminal Equipment) a měl by být použit přímý ethernetový kabel pro jejich připojení. Je-li k sériovým portům RipEXu připojeno zařízení DCE, musí být použit křížený ethernetový kabel (nullmodem kabel).

Tab. 2.4: Popis pinů COM1,2

Obr. 2.10: Sériové rozhraní

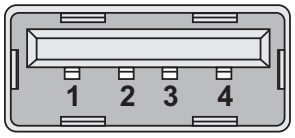
DSUB9F	COM1, 2 – RS232		COM2 – RS485	
Pin	**Signál**	**In/ Out**	**Signál**	**In/ Out**
1	CD	Out	—	
2	RxD	Out	line B	In/Out
3	TxD	In	line A	In/Out
4	DTR	In	—	
5	GND		GND	
6	DSR	Out	—	
7	RTS	In	—	
8	CTS	Out	—	
9	—	—	—	

RipEX trvale drží pin 6 DSR na úrovni logické 1 podle standardu RS232.

2.1.5. USB

RipEX používá sériové rozhraní USB 1.1 Host. USB rozhraní je zapojeno podle standardu:

Tab. 2.5: Popis pinů USB



Obr. 2.11: Konektor sériového rozhraní

USB pin	Signál	Vodič
1	+5 V	červený
2	Data(−)	bílý
3	Data (+)	zelený
4	GND	černý

USB rozhraní je určeno pro připojení k externímu – ETH / USB adaptéru nebo k WiFi adaptéru. Ty jsou volitelným příslušenstvím RipEXu. Tyto adaptéry jsou určeny pro servisní přístup k webovému konfiguračnímu rozhraní RipEXu.

Rozhraní USB lze také použít pro připojení externího flash disku speciálně navrženého tak, aby se zjednodušily složité úkoly údržby. Jednoduché plug-in úkoly tak mohou být prováděny i nekvalifikovaným pracovníkem, který pouze musí počkat, dokud bliká LED dioda USB disku.

Konektor USB také poskytuje zdroj napájení (5 V / 0,5 A). Může být použit pro dočasné napájení připojeného zařízení, například telefonu. Konektor USB by neměl být využíván jako trvalý zdroje napájení.

Poznámka – prostředí s nebezpečím výbuchu

Pouze zařízení určená pro prostředí s nebezpečím výbuchu mohou zůstat trvala připojena k USB rozhraní.

Externí USB flash disk

Externí USB flash disk může být použit pro upgrade firmwaru, nahrávání SW klíče, zálohování a obnovu konfigurace, nahrání SSL certifikátu a SSH klíče a stažení balíčku pro technickou podporu. K těmto účelům může být použit jakýkoliv běžný USB flash disk s několika megabajty volného místa.

Poznámka

USB flash disk musí mít souborový systém FAT32 (nejpoužívanější v době psaní tohoto textu). Jakýkoli jiný souborový systém bude RipEX prostě ignorovat. V případě pochybností se obraťte na svého IT odborníka.

Jakmile RipEX rozpozná flash disk vložený do USB rozhraní, stavová LED začne pomalu blikat, střídavě červenou a zelenou barvou. To označuje začátek uploadu / downloadu souborů. Blikání LED se v průběhu procesu může měnit, úspěšné dokončení nahrávání je indikováno rychlým střídavým blikáním červené a zelené barvy (asi 3 krát za sekundu). To může trvat až 10 minut (je-li proveden upgrade FW).

Varování

Nikdy neodpojujte USB disk dříve, než začne LED signalizovat rychlým blikáním správný stav! Jinak by mohlo dojít k poškození disku.

Po úspěšném zjištění flash disku v USB rozhraní, RipEX na něj zapíše tech-support balíček, log files a k němu textový konfigurační soubor. Potom zapíše do kořenového adresáře disku README.txt soubor, který obsahuje všechny potřebné informace o struktuře s názvy souborů a adresářů. Postupujte prosím podle podrobných pokynů v tomto souboru README.txt.

Poznámka

Kdykoli se nachází v kořenovém adresáři disku soubor FW (.cpio), provede se automaticky upgrade, bez ohledu na verzi aktuálně aktivního FW. Pokud je nalezen více než jeden soubor FW použíje se nejnovější verze. Pokud nemáte v úmyslu provést upgrade, nezapomeňte odstranit soubory FW z kořene disku. Stejné zásady platí také pro aktualizaci konfigurace z disku.

2.1.6. Resetovací tlačítko

Resetovací tlačítko se nalézá na spodní straně routeru RipEX a je přístupné otvorem v pouzdru. Po stisknutí tohoto tlačítka dioda STATUS na LED panelu zhasne (což znamená, že bylo stisknuto tlačítko). Pokud podržíte tlačítko po dobu 5 sekund, dioda STATUS začne pomalu blikat, což znamená, že proběhlo resetování. Pokud i nadále podržíte tlačítko po dobu 15 sekund nebo déle (dioda STATUS začne blikat rychle) a potom jej uvolníte, obnovíte výchozí přístupové údaje daného zařízení:

Obr. 2.12: Umístění resetovacího tlačítka

ETH IP and Mask:	192.168.169.169/24
ETH Default GW:	0.0.0.0
ETH Speed:	Auto
DHCP:	Off
ARP proxy & VLAN:	Off
Firewall:	Off
Hot Standby:	Off
Routing table:	Deleted
Management:	Default (Web server=HTTP+HTTPS, CLI=SSH)
Username:	admin
Password:	admin

Poznámka

Chcete-li resetovat RipEX, použijte tlačítko RESET, jak je popsáno výše, nebo použijte tlačítko konfigurace RipEXu ve webovém prohlížeči, viz manuál *http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-miscell*. Nikdy nepoužívejte pro resetování odpojení a opětovné připojení napájení. Zatímco se hardware RipEXu restartuje, jeho software se správně neukončí, což má za následek, že neproběhne řádné uložení záznamů statistik a grafů.

2.1.7. GPS

Rádiový router RipEX může být vybavený interním GPS, viz *Model offerings*[6]. Modul GPS se používá pro synchronizaci času z NTP serveru uvnitř RipEXu. Viz *Time*[7] pro další informace. V případě, že RipEX má GPS modum panelu konektor SMA 50 Ω pro připojení antény GPS.

Obr. 2.13: SMA konektor pro GPS

[6] http://www.racom.eu/eng/products/m/ripex/product.html#model
[7] http://www.racom.eu/eng/products/m/ripex/h-menu.html#h-ntp

3. Technické parametry

Rádiové parametry	
Kmitočtová pásma	135–154; 154–174; 215-240; 300–320; 320–340; 340–360; 368–400; 400–432; 432–470; 470–512; 928–960 MHz
Šířka kanálu	6,25 / 12,5 / 25 / 50 kHz [1]
Frekvenční stabilita	±1.0 ppm
Modulace	QAM (linear): 16DEQAM, D8PSK, π/4DQPSK, DPSK FSK (exponencial): 4CPFSK, 2CPFSK
Datová rychlost (max)	> 200 kbps@50 kHz; >100 kbps@25 kHz; >50 kbps@12.5 kHz; >25 kbps@6.25 kHz [2]
FEC (Forward Error Correction)	On/Off, ¾ Trellis code with Viterbi soft-decoder

Vysílač	
Výstupní výkon	QAM: 0.5 - 1.0 - 2.0 W [3] FSK: 0.1 - 0.2 - 0.5 - 1.0 - 2.0 - 3.0 - 4.0 - 5.0 - 10 W [4]
Provozní cyklus	Kontinuální
Čas přepnutí Rx na Tx	< 1.5 ms
Intermodulation Attenuation	> 40 dB
Spurious Emissions (Conducted)	< −36 dBm
Radiated Spurious Emissions	< −36 dBm
Adjacent channel power	< −60 dBc
Transient adjacent channel power	< −60 dBc
Přijímač	
Citlivost	viz *detail*[1]
Anti-aliasing Selectivity	50 kHz @ −3 dB BW
Čas přepnutí Tx na Rx	< 1.5 ms
Max. výkon na vstupu přijímače	20 dBm (100 mW)
Rx Spurious Emissions (Conducted)	< −57 dBm
Radiated Spurious Emissions	< −57 dBm
Spurious response rejection	> 70 dB

[1] Kanálování 50 kHz je HW závislé. Ve výrobě jsou ještě starší desky, proto prosím ve své objednávce specifikujte případný požadavek na 50 kHz kanálování.
6.25 kHz kanálování není dostupné pro RipEX-928.

[2] V tabulce je uvedena přibližná datová rychlost. Uživatelská datová rychlost je proměnlivá a silně závisí na struktuře dat, účinnosti optimalizace, protokolu na rádiovém kanálu, kvalitě signálu a na mnoha dalších parametrech sítě. Doporučujeme provést praktické testy.

[3] Výstupní výkon je udáván jako průměrná hodnota. Max. špičkový výkon (PEP) je 7.0 W.

[4] Pro vysílací výkon 10 W se doporučuje užít napájecí napětí vyšší než 11 VDC
RipEX-470 – max. RF výstupní výkon 8 W.

Další technické parametry viz: *http://www.racom.eu/eng/products/m/ripex/product.html#tech-spec*.

[1] http://www.racom.eu/eng/products/m/ripex/product.html#det_param

Při přidělování kmitočtů vychází ČTÚ i z podmínky, že zabraná šířka pásma pro kanálovou rozteč 25 kHz je maximálně 16 kHz a pro kanálovou rozteč 12,5 kHz pak 11 kHz. Některé modulace použité v rádiovém modemu RipEX tuto hodnotu překračují, a proto lze v ČR použít pouze následující rychlosti viz tabulky:

Tab. 3.1: 25 kHz - maximální zabraná šířka pásma do 16 kHz

Nastavení v RipEXu				
Rozteč kanálů [kHz]	Nastavení	Modulační rychlost [kbps]	Modulace	Emisní kód
25	Narrow	10,42	2CPFSK	13K8F1DBN
25	Narrow	20,83	4CPFSK	14K2F1DDN
25	Narrow	13,89	DPSK	15K9G1DBN
25	Narrow	27,78	π/4-DQPSK	15K9G1DDN
25	Narrow	41,67	D8PSK	15K9G1DEN
25	Narrow	55,56	16DEQAM	15K9D1DEN

Tab. 3.2: 12,5 kHz - zabraná šířka pásma do 11 kHz

Nastavení v RipEXu				
Rozteč kanálů [kHz]	Nastavení	Modulační rychlost [kbps]	Modulace	Emisní kód
12,5	CE	5,21	2CPFSK	7K00F1DBN
12,5	CE	10,42	4CPFSK	7K00F1DDN
12,5	FCC	17,36	π/4-DQPSK	10K0G1D
12,5	FCC	26,04	D8PSK	10K0G1D
12,5	FCC	34,72	16DEQAM	10K0D1D

4. Instalace zařízení

Step-by-step checklist / Instalace po krocích

1. Montáž routeru RipEX do skříně.
2. Instalace antény.
3. Instalace napájecího vedení antény.
4. Řádné uzemnění zařízení.
5. Natažení kabelů a zapojení všech konektorů s výjimkou zařízení.
6. Připojení RipEXu k napájení.
7. Připojení PC na konfiguraci.
8. Nakonfigurování RipEX.
9. Otestování kvality rádiového spojení.
10. Zkontrolování routingu pomocí příkazu *ping*, zda jsou dostupné všechny IP adresy, se kterými bude jednotka komunikovat.
11. Připojení zařízení.
12. Otestování aplikace.

Poznámka - prostředí s nebezpečím výbuchu

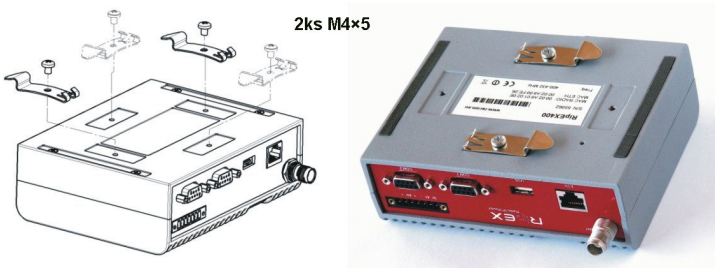
Instalace v prostředí s nebezpečím výbuchu musí být provedena v souladu s normou EN 60079-25 Výbušné atmosféry – Část 25: Jiskrově bezpečné elektrické systémy

4.1. Montáž zařízení

4.1.1. Montáž na DIN lištu

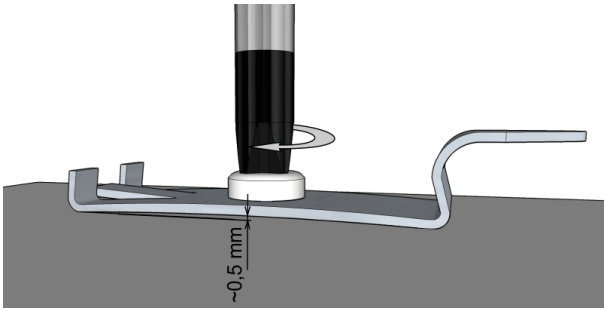
Rádiový modem RipEX se montuje přímo na DIN lištu pomocí příchytky. Montáž může být provedena na délku (doporučeno) nebo na šířku; v obou případech s RipEXem naplocho. Volba montáže na šířku nebo na délku se provádí umístěním příchytek. Každá příchytka je připevněna jedním šroubem M4. RipEX je dodáván se dvěma příchytkami a dvěma šrouby. Na spodní straně modemu jsou pro ně 4 závitové otvory. Používejte pouze šrouby M4×5 mm, které jsou součástí dodávky. Použitím nesprávných šroubů může dojít k poškození základní desky se součástkami v RipEXu!

Obr. 4.1: Montáž na DIN lištu, naplocho – na délku (doporučený způsob)



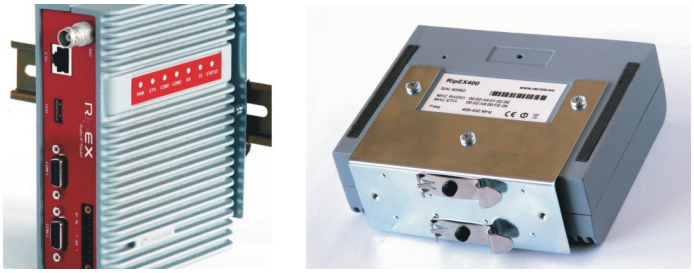
Obr. 4.2: Montáž na DIN lištu, naplocho – na šířku

Při utahování šroubu příchytky je třeba nechat mezeru 0,5 mm mezi příchytkou a tělem modemu.

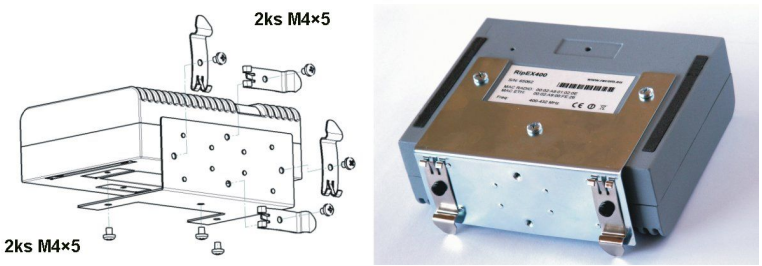


Obr. 4.3: Montáž příchytky

Pro vertikální montáž na DIN lištu se používá úhlový držák (volitelné příslušenství). Používejte pouze šrouby M4×5 mm, které jsou součástí dodávky. Použitím nesprávných šroubů může dojít k poškození základní desky se součástkami v RipEXu!



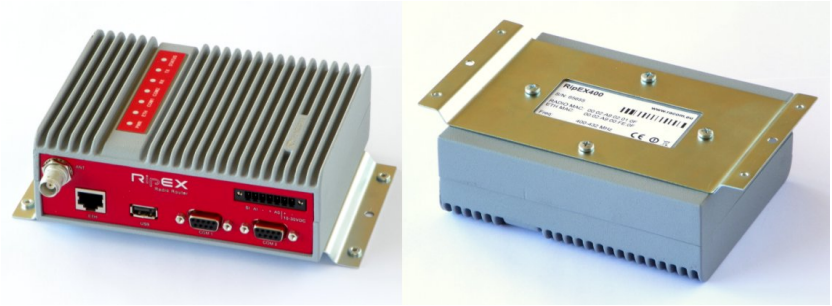
Obr. 4.4: Montáž na DIN lištu, vertikálně – na šířku



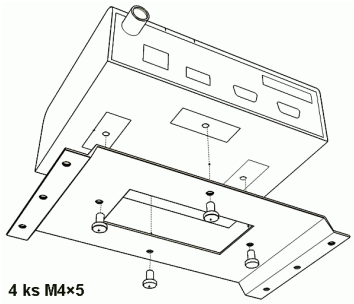
Obr. 4.5: Montáž na DIN lištu, vertikálně – na délku

4.1.2. Flat mounting / Montáž na plocho

Pro montáž na plocho – přímo na desku, je nutné použít plochý držák (volitelné příslušenství). Používejte pouze čtyři šrouby M4×5 mm, které jsou součástí dodávky. Použitím nesprávných šroubů může dojít k poškození základní desky se součástkami v RipEXu!



Obr. 4.6: Montáž na plocho s plochým držákem



Obr. 4.7: Připevnění plochého držáku k modemu RipEX

4.1.3. Montáž do skříně 19" rack

K instalaci do 19" racku můžete použít 19" polici jednoduchou nebo dvojitou pro jeden nebo dva radiomodemy RipEX. 19" rack police jsou volitelným příslušenstvím a jsou dodávány s napájením nebo bez něj.

Obr. 4.8: 19" rack police – dvojitá a jednoduchá

4.2. Montáž antény

Nejvhodnější typ antény pro každé místo v síti se určuje individuálně podle uspořádání sítě a podle požadavku na úroveň signálu. Při správném postupu určení typu antény se provádí terénní měření signálu přímo na místě. Na základě tohoto měření vznikne projekt, který stanoví nejenom typ antény, ale také její umístění, nasměrování, výšku nad terénem a typ použitého stožáru.

Anténní stožár by měl být volen s ohledem na rozměry a hmotnost antény, aby byla zajištěna odpovídající stabilita antény. Během instalace stožáru postupujte podle pokynů výrobce antény.

Anténa by nikdy neměla být nainstalována v blízkosti potenciálních zdrojů elektromagnetického rušení, zejména elektronických zařízení, jako jsou počítače nebo spínané napájecí zdroje. Typickým příkladem naprosto nesprávného umístění je montáž prutové antény přímo na horní stranu rozváděče obsahujícího veškerá průmyslová zařízení, která mají komunikovat přes radiomodem RipEX, včetně všech napájecích zdrojů.

Další bezpečnostní doporučení

Instalovat antény na stožárech a střechách nebo stěnách budov je oprávněn pouze kvalifikovaný personál s povolením pro práci ve výškách. Neinstalujte antény v blízkosti elektrických vedení. Antény a anténní držáky nikdy nesmí přijít do styku s elektrickými rozvody.

Anténa a anténní napáječe jsou elektrickými vodiči. Během instalace může vzniknout elektrostatický náboj, což by mohlo vést ke zranění. Při montáži nebo při opravě všech otevřených kovovvých částí musí být tyto části dočasně uzemněny.

Anténa a anténní napáječ musí být uzemněny po celou dobu montáže.

Neprovádějte montáž antény za nepříznivých povětrnostních podmínek, zejména za deště, silného větru a za bouře, nebo když je na pracovišti sníh nebo led.

4.3. Anténní napáječ

Vedení anténního napáječe by mělo být zvoleno tak, aby jeho útlum nepřesahoval 3 až 6 dB. Používejte pouze kabely s impedancí 50 Ω.

Čím kratší je anténní napáječ, tím lépe. Při velké vzdálenosti k dalšímu zařízení je lépe nainstalovat RipEX přímo ke stožáru antény a zbytek instalace a napájení připojit ethernetovým kabelem. Ethernetový kabel lze použít i pro jiné protokoly využívající sériový port, viz manuál *Advanced Configuration, Terminal server*[1]. Toto uspořádání je vhodné zejména tehdy, když by přívodní vedení bylo velmi dlouhé (delší než 15 metrů), a je potřeba dosáhnout malého útlumu na tomto vedení.

Vždy dodržujte všechna doporučení pro instalaci poskytovaná výrobcem kabelu (poloměr ohybu, atd.). Používejte vhodné konektory a pečlivě je zapojujte. Špatně připojené konektory zvyšují úroveň rušení a mohou způsobit nestabilitu rádiového spojení.

4.4. Uzemnění

Aby se minimalizovala možnost poškození vysílače a připojeného zařízení, je třeba zařízení bezpečně uzemnit (podle norem ČSN EN 62305-3, ČSN EN 332000-4-41 ed.2 a souvisejících norem) pospojováním anténního systému, vysílače, napájecího zdroje a připojeného datového zařízení do jednoho zemnícího bodu co nejkratším uzemňovacím vedením.

Rádiový modem RipEX se obecně považuje za dostatečně uzemněný, pokud se pro montáž použijí dodané ploché držáky rádiového modemu, přišroubované na řádně uzemněný kovový povrch. V případě, že rádiový modem není takto připojen k uzemněnému povrchu, je třeba připevnit bezpečnostní zemnicí vodič na jednu z montážních příchytek nebo ke šroubu na plášti rádiového modemu.

Na vstupu anténního napáječe do budovy se používá bleskojistka připojená k ochranné uzemnění budovy, pokud je to možné. Všechna uzemnění a veškerá kabelová vedení musí být v souladu s platnými zákony a předpisy.

4.5. Konektory

V konstrukci RipEXu byly použity standardní konektory. Používejte pouze standardní protikusy těchto konektorů.

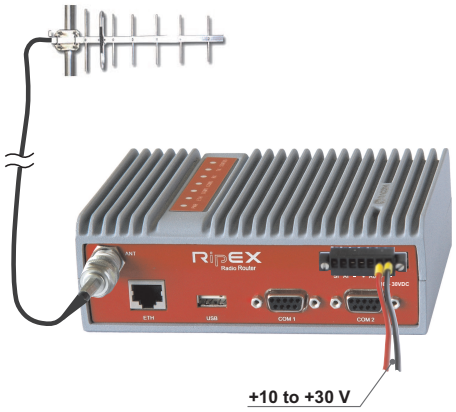
Zapojení všech konektorů najdete v manuálu v kapitole *Connectors*[2].

4.6. Napájení

Nedoporučujeme zapnutí napájecího zdroje Ripexu před připojením antény a dalších zařízení. Připojení RTU a dalších zařízení k RipEXu při zapnutém napájení zvyšuje pravděpodobnost poškození v důsledku vybití rozdílu elektrických potenciálů.

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

RipEX může být napájen jakýmkoliv dobře odfiltrovaným zdrojem energie o napětí 10 až 30 V DC. Zdroj musí poskytovat požadované vstupní hodnoty pro plánovaný RF výkon. Napájecí zdroj musí být dostatečně stabilní, aby nekolísalo napětí při přepínání radiomodemu z příjmu na vysílání, trvající méně než 1,5 ms. Aby se zabránilo rušení rádiového kanálu, musí napájení splňovat všechny příslušné normy EMC. Nikdy neinstalujte napájecí zdroj v blízkosti antény. Maximální délka napájecího kabelu je 3 m.



Obr. 4.9: Napájení10–30 VDC

Varování – prostředí s nebezpečím výbuchu

Zařízení musí být napájeno jiskrově bezpečným napájecím zdrojem pro použití v prostředí s nebezpečím výbuchu.

5. Záložní trasy

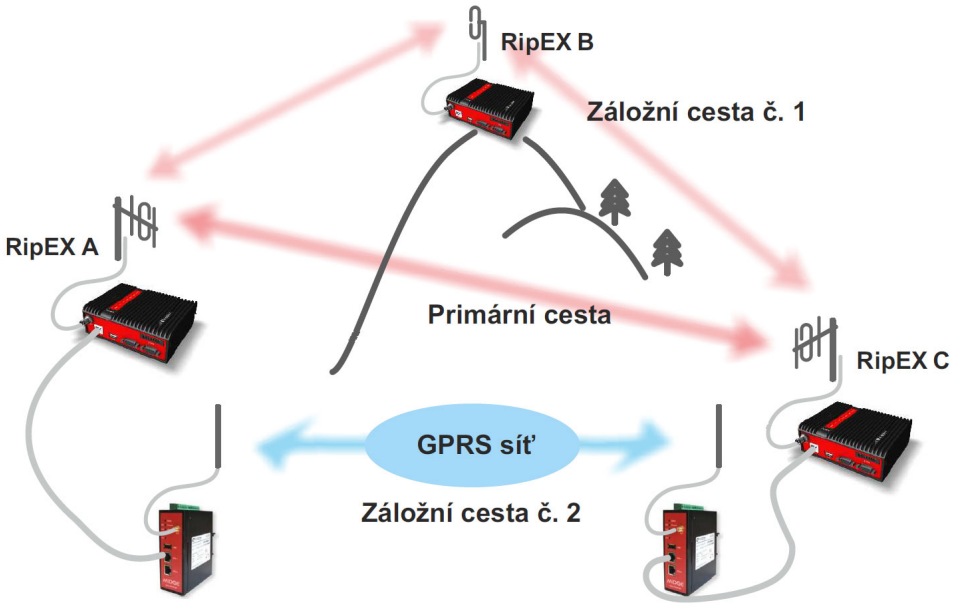
5.1. Úvod

RipEX využívá funkci **Záložní trasy** (Backup routes) pro zvýšení spolehlivosti v datových sítích prostřednictvím vytváření záložních cest.

V následujícím příkladu jsou pro trasu mezi zařízeními RipEX A a RipEX C tři možné cesty. Přímý rádiový spoj je nastaven jako primární cesta (protože je nejrychlejší). Cesta přes RipEX B je první záložní cesta (dva skoky), a záložní cesta přes GPRS síť je připravena v případě selhání rádiového spojení. V mobilních sítích je přenos dat zpoplatněný, proto je tu využit jako poslední možnost.

Prioritu cesty lze měnit podle daných požadavků. Cesta s nejvyšší prioritou je vždy primární volbou (v našem příkladu přímý rádiový spoj) a cesta s nejnižší prioritou je poslední možností (v našem příkladu GPRS síť).

Díky funkci **Záložní trasy** zvládne RipEX řešit různé problémy v síti, aniž by došlo k přerušení požadované komunikace.



Obr. 5.1: Příklad funkce Záložní trasy

Poznámka

Funkce **Záložní trasy** může být použita pouze v režimu Router mode.
Funkce zálohování tras podporuje SNMP.

5.2. Backup Routing Management Protocol

BRMP je proprietární protokol vyvinutý firmou RACOM. Ovládá funkce směrování záložních tras (Backup routing) v radiomodemech RipEX s ohledem na požadavky rádiových sítí.

Protokol

- nezatěžuje rádiové sítě
- umožňuje vytvoření jedné i více záložních tras
- řeší náhodné ztráty paketů
- umožňuje velmi rychlé přepínání cest v případě výpadku sítě

Protokol pracuje vždy mezi dvěma konkrétními rádiovými modemy RipEX. Každá síť s modemy RipEX může obsahovat různé záložní trasy a každá záložní trasa je tvořena několika alternativními cestami. Můžeme dokonce nastavit vnořené zálohovací cesty.

5.2.1. Postup protokolu

1. RipEX A rozesílá kontrolní „Hello“ pakety (UDP) všemi možnými cestami k jednotce RipEX C.
2. RipEX C tyto pakety přijímá a ukládá je i s informací o cestě, kterou pakety prošly.
3. RipEX C pošle seznam přijatých „Hello“ paketů ve svém „Hello“ paketu zpět k jednotce RipEX A.
4. RipEX A po obdržení tohoto „Hello“ paketu od jednotky RipEX C vyhodnocuje podmínky na jednotlivých cestách.

Jednotlivé alternativní cesty mohou nabývat následujících stavů:

Up	cesta je funkční a může být použita.
Down	cesta není funkční a nemůže být použita.
Unknown	stav cesty nemůže být vyhodnocen z důvodu nedostatku informací. Tento stav je aktivní ihned po spuštění radiomodemu RipEX, nebo není vyhodnocen, protože je používána cesta s vyšší prioritou a je nastaveno, že cesty s nižší prioritou se nevyhodnocují.

Volba trasy probíhá takto:

1. První trasa v tabulce Routing / Backup.
2. Při ztrátě spojení se přepne na následující trasu v tabulce Backup (režim Policy / Default).
3. Při zhoršení RSS se přepne na následující trasu v tabulce Backup (režim Policy / Manual).

5.3. Příklady konfigurace

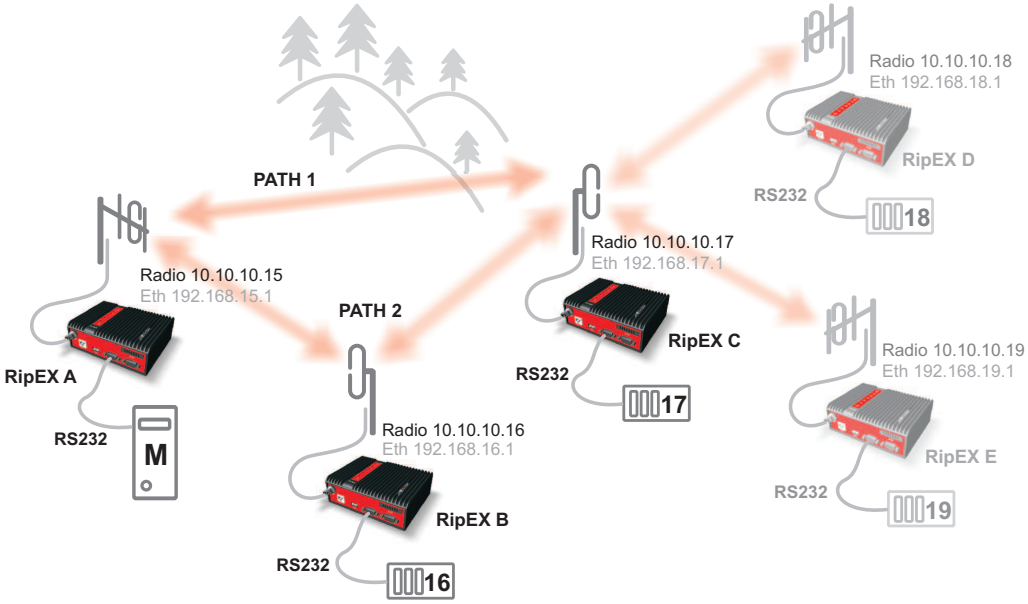
V této kapitole projdeme několik příkladů, abychom vysvětlili použití funkce **Záložní trasy** v praxi.

Projděte prosím postupně jeden příklad po druhém, abyste plně pochopili konfigurační odlišnosti a výhody různých řešení.

5.3.1. Rádio / záloha Rádio 1

Koncová zařízení připojená sériovým rozhraním.

V prvním příkladu tvoří síť pět radiomodemů RipEX. Všechna koncová zařízení jsou připojena k jednotkám RipEX přes sériové rozhraní. Je vhodné použít pouze rádiové IP adresy pro překlad a směrování dat. Ethernetové IP adresy mohou být přiřazeny náhodně (můžete ponechat výchozí nastavení, doporučujeme však pro pořádek nastavit ethernetové adresy podobně jako rádiové adresy).



Obr. 5.2: Topologie sítě 1

Zařízení připojené k jednotce RipEX A (10.10.10.15) je řídící stanice (Master), ostatní jsou podřízené (Slave).

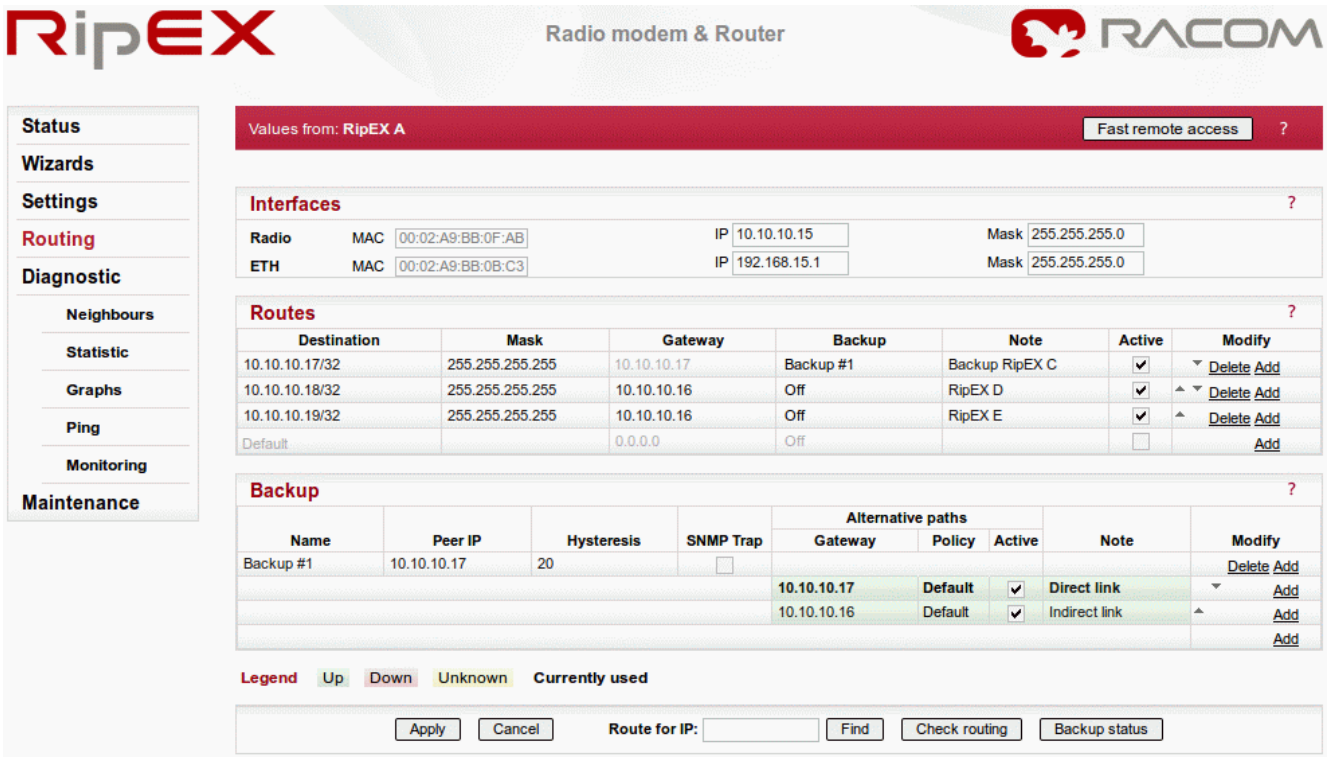
Poznámka

V této aplikační poznámce nebudeme konfigurovat rozhraní RS232.

Systém pro zálohování tras je možné použít mezi jednotkou RipEX A (.15) a jednotkou RipEX C (.17), pakety mohou být přenášeny:

- přímým rádiovým spojením mezi jednotkami RipEX A a RipEX C, nebo
- záložní (nepřímou) rádiovou cestou přes RipEX B.

Podívejte se na následující konfiguraci menu Routing jednotky RipEX A:



Obr. 5.3: Menu Routing pro RipEX A – příklad č. 1

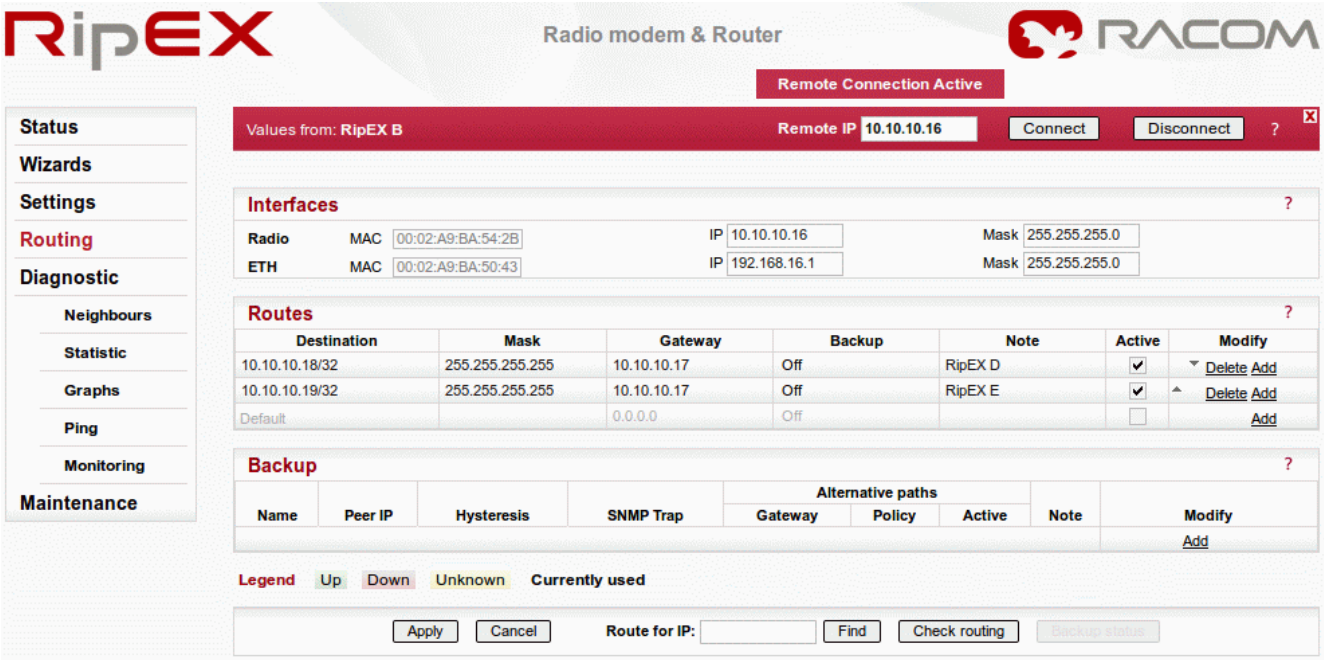
V jednotce RipEX A máme jednu trasu využívající **Backup** a dvě jednoduché trasy do dalších jednotek RipEX.

Záložní trasa je nazvaná „Backup # 1“ a její stav je kontrolovaný proti rádiové IP adrese jednotky RipEX C. Nejvyšší priorita je nastavena na přímou linku a druhou možností je použití jednotky RipEX B pro retranslaci. Obě trasy jsou nyní ve výchozím nastavení a jsou zaškrtnuty jako aktivní.

Poznámka

Použít lze buďto jen rádiovou nebo jen Ethernetovou adresu vzdálené jednotky RipEX (nelze použít IP adresy zařízení připojených za jednotkou RipEX).

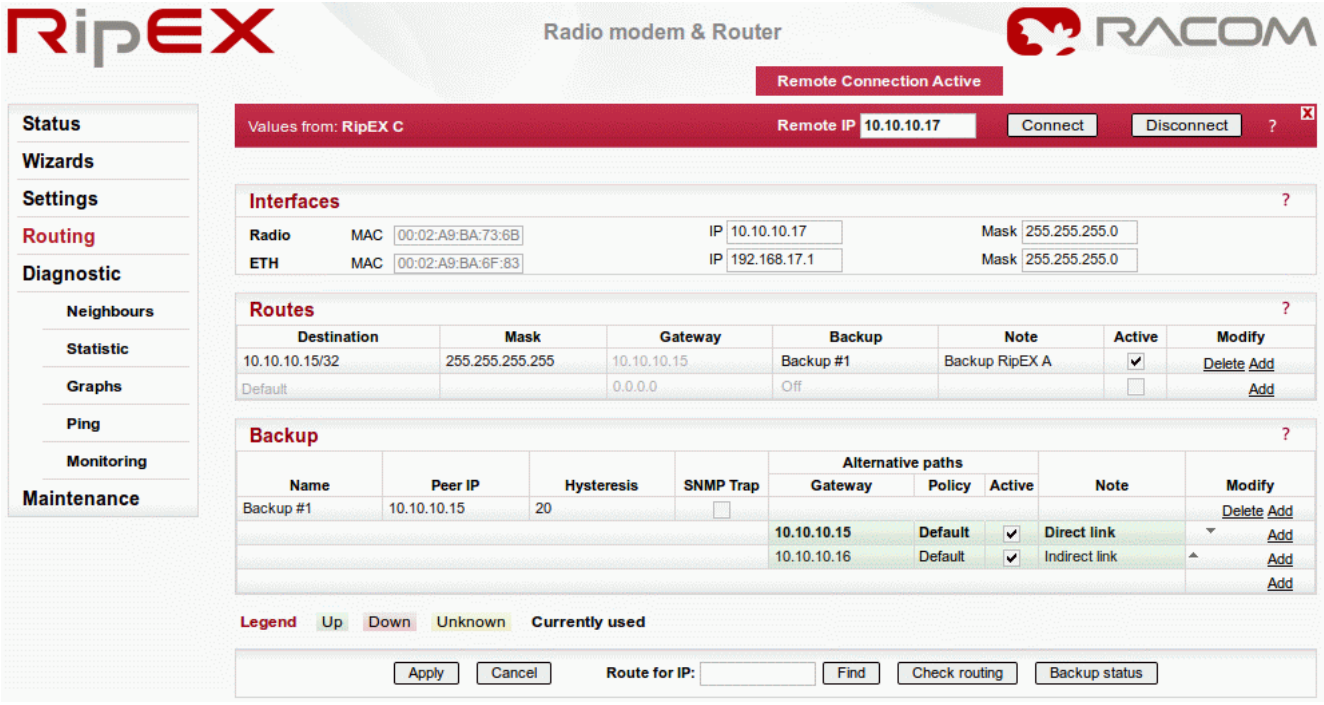
Podívejte se na příslušné konfigurace jednotek RipEX B a C.



Obr. 5.4: Menu Routing pro RipEX B – příklad č. 1

Poznámka

RipEX B není koncovým bodem (Peer IP) záložní trasy, proto v něm není záložní trasa definována.



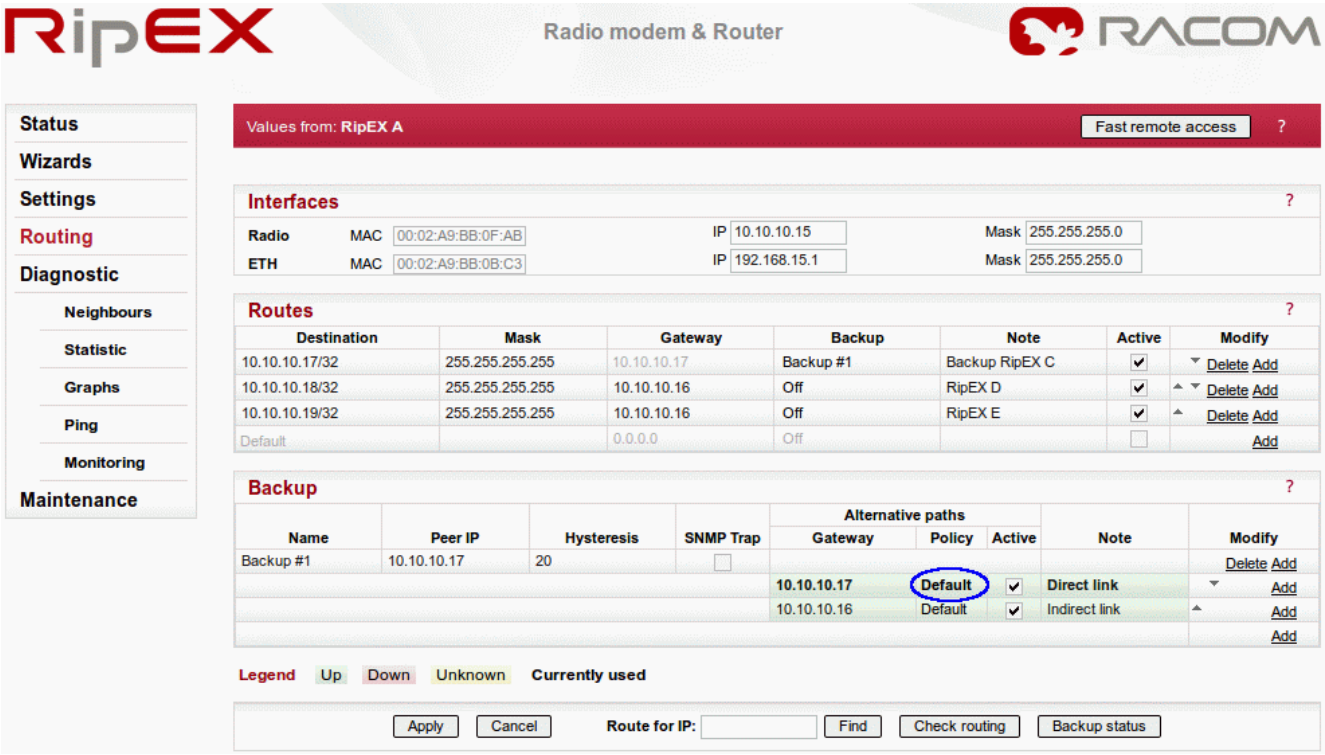
Obr. 5.5: Menu Routing pro RipEX C – příklad č. 1

Praktická zkouška

V tomto případě budeme přepínat na záložní trasu vzhledem ke kolísajícímu rádiovému signálu (velikost hodnoty RSS). Změníme proto nastavení ve sloupci Policy pro přímou linku (Direct link) a nastavíme RSS. Klikněte na příslušné tlačítko „Default“ ve sloupci Policy.

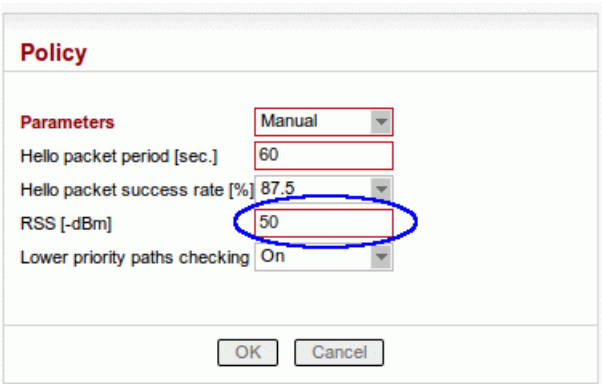
Poznámka

Spojení můžete zkontrolovat pomocí funkce Ping (**Diagnostic** → **Ping**).



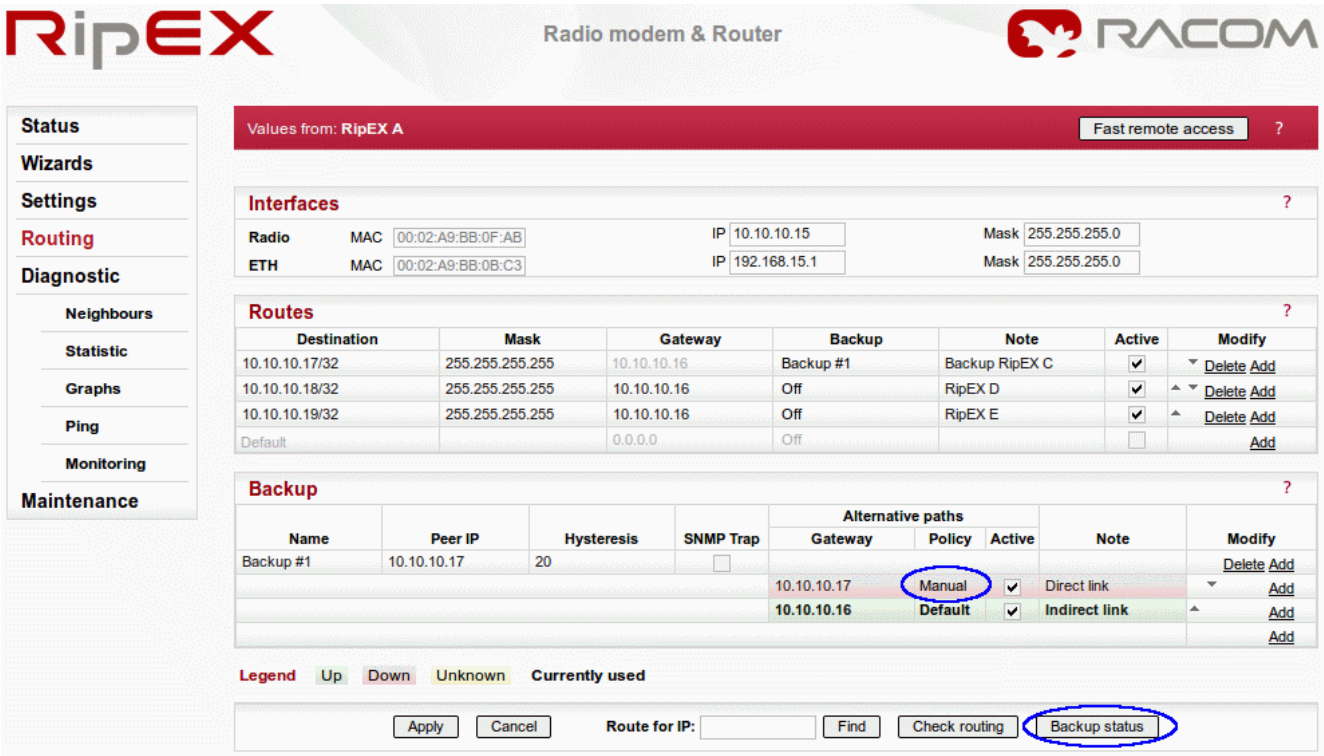
Obr. 5.6: RipEX A – Policy button

Zobrazí se nové okno. Změňte hodnotu v řádku Parameters na „Manual“ a vyplňte hodnotu v řádku RSSI [-dBm] podle aktuální RSS hodnoty (viz menu Neighbours). Hodnota musí být vyšší než je aktuální hodnota. V tomto příkladu je aktuální hodnota RSS -56 dBm a podmínka pro přepnutí na záložní (nepřímou) cestu je nastavena na -50 dBm.



Obr. 5.7: RipEX A – změna RSS záložní trasy

Uložte změny a klikněte na tlačítko „Backup status“, aby se zobrazily změny. Ve sloupci Policy je hodnota nastavena na "Manual" a záložní cesta je používána.



Obr. 5.8: RipEX A – záložní trasa je používána

Poznámka

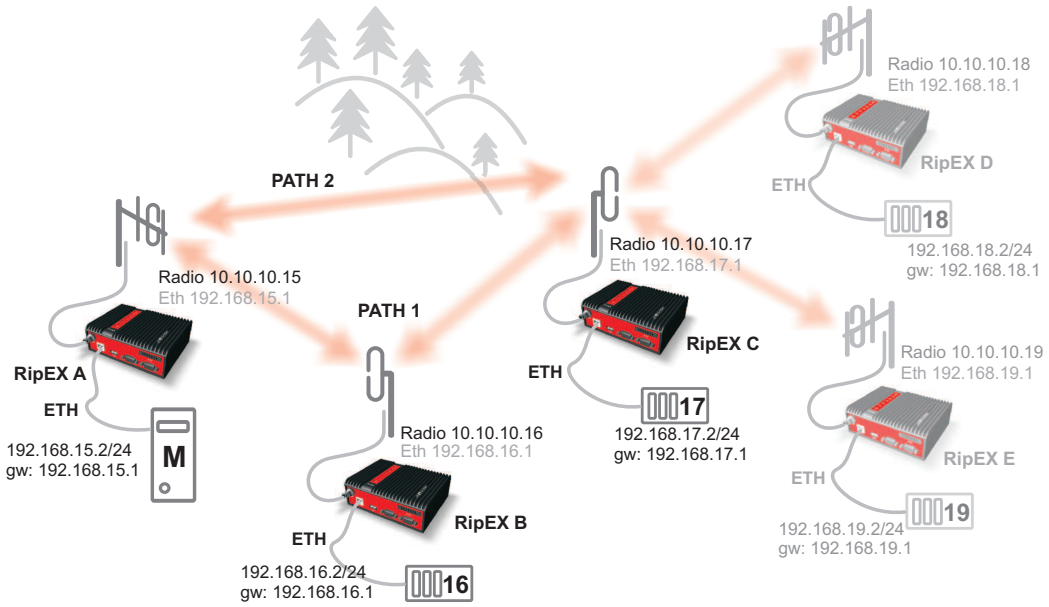
Pro správnou funkci nezapomeňte tyto kroky opakovat na protistanici – jednotce RipEX C. Nejsou-li parametry nastaveny správně na obou radiomodemech, může RipEX A komunikovat s jednotkou RipEX C primární cestou v jednom směru a záložní cestou v opačném směru (asymetrický routing).

Chcete-li se vrátit komunikaci na primární cestu, zakažte RSS kontrolu nebo zlepšete hodnotu RSS signálu mezi oběma jednotkami RipEX.

5.3.2. Rádio / záloha Rádio 2

Koncové zařízení připojené přes ethernetové rozhraní.

V druhém příkladu používáme stejnou konfiguraci jako u prvního kromě toho, že zařízení RTU jsou připojená přes ethernetová rozhraní. Viz následující obrázek:



Obr. 5.9: Topologie sítě 2

Poznámka

V tomto příkladu jsme změnili priority pro náhradní trasy.

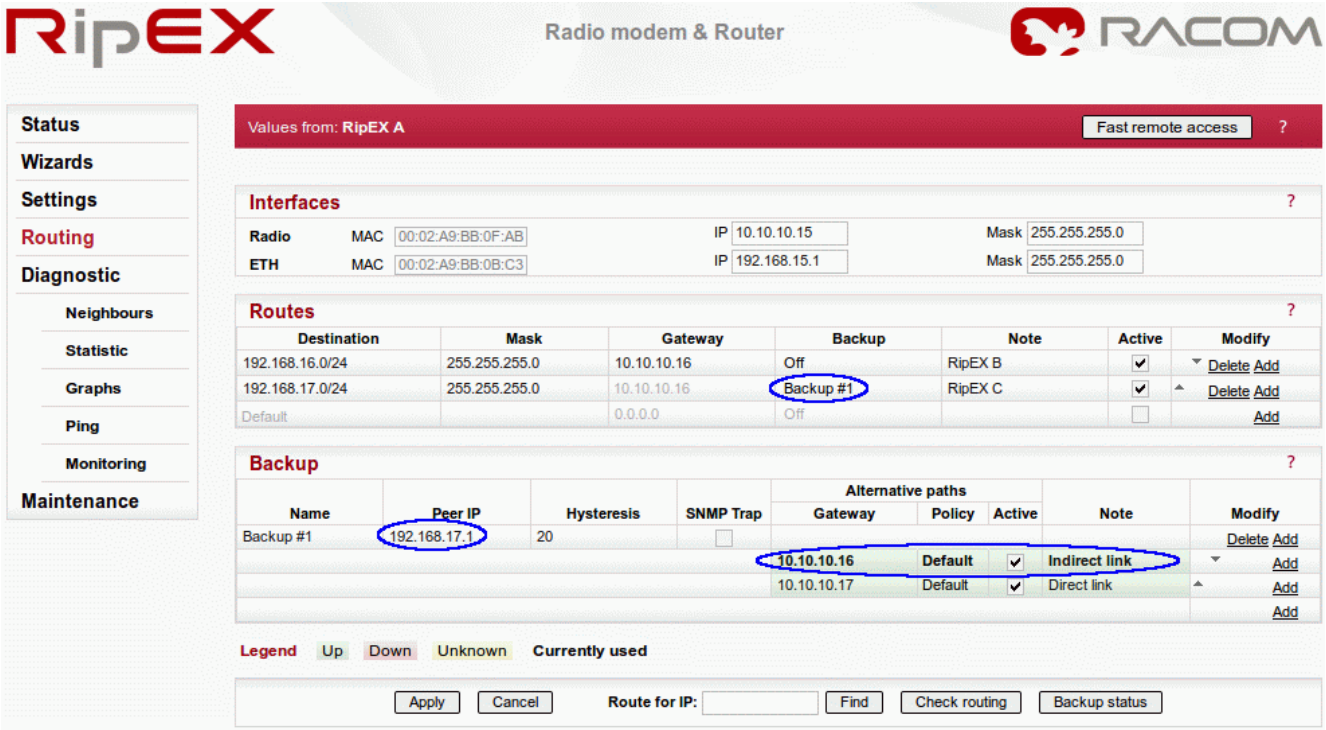
Koncová zařízení jsou nyní připojena přes ethernetové porty, což znamená, že musíme do příslušných radiomodemů RipEX doplnit správné IP adresy a routing.

Pokud již není nastavena, změňte ethernetovou IP adresu podle této topologie:

- RipEX A – 192.168.15.1/24
- RipEX B – 192.168.16.1/24
- RipEX C – 192.168.17.1/24
- ...

Teď musíme nastavit správný routing. Pro jednoduchost budeme ignorovat RipEX D a RipEX E v naší konfiguraci.

Podívejte se na nastavení routingu v jednotce RipEX A na následujícím příkladu:

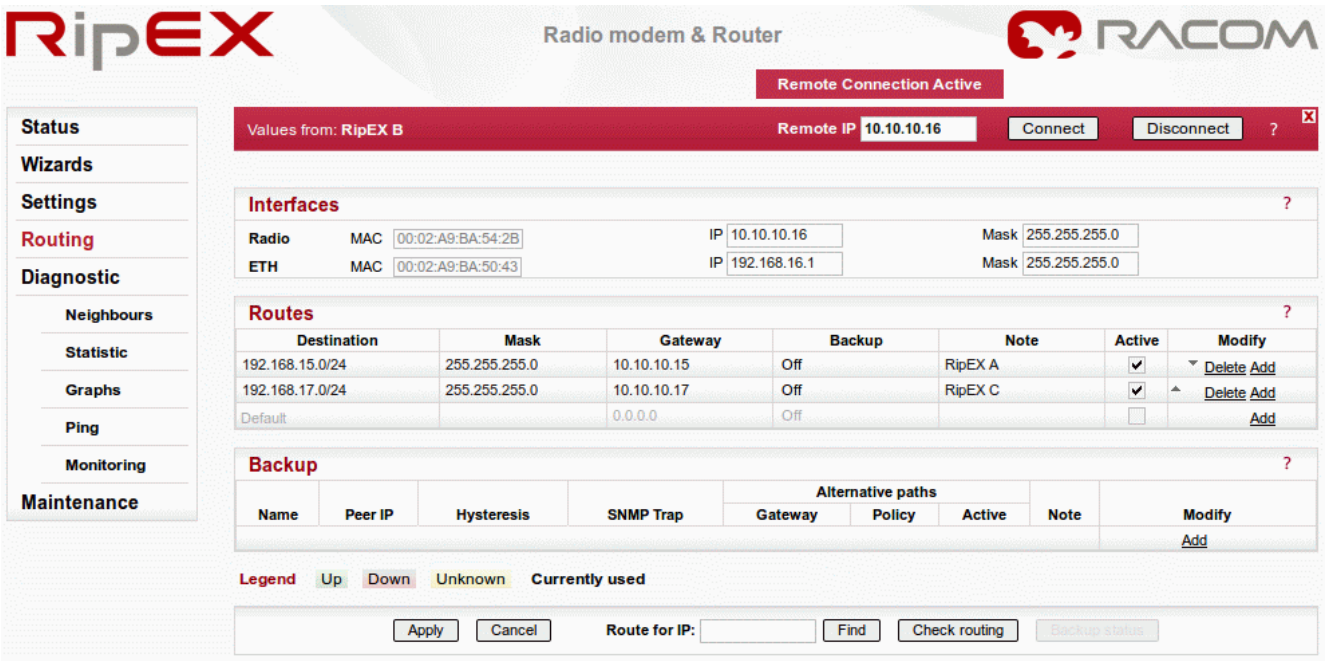


Obr. 5.10: Menu Routing pro RipEx A - příklad č. 2

Všimněte si, že jsme použili systém **Zálohování tras** pro body v síti 192.168.17.0/24. Také si všimněte, že jsme vyplnili Peer IP vzdálenou Ethernetovou IP adresou radiomodemu RipEX. Aktuálně použitá cesta je primární (nepřímá) ale obě cesty jsou barevně označeny "Up".

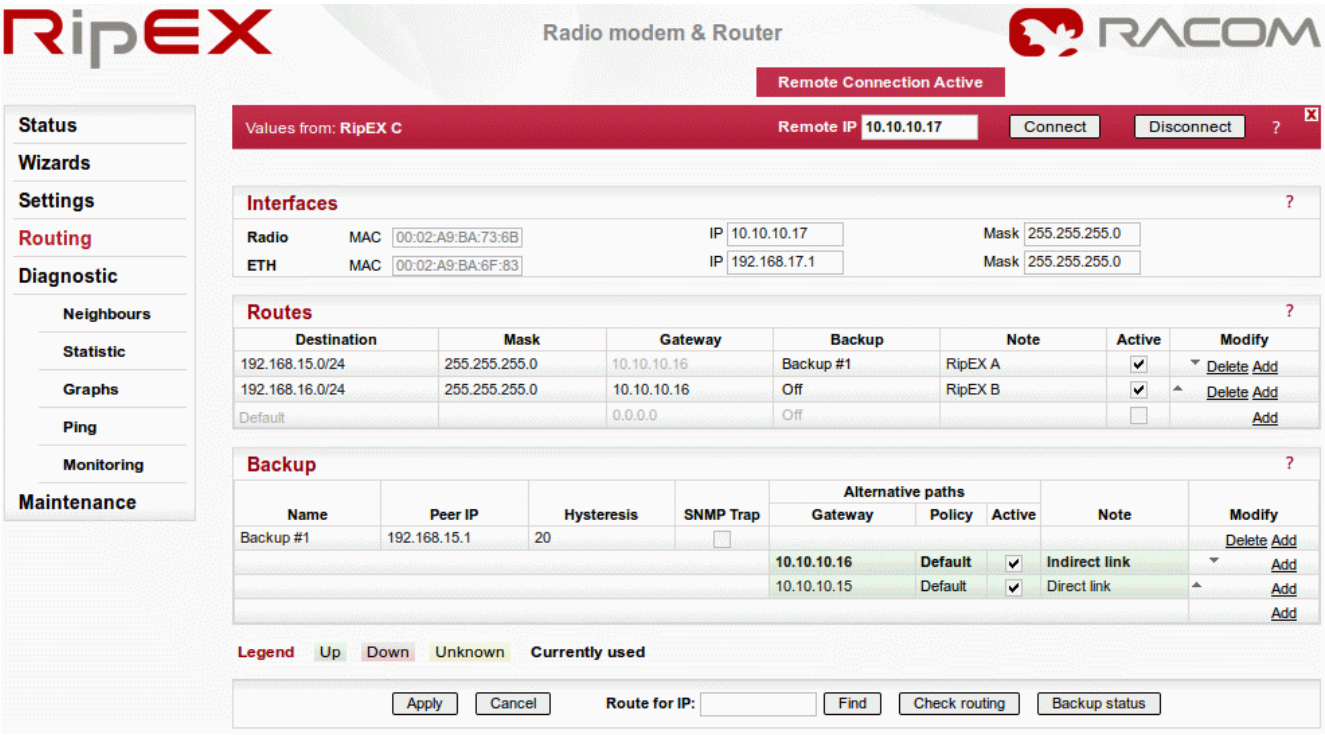
Poznámka

Je možné použít pouze IP adresu vzdáleného radiomodemu – rádiovou nebo hlavního Ethernetového rozhraní (ne subnet adresu nebo adresu připojeného zařízení).



Obr. 5.11: Menu Routing pro RipEx B - příklad č. 2

Přidali jsme také cesty do jednotky RipEX B pro ethernetové sítě za dalšími jednotkami RipEX.



Obr. 5.12: Menu Routing pro RipEx C - příklad č. 2

V jednotce RipEX C máme velmi podobnou konfiguraci jako v jednotce RipEX A, ale pro opačný směr.

Praktický test

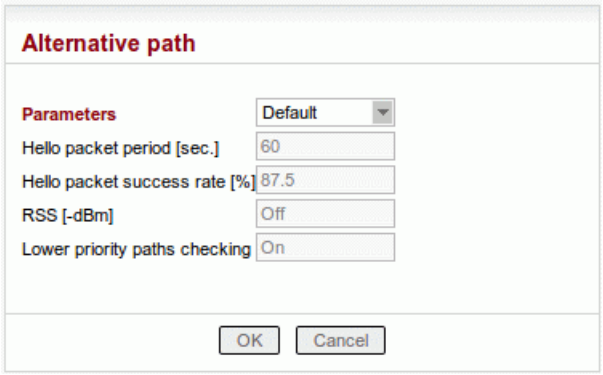
V tomto příkladu budeme používat jinou metodu pro přepínání mezi primární a záložní cestou. Nastavili jsme nejvyšší prioritu pro nepřímé spojení (naše záložní cesta v předchozím příkladu). Kdykoliv je RipEX B vypnutý, systém **Záložní trasy** použijte přímou cestu.

Rozpoznání výpadku jednotky RipEX závisí na nastavení hodnot **Policy**.

Poznámka

Pokud nastavíte nízkou hodnotu parametru **„Hello packed period“** (například 10 sekund) a **„Hello packed success rate“** na 100%, proces bude velmi rychlý. Ale při tomto nastavení snížíte kapacitu rádiového kanálu pro uživatelská data a aktivní cesta je hned po ztrátě prvního „Hello“ paketu je označena za nefunkčni („Down“).

V tomto příkladu **nebudeme měnit výchozí hodnoty**.

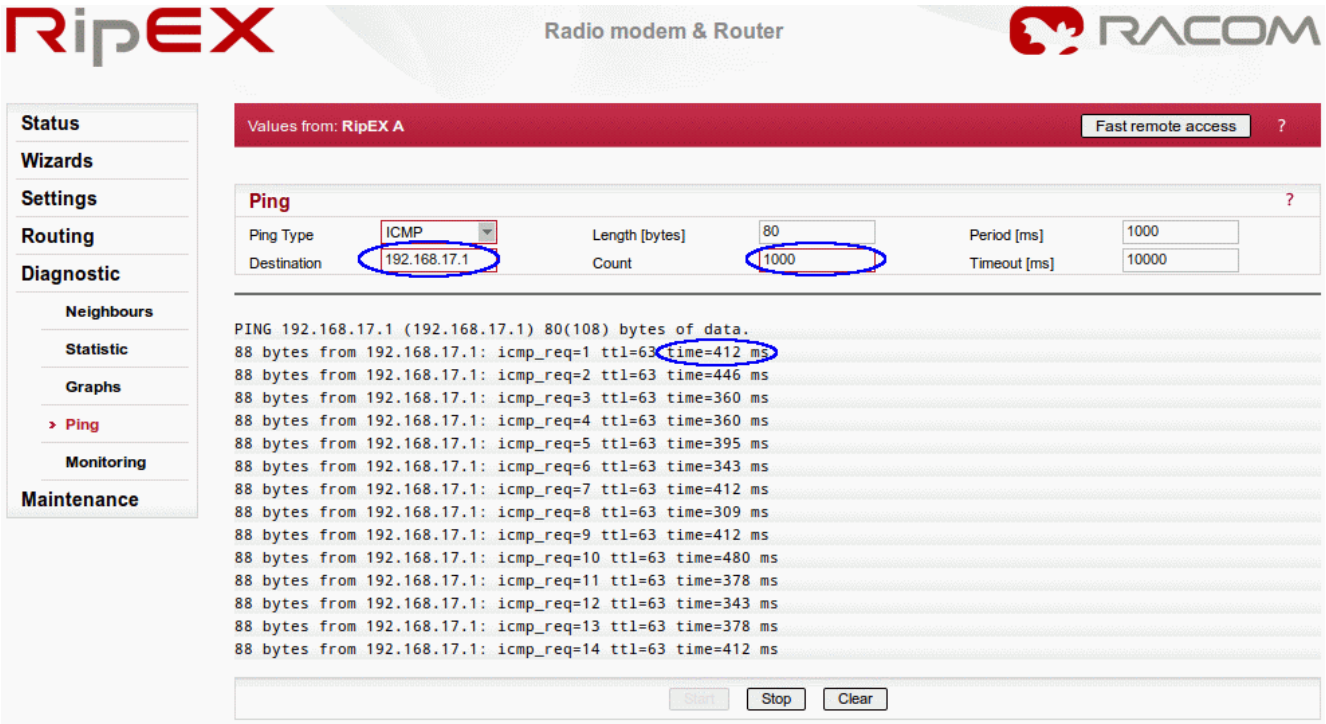


Obr. 5.13: Default hodnoty Policy

Poznámka

Hodnocení parametru „Hello packet success rate“ je založeno na posledních osmi kontrolních „Hello“ paketech.

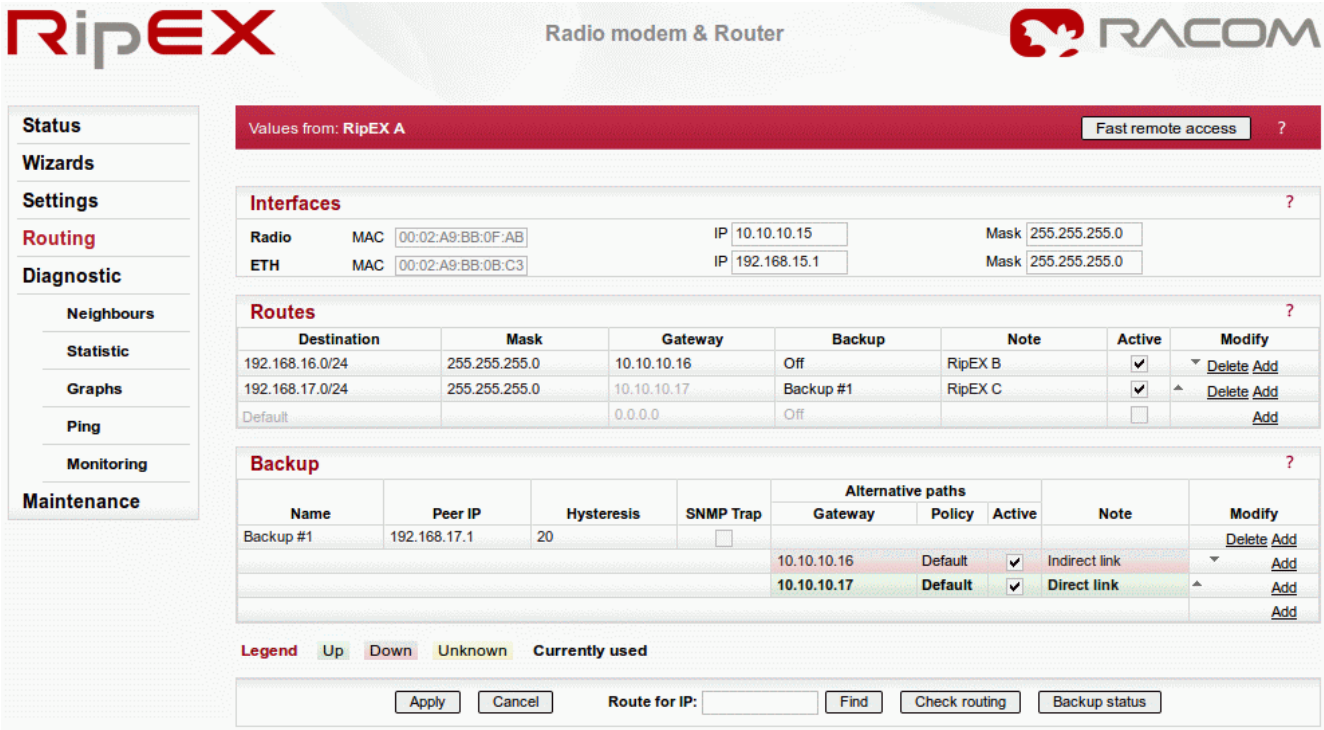
Chcete-li vidět celý postup, můžete začít s vysíláním ping paketů. Jděte do RipEX menu **Diagnostic** → **Ping** a vyplňte cílovou IP adresu (192.168.17.1). Poté budou ping pakety úspěšné a budou přenášeny primární (nepřímou) cestou (např. můžete zkontrolovat RX / TX LED diody radiomodemu RipEX).



Obr. 5.14: Úspěšné Ping pakety – primární cesta

Můžete také zapnout monitorování rádiového rozhraní. Jděte do menu **Diagnostic** → **Monitoring** a zkontrolujte rádiové rozhraní. Nechte ostatní parametry na výchozích hodnotách (default) a klikněte na tlačítko Start. Sledovat můžete všechny pakety v rádiové síti (ping pakety, „Hello“ pakety, ARP, ...).

Nyní vypněte RipEX B a sledujte rozdíly. Vidíte, že nejsou žádné odpovědi na ping pakety v **Ping** and **Monitoring** menu. Obnovte hodnoty v menu Routing (stiskem tlačítka Backup status), abyste viděli, že aktivní cesta je přepnuta na záložní (přímou) cestu.



Obr. 5.15: RipEX A routing menu – RipEX B vypnutý

Jakmile funkce Záložní Trasy vyhodnotí situaci správně, ping pakety opět úspěšně procházejí. Všimněte si také, že RTT hodnota ping paketů je nižší než u používané primární (nepřímé) cesta.

```
ping: recvmsg: No route to host
ping: recvmsg: No route to host
From 192.168.15.1: icmp_seq=558 Destination Host Unreachable
From 192.168.15.1: icmp_seq=559 Destination Host Unreachable
88 bytes from 192.168.17.1: icmp_req=563 ttl=64 time=174 ms
88 bytes from 192.168.17.1: icmp_req=564 ttl=64 time=157 ms
88 bytes from 192.168.17.1: icmp_req=565 ttl=64 time=174 ms
```

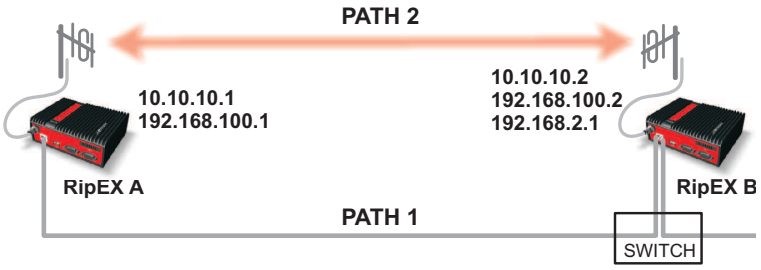
Obr. 5.16: RipEX A Ping pakety – záložní (přímá) cesta

Nyní můžete RipEX B znovu zapnout. Vzhledem k tomu, že RipEX pravidelně kontroluje primární (nepřímou) cestu pomocí kontrolních Hello" paketů, přepne se zpět na primární cestu. Tato změna nezpůsobí žádnou ztrátu ping paketů.

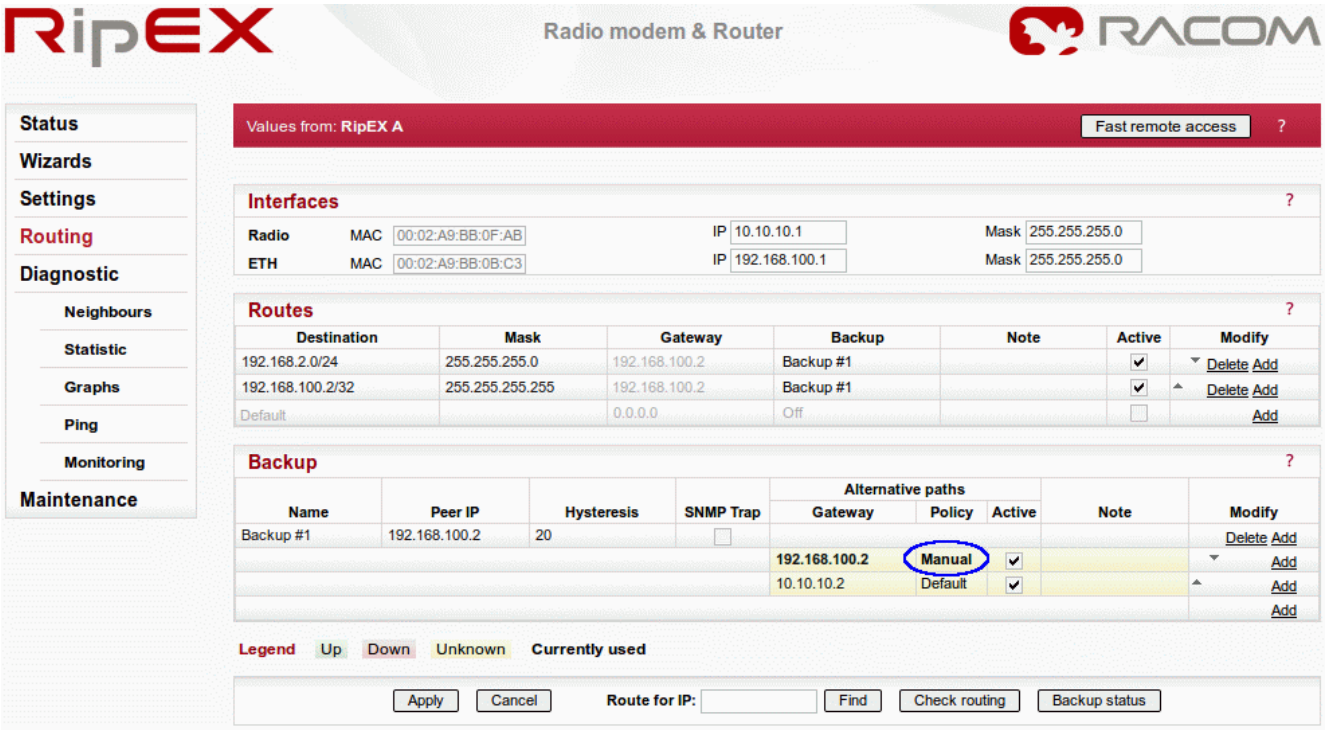
5.3.3. Ethernet / záloha Rádio

V tomto případě je primární cestou ethernetová linka, zálohou je rádiová linka.

Podívejte se na následující příklad:



Obr. 5.17: Topologie sítě č.3



Obr. 5.18: Menu Routing pro RipEX A – příklad č. 3

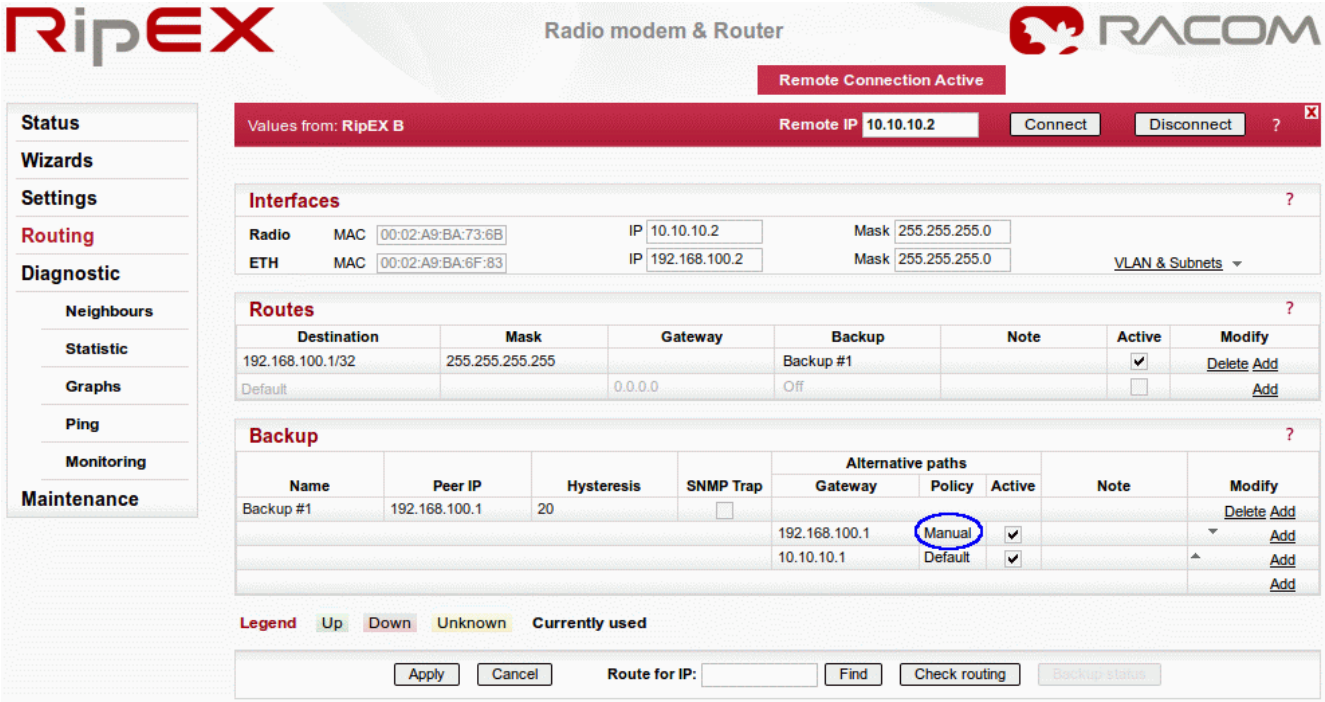
Primární ethernetová linka poskytuje vysokou kapacitu pásma. Je vhodné posílat kontrolní "Hello" pakety každou sekundu. To povede, v případě výpadku ethernetové linky, k rychlému přepnutí na záložní rádiovou linku, která použije svoji delší "Hello packet period" .

```
ping: recvmsg: No route to host
ping: recvmsg: No route to host
From 192.168.15.1: icmp_seq=558 Destination Host Unreachable
From 192.168.15.1: icmp_seq=559 Destination Host Unreachable
88 bytes from 192.168.17.1: icmp_req=563 ttl=64 time=174 ms
88 bytes from 192.168.17.1: icmp_req=564 ttl=64 time=157 ms
88 bytes from 192.168.17.1: icmp_req=565 ttl=64 time=174 ms
```

Obr. 5.19: Perioda Hello paketů nastavena na jednu sekundu

RipEX B je nakonfigurován s IP adresou 192.168.100.2/24, která se používá pouze pro komunikaci mezi jednotkami RipEX. Další podsítě 192.168.2.0/24 se využívá pro zbytek komunikace po Ethernetu. Podívejte se na podrobnosti v kapitole ARP Proxy a VLAN.

Pro RipEX B je také nastavena perioda opakování kontrolních „Hello“ paketů na ethernetové lince na jednu sekundu.



Obr. 5.20: Menu Routing pro RipEX B – příklad č. 3

Po odpojení primární ethernetové cesty se systém automaticky přepne na záložní rádiovou cestou. Můžete tuto funkci zkontrolovat při použití stejných nástrojů jako v předchozích příkladech.

6. VPN

6.1. IPsec

6.1.1. Základní popis

IPsec je službou běžící v Linuxovém jádře, která zachytává vybrané pakety, šifruje je a přebaluje do paketů **ESP (Encapsulating Security Payload)**, které jsou poslány protistraně. Druhá strana přijímá ESP pakety a dešifruje je do původní podoby.

V RipEXu je implementován IPsec v tunelovém módu.

Princip funkce IPsec

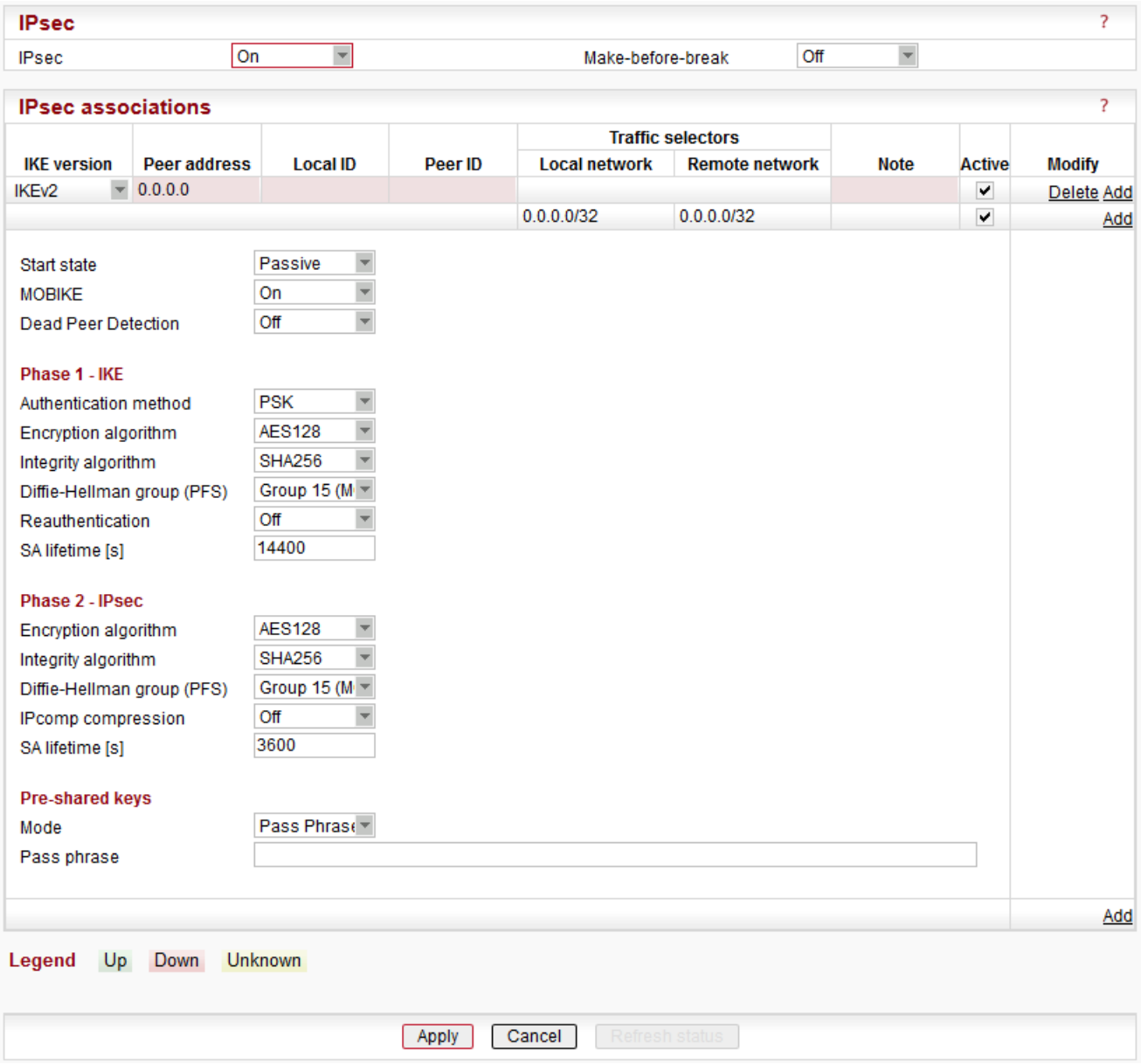
- IPsec používá pro šifrování symetrické sdílené klíče. Tyto klíče se musí před vytvořením spojení bezpečně předat protistraně a v průběhu existence spojení se musí po čase vyměňovat za nové, aby nebyla ohrožena bezpečnost spojení. Výměna klíčů je zajišťována protokolem **IKE (Internet Key Exchange)**, buď starší verzi 1 nebo novější 2.
- Protokol IKE komunikuje s protistranou pomocí **UDP paketů na portu 500** a nebo při aktivním NAT-T (NAT Traversal) nebo MOBIKE (MOBile IKE) **na portu 4500**.
- Tunel IPsec je zajišťován **bezpečnostními asociacemi (SA, Security Association)**. Asociací jsou 2 druhy:
  - **IKE SA**: Bezpečnostní asociace IKE, která slouží k výměně klíčů SA s protistranou.
  - **CHILD SA**: Bezpečnostní asociace IPsec, která provádí šifrování vybraných paketů.
- Každý tunel IPsec má právě 1 IKE SA a alespoň 1 CHILD SA.aa
- **Metoda autentizace** slouží k bezpečnému ověření protistrany. V RipEXu je implementována metoda **PSK** (Pre-Shared Key): Obě strany mají nastavený stejný klíč (heslo).
- Po **vyprchání doby platnosti CHILD SA** proběhne vygenerování nových klíčů a jejich výměna pomocí IKE SA.
- Po **vyprchání doby platnosti IKE SA v IKEv1** proběhne nová autentizace a výměna klíčů a vytvoření nové IKE SA (a podřízených CHILD SA).
- Po **vyprchání doby platnosti IKE SA v IKEv2** se chování liší podle nastavení. Pokud je vyžadována reautentizace, chová se podobně jako IKEv1. Pokud není vyžadována, jen se vygenerují a vymění nové klíče IKE SA.

6.1.2. Konfigurace

Popis konfiguračních položek

- IPsec v Ripexu může být nakonfigurován buď pomocí Webového rozhraní (stránka IPsec), nebo pomocí CLI (příkazy cli_cnf_set_ipsec, cli_cnf_set_ipsec_assoc, cli_cnf_set_ipsec_tsel, cli_cnf_set_ipsec_psk).

- Následující popis se drží Webového rozhraní. CLI je podobné, jen má všechny tabulky oddělené a ne zanořené.



Obr. 6.1: Menu VPN - IPsec

- Listbox “**IPsec**”: Zapíná celý subsystém IPsec. Default je “Off”.
- Listbox “**Make-before-break**”: Globální nastavení pro všechny IKE SA používající IKEv2 s reautentizací. Pokud je zapnuto, nedochází k dočasnému přerušení spojení během reautentizace IKE_SA. Nemusí fungovat se všemi protistranami. Default je “Off”.
- Tabulka “**IPsec associations**”:
  - Každý řádek odpovídá jedné IKE SA. Současně může být nakonfigurováno maximálně 8 aktivních IKE SA.
  - Klíčem tabulky je položka “Peer ID”, která slouží pro jednoznačnou identifikaci IKE SA a k provázání s CHILD SA (tabulka Traffic selectors) a s PSK.

- Listbox “**IKE version**”: Výběr verze IKE. Musí odpovídat nastavení na protistraně. Default je “IKEv2”.
- Položka “**Peer address**”: IP adresa protistrany, kde běží IKE daemon, se kterým se bude vyjednávat.
- Položka “**Local ID**”: Identifikátor lokální strany, buď IP adresa nebo FQDN (Fully Qualified Domain Name). Musí odpovídat “Peer ID” na protistraně.
- Položka “**Peer ID**”: Identifikátor protistrany, buď IP adresa nebo FQDN. Musí být v tabulce unikátní. Musí odpovídat “Local ID” na protistraně.
- Položka “**Note**”: Popisek řádku tabulky.
- Přepínač “**Active**”: Zneplatňuje řádek (IKE SA a všechny přidružené CHILD SA).
- Tabulka “**Traffic selectors**”:
  - Každý řádek odpovídá jedné CHILD SA přidružené k dané IKE SA (přes “Peer ID”).
  - Je povoleno mít maximálně 16 aktivních CHILD SA (dohromady přes všechny aktivní IKE SA).
  - Každý aktivní řádek musí mít ekvivalentní řádek na protistraně s prohozenými hodnotami “Local network” a “Remote network”.
  - Položka “**Local network**”: Rozsah (adresa/maska) zdrojových IP adres paketů, které budou zachyceny a šifrovány.
  - Položka “**Remote network**”: Rozsah cílových IP adres paketů, které budou zachyceny a šifrovány.
  - Přepínač “**Active**”: Zneplatňuje řádek (CHILD SA).
  - “Local network” a “Remote network” nesmí být stejné. Také se nesmí překrývat s rozsahem sítě servisního připojení (10.9.8.7/28) nebo připojení k FPGA (192.0.2.233/30).
  - Nesmí existovat dva aktivní selektory (klidně i pro různé IKE SA), které mají stejnou dvojici “Local network” a “Remote network”.
- Listbox “**Start state**”: Nastavuje počáteční stav spojení:

  “Passive” Spojení se nenavazuje, čeká na druhou stranu. Default.

  “On Demand” Spojení se začne navazovat až se přes něj pokusí projít nějaký paket. Paket čeká, než se spojení naváže.

  “Start” Spojení se hned navazuje.
- Listbox “**MOBIKE**”: Zapíná funkci MOBIKE pro IKEv2 (podpora mobility/migrace tunelů). Vedlejším účinkem MOBIKE je okamžitý přesun IKE z portu 500 na port 4500, s čímž můžou mít problém některé protistrany nebo firewally po cestě. Mělo by souhlasit s protistranou. Default je “On”.
- Listbox “**Dead Peer Detection**”: Zapíná detekci ztráty spojení s protistranou. Posílají se testovací IKE pakety. Pokud se vyopakují bez odpovědi, spojení se zruší (a následují příslušné akce). Pokud není zapnuto, tak se ztráta spojení zjistí až při příští výměně klíčů. Default je “Off”.

- Položka “**DPD check period**”: Perioda [s] kontroly spojení. Rozsah je 5s – 28800s (8h), default je 30s.
- Listbox “**DPD action**”: Do jakého stavu se spojení uvede, když bylo zjištěno jeho přerušení:

  “Clear” Spojení se uzavře a čeká.

  “Hold” Spojení se uzavře, začne se navazovat, až se přes něj pokusí projít paket. Default.

  “Restart” Okamžitě se pokouší navazovat nové spojení.

- Blok “**Phase 1 – IKE**”:
  - Nastavuje parametry IKE SA.
  - Listbox “**Authentication method**”: Metoda autentizace protistrany. V současnosti je podporováno pouze “PSK”. Musí souhlasit s protistranou.
  - Listbox “**Encryption algorithm**”: Algoritmus pro šifrování IKE SA. Volby označené “(legacy)” neposkytují dostatečnou bezpečnost. Musí souhlasit s nastavením protistrany. Default je “AES128”.
  - Listbox “**Integrity algorithm**”: Algoritmus pro zajištění integrity IKE SA. Volby označené “(legacy)” neposkytují dostatečnou bezpečnost. Musí souhlasit s nastavením protistrany. Default je “SHA256”.
  - Listbox “**Diffie-Hellman group (PFS)**”: Perfect Forward Secrecy zvyšuje bezpečnost výměny klíčů IKE SA. Výrazně ovlivňuje zátěž Ripexu během výměny klíčů. Volby označené “(legacy)” neposkytují dostatečnou bezpečnost. Musí souhlasit s nastavením protistrany. Default je “Group 15 (MODP3072)”.
  - Listbox “**Reauthentication**”: Nastavuje chování po uplynutí životnosti IKE SA při použití IKEv2. Pokud je zapnuto, dochází k vyjednání celé nové IKE SA včetně nové autentizace. Užitečné při práci s certifikáty, protože hlídá jejich vyprchání. Pokud je vypnuto, jen se vyměňují nové klíče. Default je “Off”.
  - Položka “**SA lifetime**”: Doba platnosti [s] IKE SA. Po jejím uplynutí se provede nová výměna klíčů, případně reautentizace. Rozsah je 300s – 86400s (1 den). Default je 14400s (4h).
- Blok “**Phase 2 – IPsec**”:
  - Nastavuje sdílené parametry všech podřízených CHILD SA.
  - Listbox “**Encryption algorithm**”: Algoritmus pro šifrování CHILD SA (uživatelského provozu). Volby označené “(legacy)” neposkytují dostatečnou bezpečnost. Musí souhlasit s nastavením protistrany. Default je “AES128”.
  - Listbox “**Integrity algorithm**”: Algoritmus pro zajištění integrity CHILD SA (uživatelského provozu). Volby označené “(legacy)” neposkytují dostatečnou bezpečnost. Musí souhlasit s nastavením protistrany. Default je “SHA256”.
  - Listbox “**Diffie-Hellman group (PFS)**”: Perfect Forward Secrecy zvyšuje bezpečnost výměny klíčů CHILD SA (uživatelského provozu). Výrazně ovlivňuje zátěž Ripexu během výměny klíčů. Volby označené “(legacy)” neposkytují dostatečnou bezpečnost. Musí souhlasit s nastavením protistrany. Default je “Group 15 (MODP3072)”.

- Listbox “**IPcomp compression**”: Zapíná paketovou kompresi před šifrováním uživatelského provozu. Musí souhlasit s nastavením protistrany. Default je “Off”.
- Položka “**SA lifetime**”: Doba platnosti [s] CHILD SA. Po jejím uplynutí se provede nová výměna klíčů přes IKE SA. Rozsah je 180s – 86400s (1 den). Default je 3600s (1h).

■ Blok “**Pre-shared keys**”:

- Nastavení autentizace PSK pro IKE SA (svázáno pomocí “Peer ID”).
- Klíč musí být stejný jako u protistrany.
- Listbox “**Mode**”: Volí způsob zadání sdíleného klíče.
  - “Pass Phrase”: Zadání pomocí hesla (řetězce). Default.
    - Položka “**Pass phrase**”: Heslo. Nesmí být prázdné.
  - “Key”: Zadáno jako 256b číslo.
    - Položka “**Key**”: 256b klíč jako hexadecimální číslo s 64 číslicemi.
    - Tlačítko “**Generate**”: Vygeneruje do položky “Key” nový 256b klíč.

Pokročilé vlastnosti konfigurace

- Vlastnosti “**Peer address**”:

■ Volit tak, aby nastavena adresa souhlasila s adresou, ze které protistrana odpovídá. Ripex se automaticky snaží vybrat lokální adresu, která odpovídá adrese protistrany.

■ Lze nastavit adresu protistrany tak, že provoz IKE/IPsec odpovídá nastavení selektoru CHILD SA. Provoz IKE/IPsec má výjimku a nebude zachycen.

- Příklad: Propojuje se Ripex A s ETH 192.168.1.41/24 a Ripex B s ETH 192.168.2.67/24. Na Ripexu A je možné nastavit adresu protistrany jako 192.168.2.67 a selektor 192.168.1.0/24 → 192.168.2.0/24 a spojení bude fungovat a nezacyklí se.

- **Hlídač spojení** se aktivuje jen pro spojení se “Start state” nastaveným na “Start”, která buď mají vypnuté “Dead Peer Detection” nebo mají nastavené “DPD action” na “Restart”. Jenom u takových spojení lze prohlásit, že musí být vždy vytvořená a nikdy nečekají v neaktivním stavu.
- V Ripexu lze vytvořit **navazující tunely IPsec**, ale musí existovat směrovací pravidlo pro přeposílané uživatelské pakety. Je jedno, kam toto pravidlo míří, lze použít i default GW. Paket přijatý z jednoho tunelu se dešifruje a potom je zachycen a zašifrován druhým tunelem.

■ Příklad: V Ripexu 192.168.1.41 končí IPsec tunel se selektorem 10.10.67.0/24 -> 10.10.42.0/24 navázaný na router 192.168.1.42 a tunel se selektorem 10.10.42.0/24 → 10.10.67.0/24 navázaný na router 192.168.2.67. Ve směrovací tabulce Ripexu 192.168.1.41 musí být směrovací pravidla pro adresy 10.10.42.0/24 a 10.10.67.0/24, například 10.10.42.0/24 → 192.168.1.42 a 10.10.67.0/24 → 192.168.2.67. Paket jdoucí z 10.10.42.1 na 10.10.67.1 se potom v Ripexu vybalí z ESP, nalezne se pro něj směrovací pravidlo (takže se nezahodí), následně je zachycen a zabalen do ESP druhým tunelem. Opačný směr je obdobný.

- **Doby platnosti SA** se randomizují v rozsahu 90%-110% při každém zahájení odpočtu, aby nedocházelo ke kolizím při zahájení výměny klíčů z obou stran zároveň.

- **Počet a doba opakování paketů IKE** jsou v defaultním nastavení: 5 opakování s rostoucím odstupem, po uplynutí 165s (celkem) opakování končí neuspěchem.

  ■ Při zapnutém DPD s periodou 30s je nejdelší doba od přerušení spojení do uzavření SA 30s+165s = 195s.

- **Dead Peer Detection** může běžet výrazně rychleji než výměna klíčů ("**SA lifetime**"), protože představuje mnohem menší zátěž jak pro CPU, tak pro síť.

- Nastavení "**SA lifetime**" by mělo odpovídat množství dat procházejícímu přes SA. Pro IKE SA, přes které prochází jen výměny klíčů, může být použita velká hodnota. CHILD SA bude mít typicky několikanásobně kratší dobu životnosti. Častější výměny klíčů zabraňují prolomení šifry útočníkem, který by analyzoval velké množství stejně šifrovaných dat. Příliš časté výměny klíčů zatěžují CPU a síť. Velká část zátěže CPU při výměně klíčů závisí na nastavení PFS, čím vyšší "Diffie-Hellman group", tím vyšší zátěž.

- Ripex nepodporuje vyjednávání spojení IKEv1 pomocí "**aggressive mode**", ale jen "**main mode**". Agresivní mód není v kombinaci s PSK bezpečný.

- **PRF (Pseudo-Random Function)** pro IKE SA se v Ripexu nekonfiguruje, používá se default, tedy to samé, co je v "Integrity algorithm".

6.1.3. Součinnost IPsec s ostatními službami Ripexu

- IPsec není dovoleno spustit v režimu **Bridge**.

- Uživatelem definovaný **firewall** filtruje pakety před zašifrováním v IPsec nebo po dešifrování.

- IPsec lze nakonfigurovat a provozovat přes **rádiový kanál**. Adresa protistrany může být rádiová IP adresa i IP adresa ETH (primární).

- IPsec může pracovat vedle **optimalizátoru**. Provoz zachycený IPsec se nebude optimalizovat.

- IPsec lze provozovat přes **zálohované trasy (Backup routes)**. Stačí nastavit adresu protistrany tak, že se směruje přes pravidlo se zálohovanou trasou.

- IPsec lze použít zároveň s **TCP Proxy**. Nejdříve TCP Proxy zachytí TCP paket a přebalí ho do UDP, potom zabere IPsec. Na protistraně je postup opačný.

- IPsec lze používat současně s protokolem **SLIP** (rozhraní COM, terminal server). IPsec spojení může být vytvořeno přes tunel SLIP a umožňuje směrovat skrz něj uživatelský provoz.

- IPsec může vytvořit spojení přes **VLAN nebo subnet**. Při přípravě konfigurace Ripex vybere odpovídající zdrojovou adresu.

- IPsec je schopen fungovat v režimu **HotStandby**. V pasivním režimu je IPsec vypnutý, při přechodu do aktivního režimu startuje a otevírá nové asociace, které u protistrany nahradí asociace k nyní pasivnímu Ripexu. Přesné chování závisí na nastavení "Start state" a DPD. Nejrychlejší reakce na přepnutí bude, pokud mají Ripexy v HotStanby "Start state" nastavené na "Start".

6.2. GRE

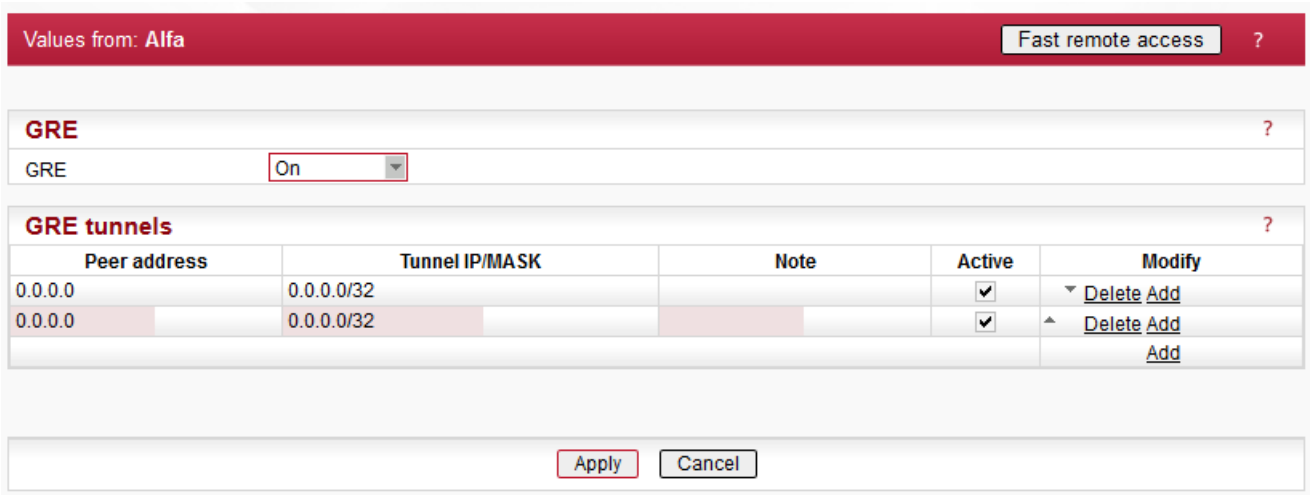
6.2.1. Základní popis

- GRE slouží k tunelování uživatelského provozu. Vytváří virtuální point-to-point zařízení, paket do něj nasměrovaný je vložen do GRE paketu, který je poslán protistraně, kde je vybalen. Z hlediska přenášneného provozu se GRE tunel jeví jako 1 hop.
- GRE může fungovat v režimu tunelu (TUN) nebo může být vytvořeno L2 transparetní spojení pomocí režimu (TAP) a SW bridge. V Ripexu **podporujeme pouze režim TUN**, GRE TAP není implementován do verze jádra Linuxu v Ripexu.
- Paket zabalený do GRE není nijak chráněný proti ztrátě a **není šifrován**.
- GRE neprovádí žádné navazování ani udržování spojení, tunel GRE je vytvořen bez ohledu na stav (nebo existenci) protistrany.
- Tunel GRE má vlastní IP adresu a masku. Síť tvořená adresou a maskou obsahuje jen 2 uzly – oba konce tunelu.
- Protože tunel přidává k balenému paketu GRE hlavičku, má nastavené nižší MTU (1476B), aby nedocházelo k fragmentaci GRE paketů. Vstupující pakety mohou být fragmentovány na GRE rozhraní.

6.2.2. Konfigurace

Popis konfiguračních položek

- GRE může být v Ripexu nakonfigurováno buď pomocí Webového rozhraní (stránka GRE), nebo pomocí CLI (příkazy cli_cnf_set_gre a cli_cnf_set_gre_tunnels).
- Následuje popis Webového rozhraní, CLI je organizováno podobně.



Obr. 6.2: Menu VPN - GRE

- Listbox “**GRE**”: Zapíná celý subsystém GRE. Default je “Off”.
- Tabulka “**GRE tunnels**”:

- Každý řádek odpovídá jednomu GRE tunelu. Nemělo by být současně vytvořeno více než 20 tunelů (doporučení).
- Klíčem tabulky je položka “Peer address”, která slouží k jednoznačné identifikaci tunelu.
- Položka “**Peer address**”: IP adresa protistrany, na které je druhý konec GRE tunelu. Nelze vytvořit 2 GRE tunely na stejnou cílovou adresu, protože kernel rozlišuje podle zdrojové adresy, kterému tunelu patří GRE pakety přicházející od protistran. Lokální (zdrojová) adresa se vybírá automaticky podle druhu (rozhraní) zvolené cílové adresy. Adresy na obou stranách se musí nastavit tak, aby si navzájem odpovídaly.
  - Příklad: Propojují se 2 Ripexy (A a B) s adresami: ETH(A) a AIR(A), ETH(B) a AIR(B). Na Ripexu A existuje směrovací pravidlo ETH(B)→AIR(B), na Ripexu B ETH(A)→AIR(A). Tunel bude veden přes vzduch. Potom lze použít nastavení “Peer address”: na A AIR(B) a na B AIR(A) nebo na A ETH(B) a na B ETH(A). Nelze nastavit například na A ETH(B) a na B AIR(A), protože GRE pakety z A by měly zdrojovou adresu ETH(A) a na B není žádný GRE tunel na ETH(A), který by je rozbalil.
- Položka “**Tunnel IP/MASK**”: IP adresa a maska rozhraní tunelu. Síť definovaná touto položkou musí pokrývat jen lokální adresu tunelu a adresu na vzdáleném konci. Oba konce tunelu musí mít nastavenou stejnou síť a musí mít různé IP adresy. IP adresa druhého konce tunelu se používá jako “Gateway” při nastavování směrování do tunelu.
- Položka “**Note**”: Popisek řádku tabulky (tunelu).
- Přepínač “**Active**”: Zneplatňuje řádek (tunel).

- Směrování paketů do GRE tunelu lze nastavit na stránce Routing, stačí do sloupce “Gateway” vyplnit adresu druhé strany GRE tunelu (IP adresu rozhraní). CLI rozhraní pro nastavení směrovací tabulky zatím neexistuje (únor 2017).

6.2.3. Součinnost s ostatními službami Ripexu

- Přístup na management (Web, CLI) přes GRE není povolen.
- Vzdálený přístup (QSSH) používaný Webem a CLI může probíhat přes GRE tunel.
- Uživatelský firewall dokáže filtrovat pakety přeposílané do a z GRE tunelu.
- Proxy ARP na LAN funguje pro adresy směrované do GRE tunelu.
- Lze vytvořit GRE tunel procházející přes rádiové rozhraní.
- Zálohované trasa (Backup route) může používat alternativní cestu přes GRE tunel. V “Alternative paths” se nastaví “Gateway” na IP adresu druhého rozhraní GRE tunelu.
- GRE tunel může být vytvořen přes zálohovanou trasu (Backup route). Pozor: Zdrojová adresa GRE paketů bude typicky hlavní ETH adresa Ripexu (unifikace adres). Tomu musí být přizpůsobeno nastavení protistrany GRE. Rádiová adresa Ripexu bude vybrána jako zdroj, jen pokud zálohovaná trasa obsluhuje směrovací pravidlo na adresy z rozsahu rádiové sítě (v tabulce “Routes”).
- Optimalizátor může být zapnutý zároveň s GRE. Pakety zabalené do GRE v Ripexu se nebudou optimalizovat. Procházející GRE pakety se optimalizují.

- Lze vytvořit GRE tunel přes jiný GRE tunel (i ve stejném Ripexu). Pozor na zacyklení a rostoucí režie (přidávání GRE hlaviček, fragmentace).
- GRE tunel lze používat zároveň s TCP proxy. TCP proxy je schopně zachytávat TCP z GRE i posílat své UDP pakety přes GRE.
- GRE tunel lze použít v HotStanby režimu, je bezestavový.
- IPsec může komunikovat se svojí protistranou přes GRE tunel.
- Lze vytvořit GRE tunel, který je chráněn pomocí IPsec. Pozor na nastavení adres: Musí se nastavit selektor IPsec tak, aby zachycoval GRE pakety, ale aby nedocházelo k interferenci se směrováním do GRE. V případě nutnosti je možné přidat Ripexu další adresy v nastavení “ARP proxy & VLAN”.

7. ARP Proxy a VLAN

ARP Proxy lze použít, pokud IP adresy RTU za různými radiomodemy RipEX jsou z jakéhokoli důvodu v rámci stejné IP podsítě, nejdou tedy routovat.

Virtuální LAN (VLAN) funkce se obvykle používá, když je potřeba rozdělit síť do několika logických částí. Např. pro rozlišení mezi uživatelskými daty a správou zařízení nebo mezi různými aplikacemi (například různé technologie RTU).

Obě funkce je možné pro získání potřebných funkcí kombinovat.

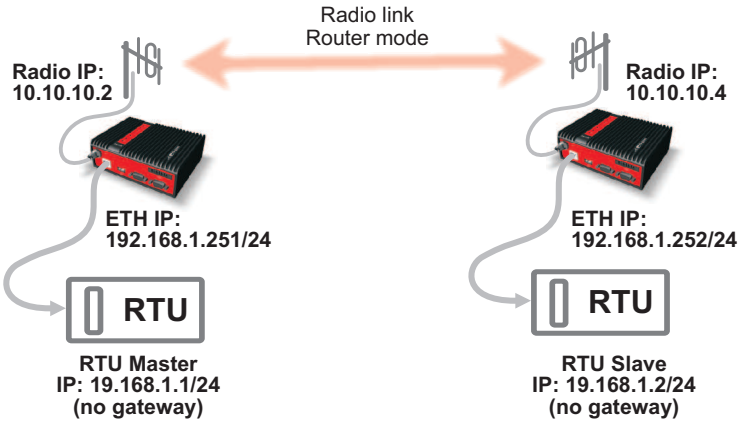
7.1. Transparentní LAN (ARP Proxy)

I když RipEX funguje jako standardní IP router, umožňuje propojit i části stejné IP podsítě za různými jednotkami RipEX, a to bez definování výchozí brány. To může být provedeno použitím funkce proxy ARP.

Poznámka

Viz *1.4 – „Flexible protokol v režimu Router“* – příklady konfigurace bez použití ARP proxy.

RipEX může odpovědět na jakoukoliv ARP žádost s tím, že předstírá, že má tuto konkrétní IP adresu (RipEX může odpovídat na více ARP požadavků). Tato funkce se obvykle používá tam, kde IP adresy RTU jsou za různými jednotkami RipEX ve stejné IP podsíti a RTU nemají schopnost routingu.



Obr. 7.1: Základní použití ARP proxy

V tomto diagramu RTU nemají schopnost routingu (tj. RTU očekává, že její protějšek je ve stejné fyzické síti Ethernet). Pokud RTU Master začíná komunikovat s RTU Slave, požaduje jeho MAC adresu. RTU Slave, přestože je ve stejné podsíti LAN, neodpoví (protože je až za radiomodemem RipEX). Pokud však jednotka RipEX (radio IP 10.10.10.2) má funkci ARP proxy zapnutu, odpoví na tuto ARP žádost.

Takže s funkcí ARP proxy serveru, může lokální RipEX napodobit jakoukoliv IP adresu a odpovídat na ARP žádosti. V našem případě RTU Master bude považovat MAC adresu jednotky RipEX za MAC adresu Slave. A s příslušnými pravidly Routingu v jednotkách RipEX, můžeme dosáhnout potřebného vzájemného propojení. Nepotřebujeme nic nastavovat na připojeném RTU – bez brány a pravidel pro routing.

Důležité

Při použití této funkce buďte velmi opatrní, protože pomocí ARP Proxy lze zakázat veškerý provoz v LAN síti!

Poznámka

- Můžete kombinovat funkce ARP proxy, TCP proxy a terminál serveru. Viz podrobnosti příslušného helpu ve webovém rozhraní jednotky RipEX.
- RipEX, ani při zapnuté funkci ARP proxy, nevysílá broadcast pakety přes rádiové linky.

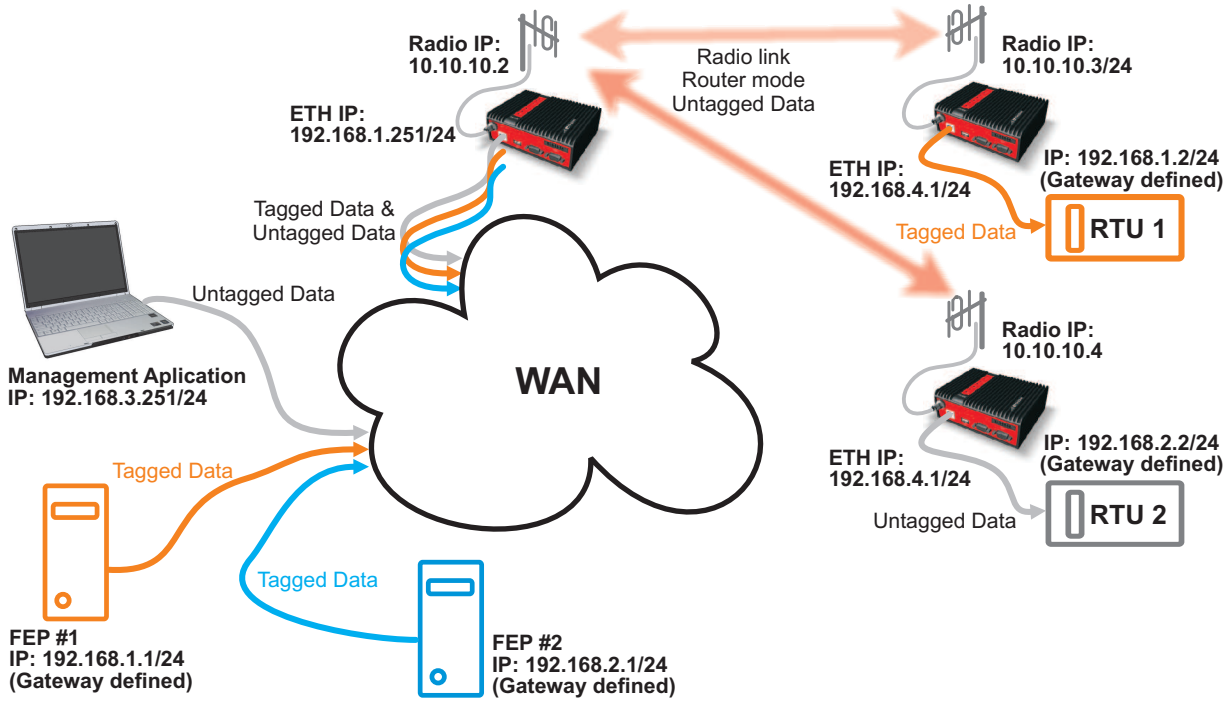
7.2. Transparentní VLAN

VLAN tag (802.1Q protokol) tvoří pole 4 bytů Ethernetového rámce. Je vložen mezi MAC adresou a polem EtherType/Length fields původního rámce.

VLAN paket je definován dvěma hlavními parametry:

VLAN tag – VLAN identifikátor (VID) je také nazýván „číslo VLAN“. Je 12 bitů dlouhý, takže můžeme mít až 4096 sítí VLAN (hodnoty 0x0000 a 0xFFF jsou vyhrazeny).

Priority Code Point (PCP) – Tří bitové pole, které se vztahuje k prioritě IEEE 802.1p. Určuje úroveň priority rámce. Možné hodnoty jsou od 0 (best effort) do 7 (nejvyšší priorita); 1 představuje nejnižší prioritu. Tyto hodnoty mohou být použity pro stanovení priorit různých způsobů provozu (hlas, data, ...).



Obr. 7.2: Schéma VLAN

Jak je vidět z *Obr. 7.2 – „Schéma VLAN“*, máme samostatné sítě VLAN pro Management a dvě odlišné technologie, každá podsíť s vlastním IP.

Poznámka

Můžete kombinovat funkce VLAN, TCP proxy a Terminal server. Viz podrobnosti příslušného helpu ve webovém rozhraní jednotky RipEX.

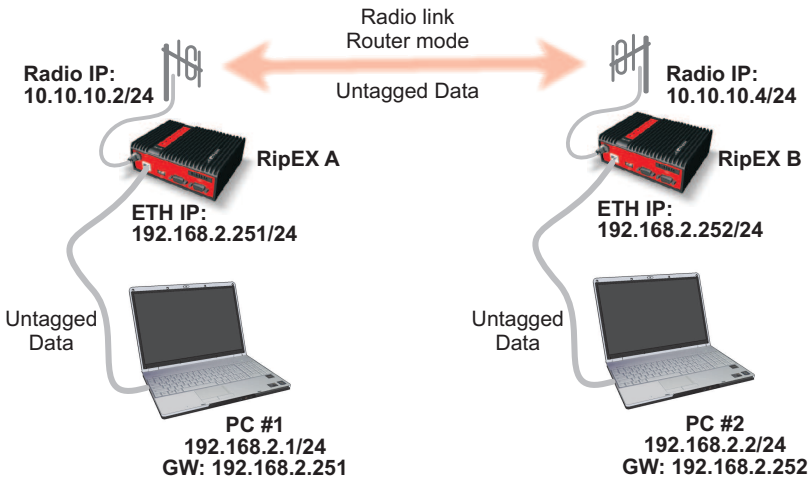
7.3. Příklady konfigurace

V této kapitole projdeme několik příkladů s cílem vysvětlit ARP proxy server a funkce VLAN v praxi. Všechny příklady budou mít stejnou hardwarovou konfiguraci a budeme měnit pouze nastavení softwaru (ARP proxy serveru, VLAN tagging, routing, ...). Namísto RTU použijeme osobní počítače (PC).

Postupujte prosím jeden příklad po druhém, pro úplné pochopení rozdílů v konfiguraci a přínosů různých řešení.

7.3.1. Bez ARP Proxy a bez VLAN

Začneme se základním příkladem konfigurace bez použití ARP proxy nebo VLAN. Viz následující schéma:



Obr. 7.3: Schéma základní konfigurace

Tento příklad neodráží typickou konfiguraci, protože počítače sdílejí stejnou IP podsíť, ale za různými jednotkami RipEX v režimu Router. Obvykle by jednotky RipEX propojily různé IP podsítě. To lze snadno provést pomocí ARP proxy, ale v tomto případě je můžeme nastavit i zvláštními pravidly routingu.

Poznámka

Nepřipojujte PC přes ETH/USB adaptér, ale používejte Ethernetové rozhraní. ETH/USB adaptér lze použít jen pro konfiguraci, nelze použít pro testy připojení.

Konfigurace routeru Ripex

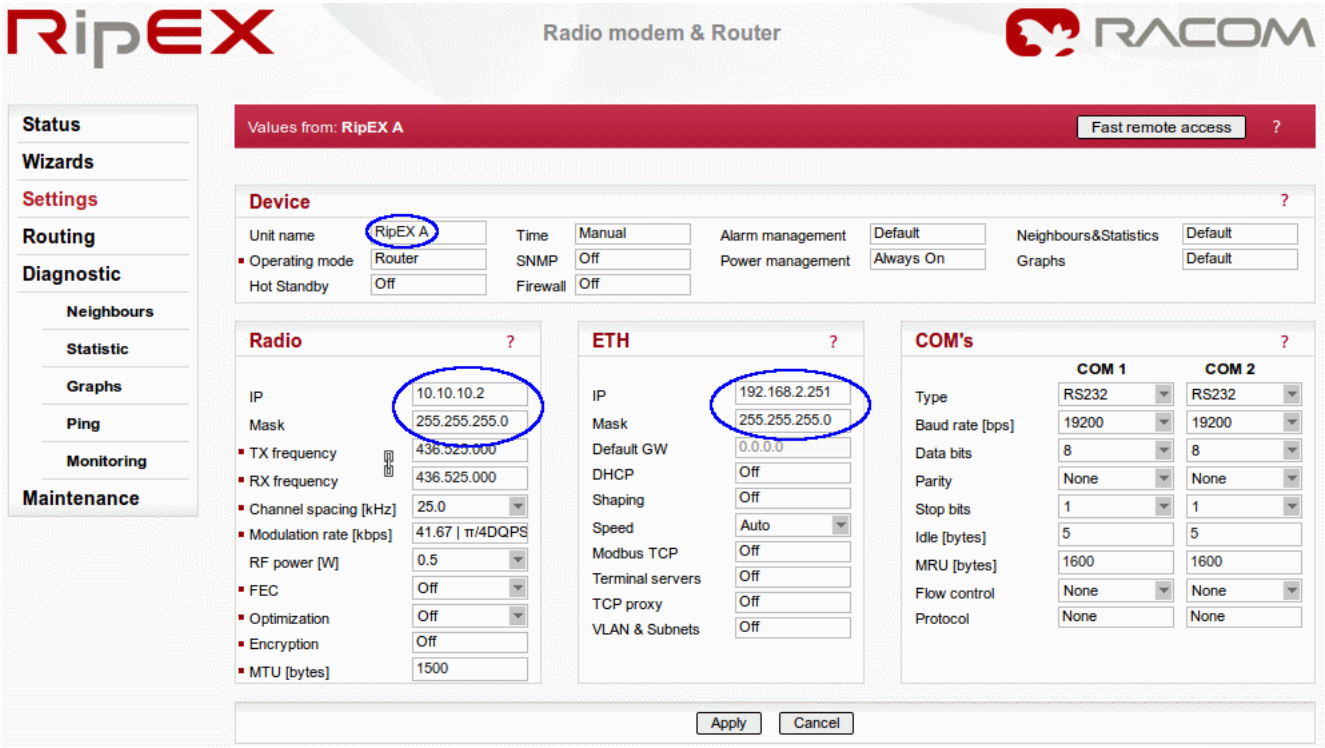
Pro přístup do první jednotky RipEX jděte do Settings a nazvěte ji RipEX A. Nastavte následující IP adresy:

- Radio IP address: 10.10.10.2, mask 255.255.255.0
- Ethernet IP address: 192.168.2.251, mask 255.255.255.0

Na druhé jednotce, nastavte jméno RipEX B a nakonfigurujte ji s příslušnými IP adresami:

- Radio IP address: 10.10.10.4, mask 255.255.255.0
- Ethernet IP address: 192.168.2.252, mask 255.255.255.0

Viz nastavení jednotky RipEX A na následujícím snímku obrazovky.



Obr. 7.4: Nastavení jednotky RipEX A

Nezapomeňte nastavit stejně frekvence TX/RX, kanálový odstup (Channel spacing), modulační rychlost (Modulation rate) a další parametry na obou jednotkách RipEX. **Nepovolujte** ARP proxy nebo VLAN.

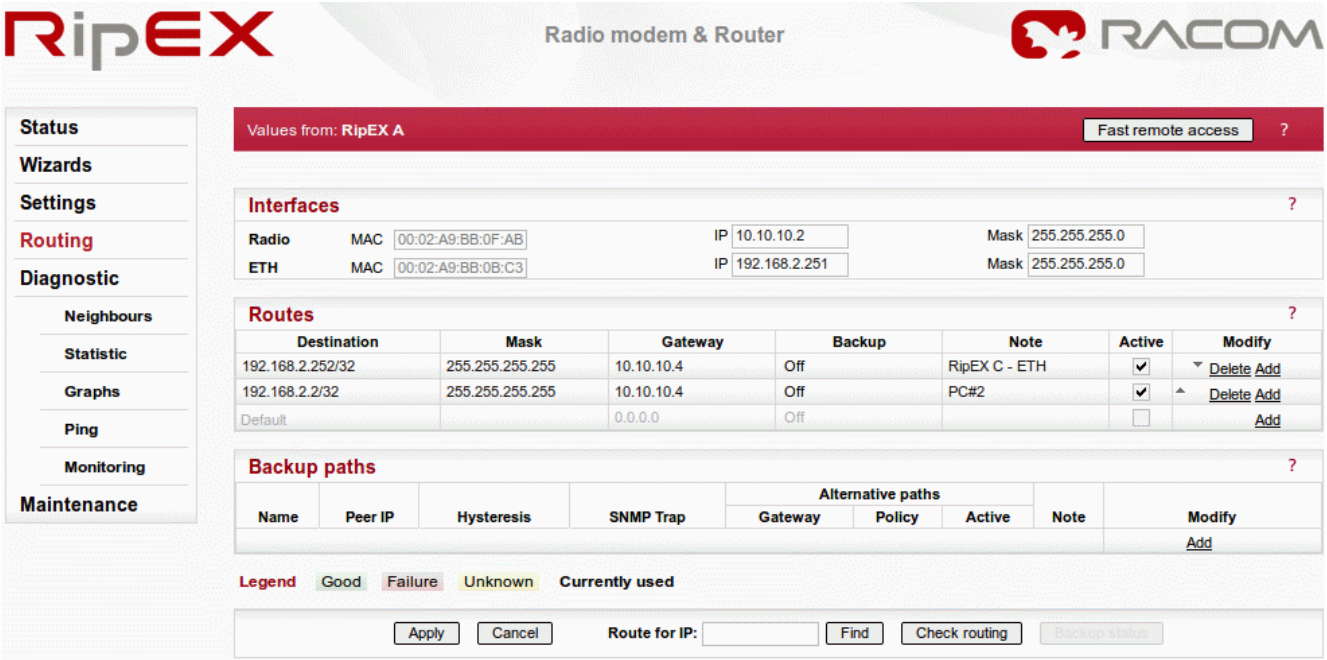
Dalším krokem je nastavení Routingu (viz menu **Routing**). Konfigurujte jednotku RipEX A s těmito pravidly Routingu:

- Destination: 192.168.2.252/32, Mask: 255.255.255.255, Gateway 10.10.10.4
- Destination: 192.168.2.2/32, Mask: 255.255.255.255, Gateway 10.10.10.4

RipEX B bude mít velmi podobné cesty:

- Destination: 192.168.2.251/32, Mask: 255.255.255.255, Gateway 10.10.10.2
- Destination: 192.168.2.1/32, Mask: 255.255.255.255, Gateway 10.10.10.2

Nezapomeňte aktivovat obě cesty. Můžete také přidat poznámku ke každé trase. Viz příklad RipEX A Routing:



Obr. 7.5: RipEX A Routing

Konfigurace počítače

Když jsme úspěšně nakonfigurovali obě jednotky RipEX, můžeme pokračovat s nastavením počítače.

- **PC #1:** IP address: 192.168.2.1, Mask: 255.255.255.0, Default Gateway: 192.168.2.251
- **PC #2:** IP address: 192.168.2.2, Mask: 255.255.255.0, Default Gateway: 192.168.2.252

Poznámka

Pokud si nevíte rady s konfigurací těchto počítačů, viz manuál RipEX, *http://www.racom.eu/eng/products/m/ripex/bench-test.html#connect-PC* (anglicky).

Při společné konfiguraci se dvěma různými IP podsítěmki za jednotkami RipEX, bychom nepotřebovali žádné další kroky k připojení koncového bodu. V tomto příkladu musíme přidat dvě routovací pravidla na obou počítačích.

Chcete-li přidat pravidla Routingu v systému Windows, musíte spustit **Windows Command Processor** (cmd). Klikněte na tlačítko **Start** a potom zadejte příkaz *cmd* ve vyhledávacím poli **Start**. Vyberte ikonu Cmd.

Poté, co se zobrazí okno příkazového řádku, zadejte následující příkazy na PC # 1:

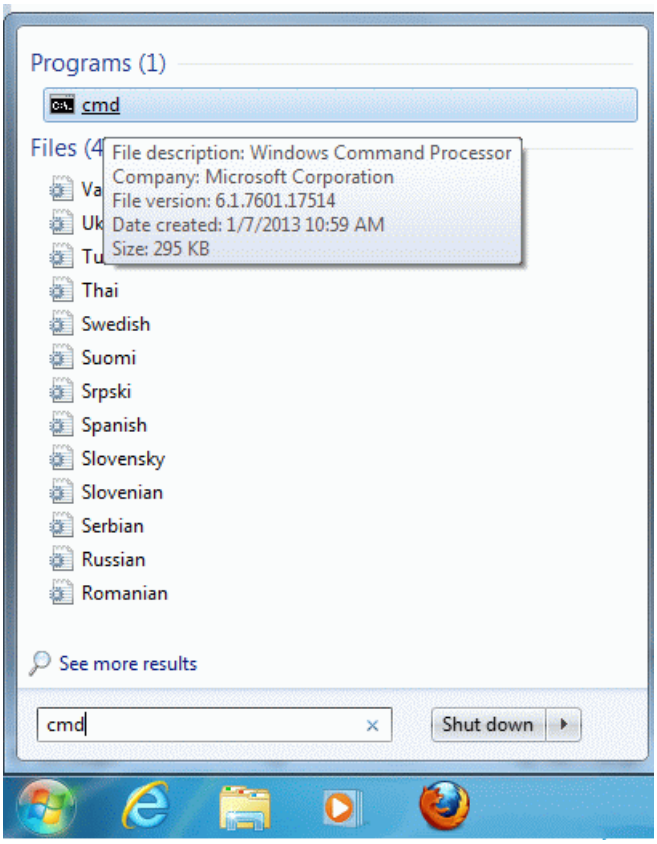
- `route add 192.168.2.252 mask 255.255.255.255 192.168.2.251`
- `route add 192.168.2.2 mask 255.255.255.255 192.168.2.251`

Je také potřeba přidat podobná pravidla Routingu na PC # 2:

- `route add 192.168.2.251 mask 255.255.255.255 192.168.2.252`
- `route add 192.168.2.1 mask 255.255.255.255 192.168.2.252`

Poznámka

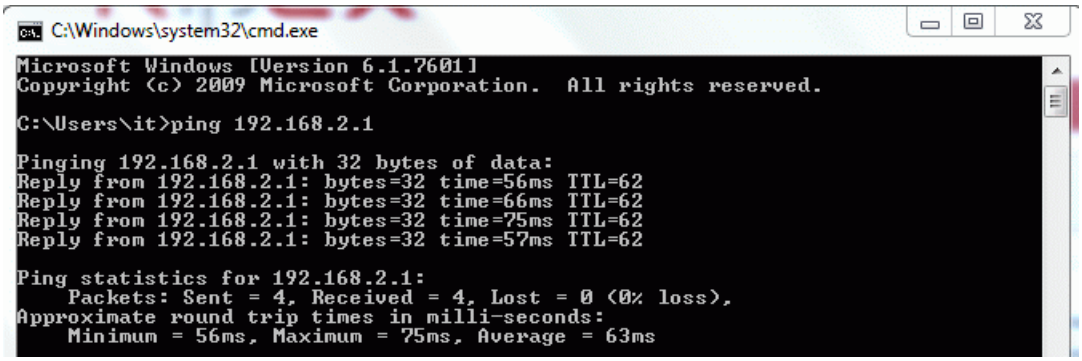
V OS Windows 7 potřebujete pro přidání cesty oprávnění správce (Admin).



Obr. 7.6: Příkazový řádek

Test připojení

Zkontrolujte připojení spuštěním příkazu **ping**, který je také spuštěn z příkazového řádku. Zadejte "ping 192.168.2.1" nebo "ping 192.168.2.251", pokud jste provedli ping z PC # 1 a kontrolujte výsledky. Můžete také zkusit jiný směr, stačí přepnout IP adresy. Viz následující příklad:



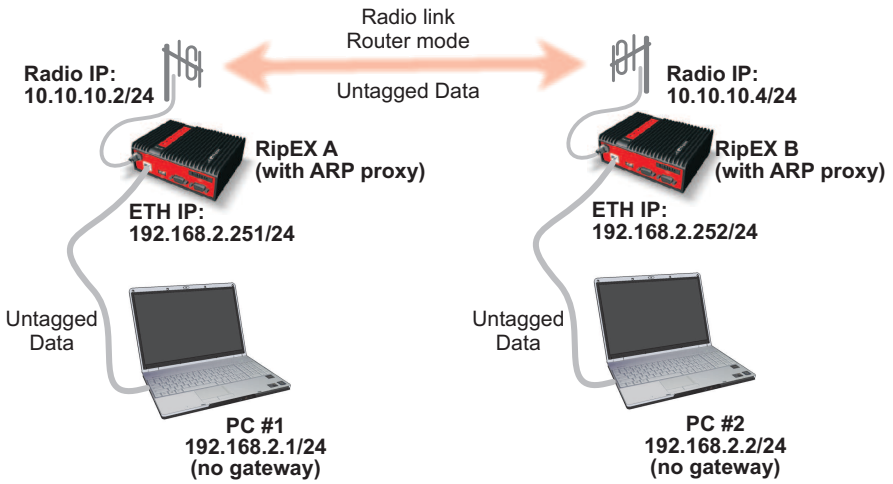
Obr. 7.7: Výsledky příkazu Ping (základní konfigurace)

Poznámka

Pokud ping není úspěšný, zkuste vypnout firewall systému Windows. Ten může blokovat ping pakety.

7.3.2. ARP Proxy

Pokud bychom neměli počítače jako koncové stanice, ale pouze jednoduché stanice RTU, může se stát, že nemohou být nakonfigurovány trasy a výchozí brány. V tomto případě musíme dosáhnout připojení prostřednictvím funkce serveru proxy ARP. Viz diagram:

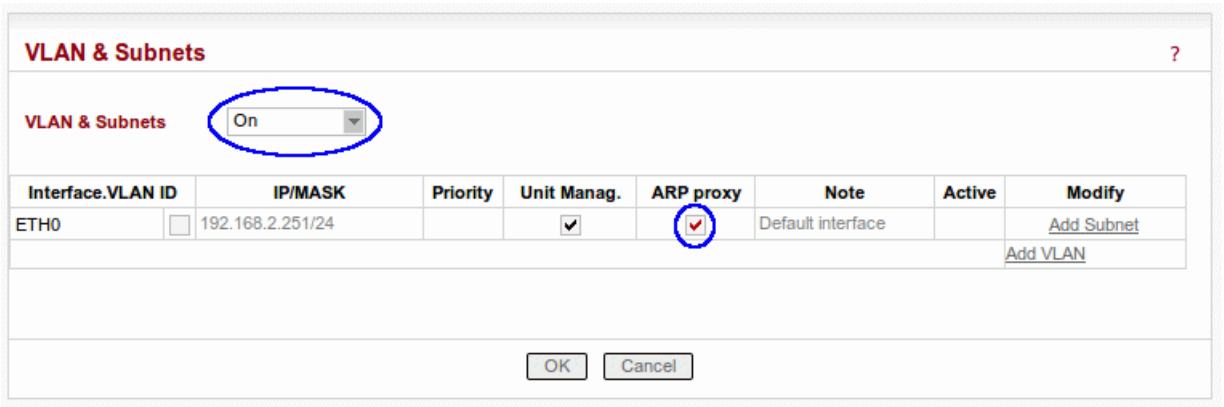


Obr. 7.8: Schéma konfigurace ARP proxy

Konfigurace radiomodemu RipEX

Na obou jednotkách RipEX máme již skoro všechno nakonfigurováno. Stačí jít do menu **Settings** a kliknout na tlačítko **VLAN & Subnets**.

Zapněte funkci a zaškrtněte volbu ARP proxy na obou jednotkách. Potvrďte a uložte změny.



Obr. 7.9: Povolení ARP proxy

Nemusíte měnit pravidla routingu. Jen nezapomeňte, že funkce proxy ARP funguje pro všechny cílové IP adresy v routingové tabulce jednotky RipEX. RipEX nebude napodobovat ARP proxy v odpovědích na jinou IP adresu.

Přidání routingových pravidel umožní ARP proxy na jiných IP adresách (například pokud chcete používat ARP proxy pro IP adresy 192.168.2.8-15, přidejte IP podsítě 192.168.2.8/29 do routingových pravidel).

Konfigurace počítače

Oba počítače mají stejné IP adresy jako v příkladě základní konfigurace. Stačí odstranit výchozí bránu.

- **PC #1:** IP address: 192.168.2.1, Mask: 255.255.255.0
- **PC #2:** IP address: 192.168.2.2, Mask: 255.255.255.0

Je třeba odstranit routingová pravidla, která jsme přidali dříve. Stačí jít znovu do příkazového řádku a zadat následující příkazy:

- **PC #1:**
  - route delete 192.168.2.252 mask 255.255.255.255 192.168.2.251
  - route delete 192.168.2.2 mask 255.255.255.255 192.168.2.251
- **PC #2:**
  - route delete 192.168.2.251 mask 255.255.255.255 192.168.2.252
  - route delete 192.168.2.1 mask 255.255.255.255 192.168.2.252

Zkouška spojení

Test je úplně stejný jako v kapitole *„Test připojení“*.

Nejdůležitější věcí je zapamatovat si v příkladě s ARP proxy, že jsme nemuseli konfigurovat jakoukoli výchozí bránu nebo routingová pravidla na počítačích (RTU stanicích). Díky tomu můžeme přidat i „jednoduché“ RTU stanice do naší sítě a můžeme mít stejné IP podsítě za různými jednotkami RipEX.

Tip

Pečlivě zvažte návrh sítě, protože dobrý design sítě může výrazně snížit počet potřebných routingových pravidel v routingové tabulce jednotky RipEX.

Příklad 7.1. Routingová pravidla

Máte čtyři koncové stanice s IP adresami 192.168.2.1, .2.2, .2.5 a 2.6 a potřebujete dvě z nich za jednotkou RipEX A a dvě z nich za jednotkou RipEX B. S adresou 192.168.2.1 a .2.2 za jednotkou RipEX A, budete potřebovat přidat pouze jedno pravidlo v jednotce RipEX B: 192.168.2.4/30 přes RipEX A. V opačném případě budete muset přidat dvě pravidla (např s .2.1 a .2.5 IP adresami).

7.3.3. VLAN

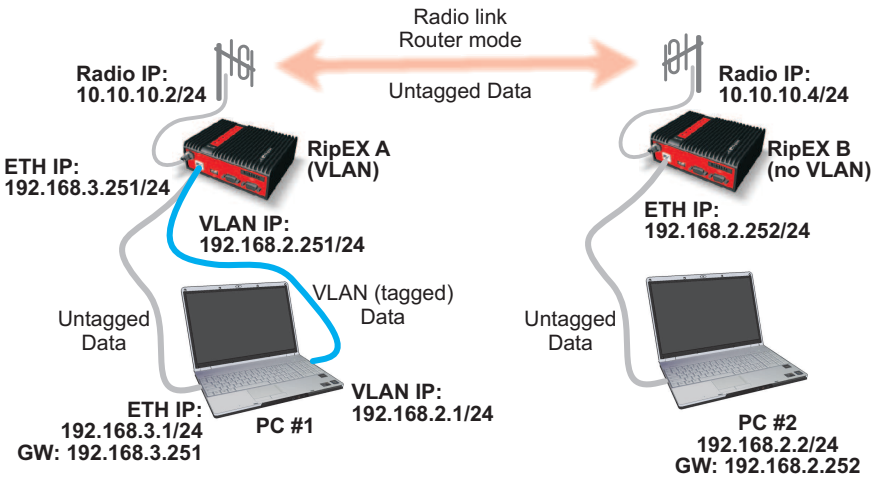
Vysvětlíme dva podobné příklady ukazují funkci VLAN.

VLAN na jednom konci

V tomto příkladě budeme mít VLAN ID 2 použitou mezi jednotkou RipEX A a PC # 1. Management jednotky RipEX na stejném ethernetovém portu bude netagovaný.

Provoz na rádiovém kanálu je vždy netagovaný.

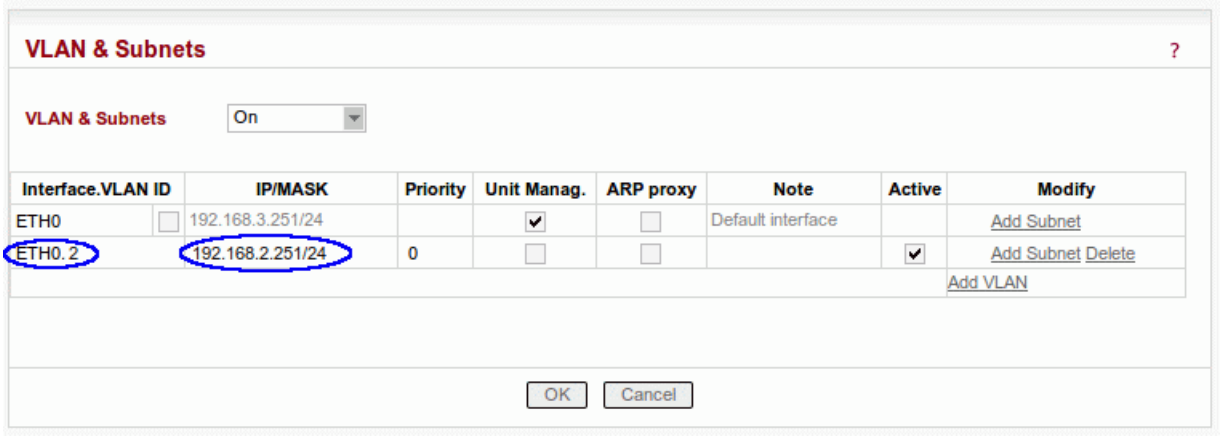
Komunikace mezi jednotkou RipEX B a PC # 2 bude také netagovaná.



Obr. 7.10: Schéma konfigurace VLAN

Konfigurace radiomodemu RipEX

Konfigurace jednotky RipEX A bude trochu složitější. K dispozici budou dvě podsítě, jedna pro VLAN a jedna pro ostatní komunikaci. Jděte do menu **Settings** a změňte Ethernetovou IP adresu na 192.168.3.251. Poté klikněte na tlačítko **VLAN & Subnets** a přidejte novou VLAN – budeme používat VLAN ID 2 s IP adresou 192.168.2.251.



Obr. 7.11: RipEX A – konfigurace VLAN

Na jednotce RipEX B, vypněte volbu VLAN & Subnets.

Pravidla routingu mohou zůstat na obou jednotkách stejná jako u předchozího příkladu ARP proxy. Chcete-li mít management IP podsítě (ETH) jednotky RipEX A dostupný z jednotky RipEX B, přidejte toto pravidlo pro routing: 192.168.3.0/24 přes 10.10.10.2. Ale není to nutné pro připojení koncové stanice.

Nastavení počítače

Konfigurace IP PC #2 je stejná.

- IP address: 192.168.2.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.2.252

Nastavení PC # 1 není tak jednoduché. Nastavte prosím následující parametry:

- IP address: 192.168.3.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.3.251

Jak můžete vidět, jsme napojeni na RipEX A uvnitř managementu IP podsítě 192.168.3.0/24. My ale stále potřebujeme nakonfigurovat rozharní VLAN. Tento krok se liší podle operačního systému (OS), který používáte. Popíšeme nezbytné kroky v Ubuntu 12.04 a dáme vám také krátký popis pro Windows 7.

Ubuntu 12.04

V příkazovém řádku zadejte následující příkazy:

```
modprobe 8021q
vconfig add eth0 2
ip link set eth0.2 up
ip link set mtu 1496 dev eth0.2
ip addr add 192.168.2.1/24 dev eth0.2
```

Nejdůležitější je příkaz **vconfig**, který vytváří VLAN rozhraní s názvem eth0.2. Umožníme tím rozhraní snížit MTU, protože další 4 bajty jsou přidány do každého frame kvůli VLAN tag a samozřejmě přiřadíme IP adresu rozhraní.

Poslední dva příkazy vytvářejí cesty, takže paket určený pro 192.168.2.2 nebo 192.168.2.252 je směrován přes gateway 192.168.2.251 (rozhraní RipEX VLAN).

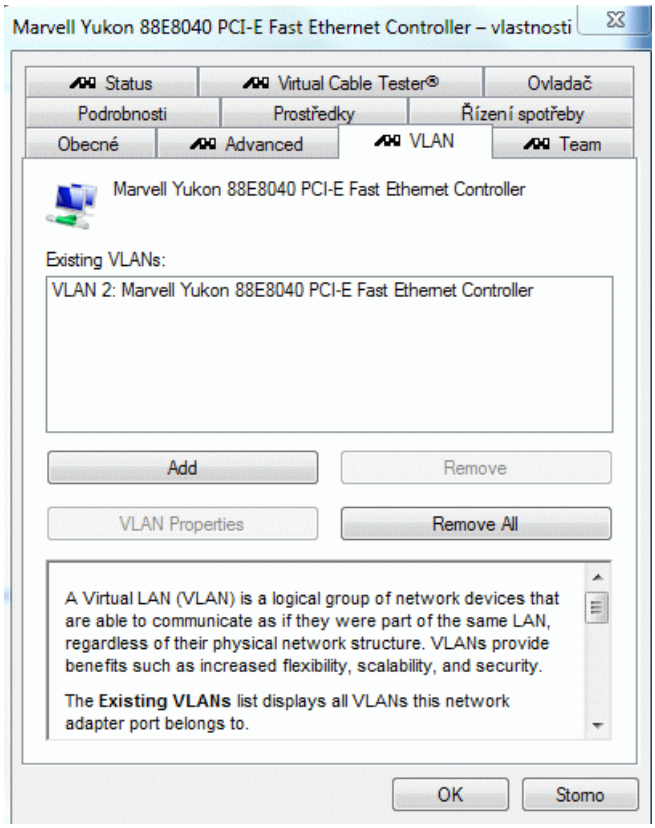
Windows 7

V operačním systému Windows 7 neexistuje žádný nástroj jako vconfig. Funkce VLAN jsou závislé na síťovém adaptéru a nainstalovaných ovladačích. Podívejte se prosím na příslušné stránky vaší síťové karty pro získání správného ovladače VLAN.

Poznámka

Může se stát, že vaše síťová karta nebude sítě VLAN vůbec podporovat.

Chcete-li zjistit, jakou máte síťovou kartu a ovladače, jděte do menu **Start** → **Ovládací panely** → **Systém a zabezpečení** → **Správce zařízení** → **Síťové adaptéry**. Zde byste měli vidět vaši síťovou kartu. Klikněte na ni pravým tlačítkem myši a zvolte možnost **Vlastnosti**.



Obr. 7.12: Přidání VLAN v OS Windows 7

V našem příkladě jsme přidali rozhraní VLAN 2. Pro více informací viz manuál síťové karty.

Pokud jste byli úspěšní při přidávání nového VLAN rozhraní, měli byste vidět toto rozhraní mezi jinými fyzickými rozhraními sítě. Nastavte IP adresu, masku a bránu jako obvykle:

- IP address: 192.168.2.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.2.251

Nyní stačí přidat cesty na IP adresy 192.168.2.2 a 192.168.2.252 IP. Spusťte příkazový řádek a zadejte:

```
route add 192.168.2.252 mask 255.255.255.255 192.168.2.251
route add 192.168.2.2 mask 255.255.255.255 192.168.2.251
```

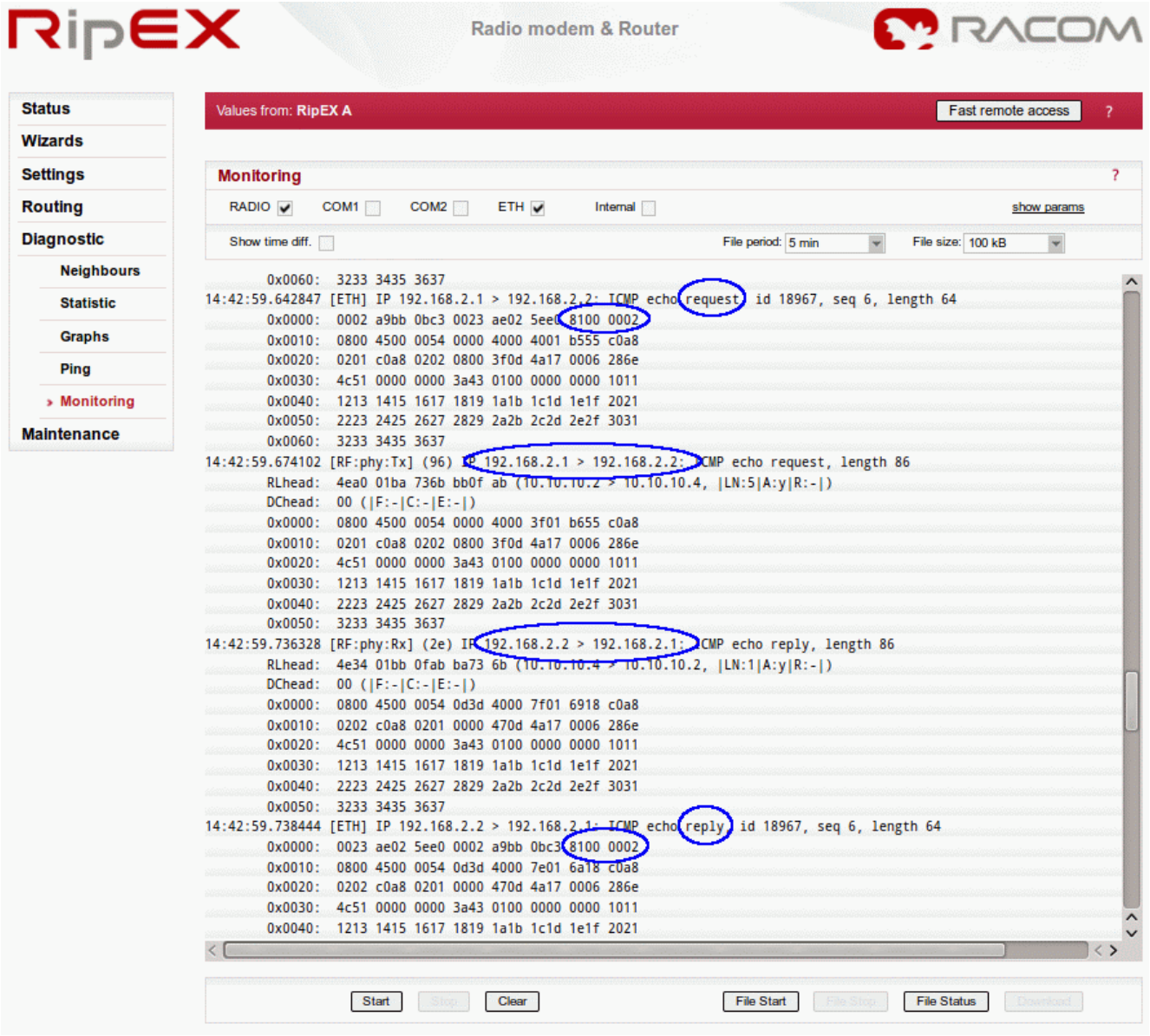
Poznámka

V OS Windows 7 potřebujete pro přidání cesty oprávnění správce (Admin).

Zkouška spojení

Tento test je stejný, jak je popsáno v předcházejících kapitolách.

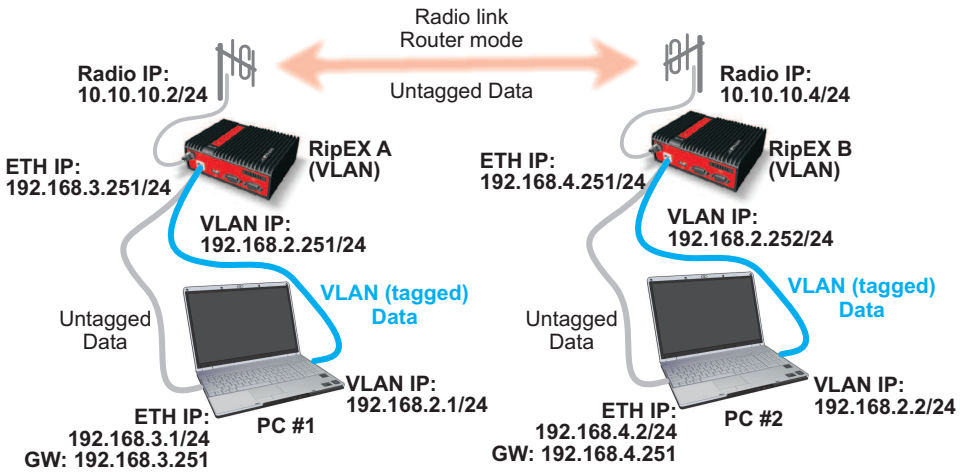
Můžete spustit funkci Monitoring v jednotce RipEX pro sledování paketů na rozhraní rádio/Ethernet a uvidíte Ethernet VLAN tagy a další informace. Viz následující příklad:



Obr. 7.13: Monitoring ping paketů s VLAN tagy

VLAN na obou koncích

Můžeme také nastavit VLAN na obou jednotkách RipEX, takže údaje VLAN (označené) budou také přenášeny prostřednictvím Ethernetové linky mezi PC # 2 a jednotkou RipEX B. Nicméně provoz je vždy neoznačený na rádiovém kanále.



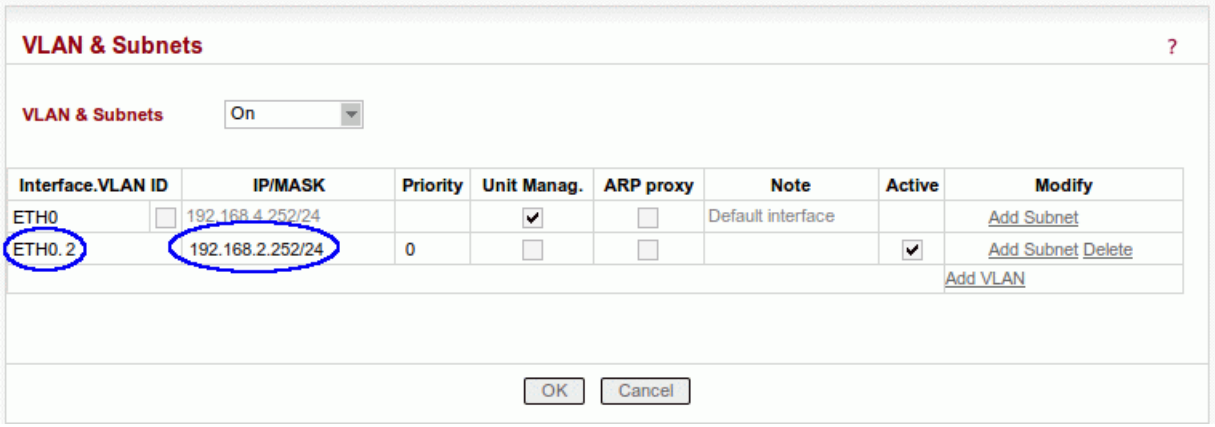
Obr. 7.14: Schéma konfigurace VLAN č. 2

Konfigurace jednotky RipEX

RipEX má stejnou konfiguraci jako v předchozím příkladu. Pokud si chcete vyzkoušet připojení ETH rozhraní jednotky RipEX, budete muset přidat toto routingové pravidlo:

- Destination: 192.168.4.0/24, Mask: 255.255.255.0, Gateway 10.10.10.4

U jednotky RipEX B je třeba provést několik změn. Změňte ethernetovou IP adresu 192.168.4.252 s maskou 255.255.255.0. Nyní přejděte do menu **VLAN & Subnets**, povolte funkci a přidejte novou VLAN - nepoužívejte VLAN ID 2 s IP adresou 192.168.2.252.



Obr. 7.15: Konfigurace VLAN jednotky RipEX B

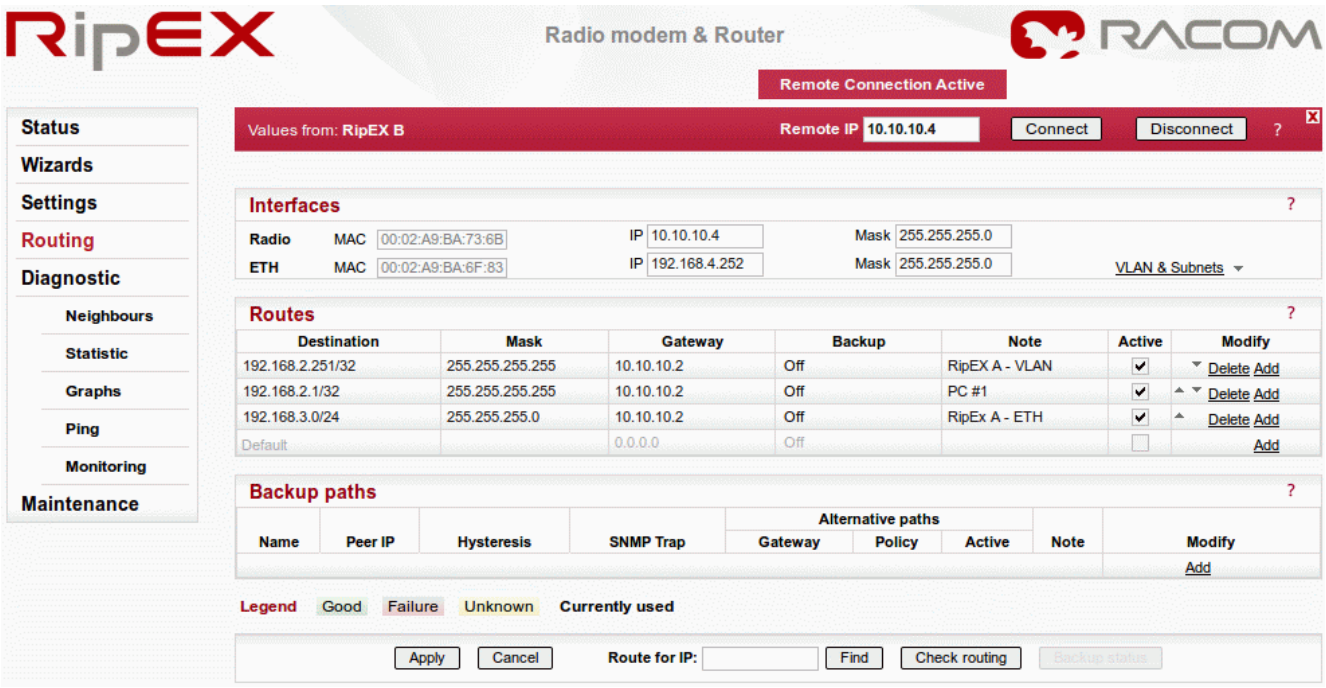
VLAN ID je stejné jako u jednotky RipEX A, ale v případě potřeby lze nastavit jakékoliv ID.

Poznámka

Po dokončení tohoto příkladu můžete zkusit povolit VLAN na výchozím rozhraní.

Routingová tabulka pro jednotku RipEX B má tři pravidla:

- Destination: 192.168.2.251/32, Mask: 255.255.255.255, Gateway 10.10.10.2
- Destination: 192.168.2.1/32, Mask: 255.255.255.255, Gateway 10.10.10.2
- Destination: 192.168.3.0/24, Mask: 255.255.255.0, Gateway 10.10.10.2



Obr. 7.16: Routingová tabulka jednotky RipEX B

Konfigurace počítače

Nemusíme nic měnit na PC # 1. PC # 2 potřebuje následující změny:

- IP address: 192.168.4.2, mask 255.255.255.0, gateway 192.168.4.252

Nyní musíme přidat rozhraní VLAN s ID 2. Viz postup v předchozím příkladu.

Pokud jste přidali rozhraní VLAN, přidejte následující pravidla pro Routing:

- **route add 192.168.2.251 mask 255.255.255.255 192.168.2.252**
- **route add 192.168.2.1 mask 255.255.255.255 192.168.2.252**

Poznámka

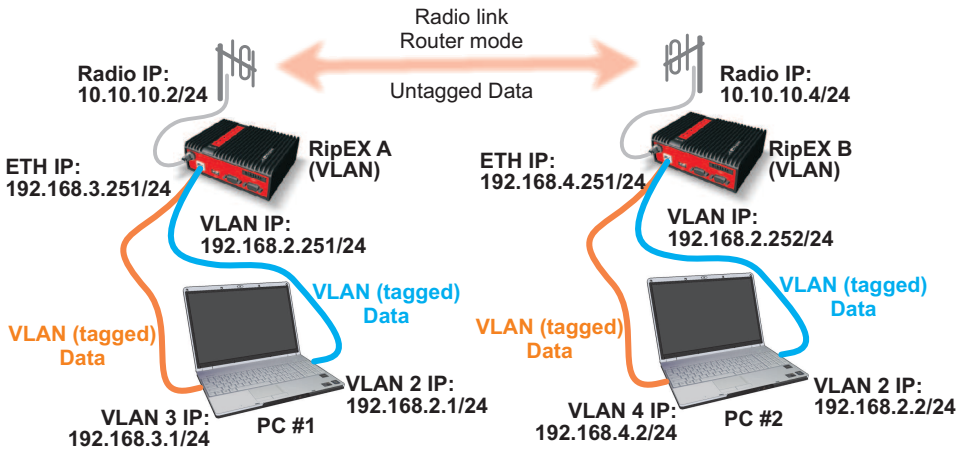
V OS Windows 7 potřebujete pro přidání cesty oprávnění správce (Admin).

Zkouška spojení

Postupujte podle kroků popsaných v některém z předchozích kapitol s názvem „Zkouška spojení“. Měli byste být schopni poslat ping z kteréhokoliv zařízení na jakoukoliv VLAN nebo Ethernetovou IP adresu.

Management VLAN

Nyní byste měli mít dostatek zkušeností pro další test. Nastavte jinou VLAN ID na obou počítačích. Použijte stejnou VLAN ID na rozhraní ETH.0 pro **RipEX management**. Budete mít sítě „VLAN only“.



Obr. 7.17: Schéma managementu VLAN

Poznámka

VLAN 2 je ve stejné podsíti 192.168.2.0/24. VLAN 3 je v podsíti 192.168.3.0/24 a VLAN 4 v podsíti 192.168.4.0/24.

8. SNMP

8.1. Simple Network

SNMP je jednoduchý, široce využívaný standardizovaný protokol, který obvykle používá Network Management Software (NMS) ke čtení hodnot ze zařízení. Hodnoty lze získávat v pravidelných intervalech nebo na základě žádostí, ukládat do databáze a následně zobrazovat jako grafy nebo tabulky.

SNMP také umožňuje zařízením samostatně generovat alarmy a oznamovat to přímo NMS (SNMP Notification).

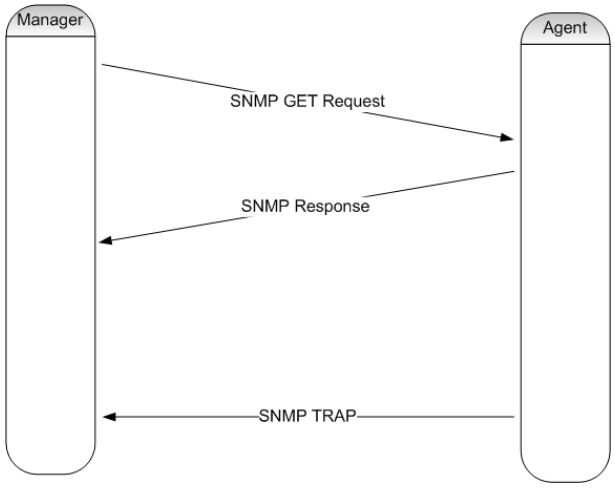
8.1.1. Jak SNMP funguje?

SNMP potřebuje pro komunikaci dvě strany :

1. SNMP "manager" (software instalovaný v počítači)
   - Můžete použít komerční software nebo free software jako je Zabbix, Zenoss, Nagios, Cacti atd. Pokud chcete číst hodnoty manuálně, můžete použít sw nástroje jako snmpwalk, snmpget nebo Mibbrowser.
2. SNMP "agent" (součást firmware ve vzdálených zařízeních jako jsou rádiové modemy RipEX)
   - Agent obdrží SNMP žádosti s dotazy na informace a reaguje na manažera. Několik manažerů může číst hodnoty najednou a mohou kdykoliv posílat své žádosti. Alternativně agent odesílá SNMP Notification vždy, když sledované hodnoty (v jednotce RipEX, např. teplota) jsou mimo stanovený rozsah. Jednotka RipEX je schopna posílat SNMP až na dva SNMP manažery (od verze firmware 1.3).

8.1.2. SNMP Komunikace

V SNMP je každá hodnota jednoznačně identifikována pomocí objektového identifikátoru (OID). Standardní komunikace začíná tím, že se pošle požadavek a pak se vrací odpověď. Alternativně agent může poslat SNMP Notification.



Obr. 8.1: SNMP komunikace

Poslání žádosti	manager nastaví zprávy typu GET obsahující OID pro požadovanou hodnotu a nastaví tuto hodnotu na NULL.
Navrácení odpovědi	agent nastaví zprávu typu odpověď a pošle požadovanou hodnotu spolu s jeho OID zpět managerovi.
Odeslání Notification	manažerovi bez jeho žádosti. Notification je Trap (bez potvrzení) nebo Inform (s potvrzením).

Základní typy zpráv

GetRequest	vrátí jednu hodnotu.
GetNextRequest	vrátí následující hodnotu (pomocí následujícího OID).
GetBulkRequest	vrací několik hodnot v jednom paketu (například teplotu, napětí, počet přenesených zpráv nebo bytů za sekundu, atd.).
Notification	odesílána z agenta manažerovi, když některá monitorovaná hodnota je mimo její mezní hodnoty.
SetRequest	slouží k nastavení různých parametrů (nepodporovaný radiomodemem RipEX).

8.1.3. MIB databáze – Management Information Base

MIB je virtuální databáze používaná ke správě subjektů v komunikační síti.

Hierarchie MIB databáze může být zobrazena jako strom s bezejmenným kořenem, jehož úrovně jsou přiřazovány různými organizacemi. MIB OID "vyšší úrovně" patří různým normotvorným organizacím, zatímco OID "nižší úrovně" jsou přiděleny přidruženými organizacemi (např. RACOM).

Příklad OID:

```
RIPEX::serialNumber
serialNumber OBJECT-TYPE
-- FROM RIPEX
SYNTAX Unsigned32
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Product serial number."
::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) racom(33555) ripex(2) ▶
station(1) device(1) 4 }
```

Jak můžete vidět, čísla 1.3.6.1.4.1.33555 jsou "vyšší úrovně" OID. V OID "nižší úrovně" jsou čísla .2.1.1.4, která jsou přidělena firmou RACOM.

8.2. SNMP v RipEXu

V jednotce RipEX lze protokol SNMP použít ke:

- Čtení konfiguračních parametrů z MIB,
- Čtení statistiky provozu na rádiovém kanále, a
- Odesílání Notification při překročení nastavené mezní hodnoty sledovaných hodnot (TxLost [%], UCC, Temp, PWR, ...)

Podrobný popis jednotlivých hodnot naleznete v sekci RipEX MIB níže.

RipEX využívá SNMP verze SNMPv1, SNMPv2c (používá řetězec „community string“ pro autentizaci, který ve výchozím nastavení nabývá hodnoty "public", avšak lze jej změnit) a SNMPv3 (používá Security User name, Security level, autentizační a kryptovací mechanismy). SNMP používá UDP protokol pro komunikaci; kontroly doručení byly prováděny od verze 2.

Poznámka

MIB modul routeru RipEX splňuje kontrolu validity pro „severity level“ 3.

Ve výchozím nastavení používá RipEX UDP port 161 (SNMP) pro dotazy. Manager, který odešle dotaz, dynamicky vybere port, z něhož posílá své dotazy RipEXu na port 161. RipEX odpovídá z portu 161 dynamicky vybranému portu managera.

RipEX spustí agenta SNMP při startu automaticky, pokud je to povoleno. RipEX také vysílá alarmové stavy (Notification) do managera z portu 162 (SNMPTRAP). Uživatelé mohou toto číslo portu změnit v RipEXu. Chování „Notification“ lze nastavit (viz RipEX manual, Adv. config., *Settings / Alarm management*[1]).

Při použití SNMP přes rádiový kanál doporučujeme nastavit RipEX do režimu „router mode“. Z hlediska rádiové sítě je SNMP obvykle samostatná aplikace sdílející rádiový kanál s ostatními. To způsobí, že kolize jsou automaticky vyřešeny pomocí protokolu rádiového kanálu v režimu router mode. Rádiový kanál nepoužívá v režimu bridge mode žádný protokol, což znamená, že dvě konkurenční aplikace lze spustit pouze s vědomím velkého rizika kolizí a toho, že pakety z obou aplikací se mohou nenávratně ztratit.

8.2.1. Omezení

Protokol SNMP je primárně určen pro ethernetové sítě, kde kapacita obecně není problém. Naproti tomu kapacita rádiového pásma je velmi omezená a router RipEX většinou pracuje přes rádiový kanál. Z tohoto důvodu se konfiguraci NMS doporučuje věnovat zvláštní péči. V případě špatného nakonfigurování si může vyžádat NMS významnou část kapacity sítě nebo síť dokonce zcela přetížit.

Potřeba šířky pásma

Je důležité si uvědomit, že průměrná velikost každého jednoho požadavku na základě zvláštního OID je přibližně 184 bajtů. Celá MIB pro jeden RipEX se sousedním RipEXem je přibližně 48 KB. Kvůli omezení velikosti MIB doporučujeme přes rádiový kanál posílat pouze pečlivě vybrané dotazy OID a ne všechna možná data. Nastavte časové intervaly SNMP ve svých NMS co možná nejdelší. Nejkratší doporučený interval se pohybuje v rozmezí od několika minut do desítek minut.

Při použití SNMPv3 je obtížnější stanovit zvýšení množství dat, protože může být zvoleno více úrovní zabezpečení. Pro přenesení zprávy SNMP ve verzi 3 je potřebné zhruba dvojnásobné množství dat ve srovnání se SNMPv2c. Berte to v úvahu, pokud se provoz SNMP přenáší rádiovým kanálem.

Kdykoli je to možné, použijte pro SNMP komunikaci RipEXu ethernetové rozhraní, aby se uvolnil rádiový kanál.

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

Poznámka

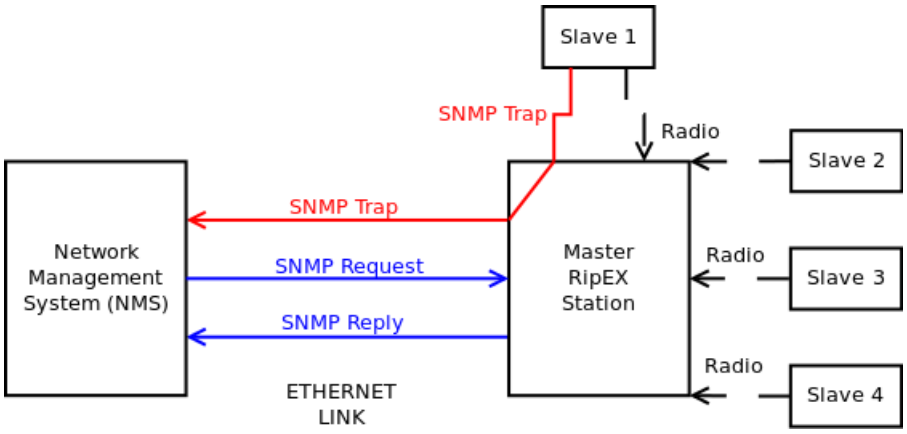
Na trhu existuje celá řada Network Management Systemů. Záleží jen na vás, který použijete, mějte ale na paměti popsaná omezení. Např. nikdy nepoužívejte NMS, který umožňuje stáhnout pouze celou MIB ze vzdáleného zařízení a ne jednotlivé OID.

Tip pro efektivní šířku pásma

Chcete-li kontrolovat mnoho sledovaných hodnot (PSV, teplota, napětí, ...) ze vzdálených stanic připojených rádiovým kanálem a máte síť s topologií hvězda, můžete zlepšit využití šířky pásma tím, že čtete OID hodnoty pouze z RipEXu Master (Repeater).

Výhodou výše uvedeného je, že sledované hodnoty vzdálených stanic jsou vysílány v pravidelných intervalech a uloženy do RipEXu Master (Repeater). Tyto hodnoty ze sousedních stanic mají své vlastní OID a lze je stáhnout z RipEXu Master (Repeater).

Na níže uvedeném obrázku - stanice Master RipEX pravidelně čte sledované hodnoty ze svých sousedních stanic Slave. Kdykoli NMS požaduje jakoukoliv uvedenou hodnotu, odpověď je odeslána pouze z RipEXu Master Station (Ethernetem) a tak šetří pásmo rádiového kanálu. SNMP využívá rádiové spojení pouze pro zasílání SNMP Notification z libovolné stanice do NMS.



Obr. 8.2: Komunikace NMS s podřízenými stanicemi

Poznámka

V takovém případě jsou sledované hodnoty sousedních stanic zobrazeny jako součást Master (Repeater) stanice.

8.2.2. RipEX SNMP Settings

SNMP agent je ve výchozím nastavení vypnutý. Chcete-li to povolit, přejděte do menu settings a klikněte na tlačítko SNMP. Můžete nastavit Community, zapnout SNMP Notification a definovat dvě IP adresy Notification destination a porty.

Důležité

Limity pro všechny SNMP Notification je možné konfigurovat z webového rozhraní RipEXu, Settings → Alarm management. Vzhledem k tomu, že se podrobný popis nastavení SNMP Notification RipEXu může lišit v závislosti na aktuálním firmware, hledejte jej prosím v nápo-

vědě přístupné online přes webové rozhraní RipEXu nebo v návodu k použití – kapitola Settings (*http://www.racom.eu/eng/products/m/ripex/h-menu.html#settings*).

8.2.3. Popis RipEX Notification (Trap, Inform)

Notification se odesílá vždy, když některá z těchto sledovaných hodnot je mimo její mezní hodnoty:

- RSS (Received Signal Strength) – Úroveň signálu
- DQ (Data Quality) – Kvalita dat
- TX Lost – Pravděpodobnost ztráty vysílaného rámce
- UCC – Napájecí napětí [V]
- Temperature [C] – Teplota [°C]
- RF Power [W] – výstupní rádiový výkon [W]
- VSWR (Voltage Standing Wave Ratio) – PSV Poměr Stojatých Vln,
  1,0 = nejlepší poměr
  1,0 - 1,8 = přijatelný poměr
  > 2,5 = indikuje vážný problém antény nebo jejího napáječe
- Ethernet RX/TX Packets ratio – Poměr přijatých a odeslaných paketů přes Ethernet
- COM1/2 RX/TX Packets ratio – Poměr přijatých a odeslaných paketů přes COM porty
- HW Alarm input – HW alarmový vstup
- Hot-Standby – SNMP Notification s identitou aktivní stanice - zaslaný aktivní stanicí
- Backup paths system – Stav záložní trasy a stav změny alternativní trasy
- Unit ready – Hardwarový alarmový výstup nebo SNMP Notification indikuje, že rádiový modem RipEX je připraven k provozu

8.3. Network Management System – ZABBIX

Pro přístup k našim SNMP hodnotám můžeme použít jakýkoliv systém pro správu sítě (NMS). Nicméně, doporučujeme používat open source monitorovací systém Zabbix. Lze jej stáhnout na adrese: *http://www.zabbix.com/download.php*

Webové stránky Zabbix obsahují následující krátký popis:

Zabbix je systém pro řešení monitoringu výkonu dostupný jako open source. Zabbix nabízí pokročilé monitorování, upozorňování a vizualizaci, jaké chybí u jiných monitorovacích systémů, dokonce i některých z nejlepších komerčních.

Pokud jste zvolili software Zabbix, přečtěte si následující stránky, kde nabízíme základní startovaci příručku na společné použití RipEXu a Zabbixu. Jeho části mohou být v každém případě užitečné jako obecně platné rady a tipy.

Poznámka

Následující návod byl testován se systémem Zabbix release 2.2.0. Měl by fungovat na libovolném release 2.0.x, nebo jakékoliv novější verzi 2.2.x. Pokud používáte některou z 1.8.x verzí, mohou některé úkoly vyžadovat jiný přístup.

Využijte příležitosti ke vzdáleného přístupu a otestujte *Zabbix demo*[2]. Kontaktujte nás pro *přístupové údaje*[3].

[2] http://www.racom.eu/eng/products/m/ripex/demo/zabbix.html
[3] http://www.racom.eu/eng/products/remote-access.html#load(product=zabbix)

8.3.1. Instalace a dokumentace

Zabbix je testován na následujících platformách:

- Linux
- IBM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Pouze Zabbix agent: Windows Server 2003, Server 2008, 7, 8, 10

Pro další informace, navštivte dokumentaci Zabbix na *http://www.zabbix.com/documentation.php*. Ta obsahuje širokou škálu informací o krocích instalace, konfigurace atd. Pokud si nejste jisti jak postupovat, při jakémkoliv úkolu, hledejte nejdříve v dokumentaci Zabbix. Tam také najdete návod k instalaci.

Tato příručka neobsahuje všechna nastavení Zabbixu, ale měla by vám pomoci včlenit funkčnost RipEX SNMP do softwaru Zabbix.

Poznámka

Následující návod vyžaduje použití MySQL databáze užité v Zabbixu. Pokud zvolíte jinou, budete muset změnit minimálně „script trap handling bash“.

Instalace ve Windows

Pokud potřebujete používat platformu Windows jako operační systém hostitele pro Zabbix, můžete si nainstalovat software VMware / VirtualBox a nainstalovat Zabbix Appliance. Software Zabbix Appliance lze stáhnout z *http://www.zabbix.com/download.php*. Mějte na paměti, že software Zabbix Appliance není určen k vážnému produkčnímu použití.

VMware download: *https://www.vmware.com/support/*
VirtualBox download: *https://www.virtualbox.org/wiki/Downloads*
Viz příslušnou dokumentaci o tom, jak nainstalovat a používat virtualizační software.

8.3.2. Šablony (Templates)

Po úspěšné instalaci můžete importovat některou z předdefinovaných šablon (template). Každá šablona je sbírkou Zabbix položek podle sady OID, triggerů, grafů a aplikací. Šablona může být snadno spojena s jakýmkoli sledovaným zařízením typu host (RipEX) a můžet mít velmi rychle přístup k požadovaným hodnotám.

Jaké šablony můžeme poskytnout?

Seznam šablon:

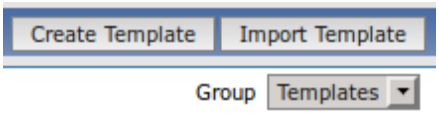
- Název: RipEX Template
  - Skládá se ze všech specifických OID poskytovaných firmou RACOM
  - Monitoruje jeden sousední RipEX
  - 17 aplikací, 237 položek, 4 triggery, 5 grafů
- Název: RipEX – RFC1213 Template

  - Skládá se z podporovaných RFC1213 OID
  - 1 aplikace, 56 položek
- Název: RipEX – RS232 Template
  - Skládá se z podporovaných RS232 OID
  - 1 aplikace, 21 položek
- Název: RipEX – SNMP Trapper Template
  - Skládá se z položek SNMP Trapper, které jsou aktivovány pomocí 15 druhů trapů
  - 1 aplikace, 15 položek, 15 trigerů
- Název: PING Template
  - Pingy definované hostem se aktivují vždy, když host je nedostupný
  - 1 aplikace, 2 položky, 1 triger

Všechny šablony je možné stáhnout ze stránek RipEX Download na: *http://www.racom.eu/download/hw/ripex/free/eng/3_fw/RipEX_Zabbix_templ.zip*

Jak importovat šablony RipEX?

Aby bylo možné importovat šablonu, klepněte na tlačítko **Configuration** → **Templates** v horní části webové stránky Zabbix. V pravém horním rohu uvidíte tlačítko **Import Template** a klikněte na něj.

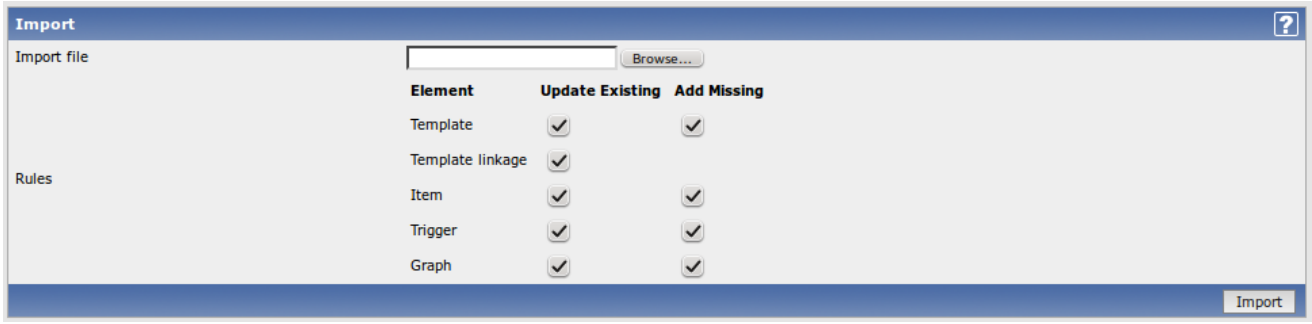


Obr. 8.3: Tlačítko Import Template

Důležité

Před importem souboru šablony si přečtěte kapitolu *8.3.4 – „Hodnoty Mappings“*. Od verze Zabbix releasse 2.2.1 je povinné definovat před importem požadované šablony value mappings.

Vyberte soubor šablony RipEXu a importujte tento soubor. Tento krok je potřeba pro každou šablonu opakovat.



Obr. 8.4: Nastavení importu šablon

Nyní vidíte všechny šablony v okně se seznamem šablon RipEXu mezi všemi ostatními šablonami, které jsou ve výchozím nastavení Zabbixu.

Poznámka

Pokud jste již dříve importovali šablonu, kterou je třeba aktualizovat, stačí naimportovat novější verzi šablony se stejným názvem a ta současná bude automaticky aktualizována.

Každá položka **Item** má své parametry, SNMP OID number, community string, UDP port (161), key, update interval a další. Jedním z klíčových parametrů je interval aktualizace (update interval), protože definuje, jak často bude Zabbix požadovat různé odpovědi ze stanic RipEX. Tento interval je předdefinovaný na 30 minut, ale měli byste zvážit jeho změnu tak, aby vyhovoval parametrům infrastruktury vaší rádiové sítě.

Jednotlivé položky mohou být v aktivním nebo neaktivním stavu. Ve výchozím nastavení jsou pouze některé položky aktivní pro jejich důležitost - další informace viz další kapitolu. Chcete-li sledovat více hodnot, aktivujte ty požadované. Ale jak již bylo dříve zmíněno, nejlépe pomocí ethernetového rozhraní RipEXu pro SNMP komunikaci, aby se zbytečně nezatěžoval rádiový kanál. Není-li to možné, zvažte, zda je sledování dalších hodnot nezbytné.

Sledujte pouze ty hodnoty, které opravdu potřebujete sledovat, a to s rozumnými intervaly aktualizace.

Položky jsou rozděleny podle užití do skupin nazývaných v Zabbixu **Aplikace**. Tyto aplikace slouží k lepšímu vysvětlení definovaných položek.

Pokud chcete dostávat upozornění, když se některá monitorovaná hodnota ocitne mimo rozsah svých mezí, můžete definovat **Trigger** pro jeho spuštění. Tato oznámení jsou zobrazitelná na hlavním panelu Zabbixu v položce historie. Můžete si také zapnout upozornění na e-mail, Jabber nebo SMS. Každé oznámení může nabývat jedné ze šesti předem definovaných úrovní závažnosti (varování, kritické, ...). V šablonách může být také definováno několik triggerů. Trigery definované v šablonách nejde indifviduálně měnit pro jednotlivé hosty (nemůžete tedy nastavovat různé mezní úrovně v rámci jedné šablony pro jednotlivá zařízení). Prosím, definujte individuálně triggery pro každý jednotlivý host (bez použití šablony).

Poznámka

Můžete využít možnosti vytváření klonů pro kopírování položek šablony nebo triggerů pro jednotlivé hosty. V takovém případě můžete upravit její předdefinované hodnoty, aby vyhovovala vašim požadavkům každého hosta zvlášť.

Grafy jsou automaticky generovány pro každou sledovanou číselnou hodnotu. Navíc můžete také vytvořit speciální grafy s několika hodnotami v jednom grafu. Nabízíme 5 předdefinovaných grafů, které obsahují několik základních sledovaných hodnot, jako např. teplota, napájecí napětí atd.

Další informace naleznete v dokumentaci Zabbix. Můžete odstranit, přidat nebo upravit jakoukoliv komponentu šablony. Předdefinovaný stav umožňuje rychlý start, ale nemusíte jej vůbec používat. Můžete si vytvořit vlastní sadu sledovaných hodnot a položek.

Jaké položky bych měl monitorovat?

Jednotlivé šablony jsou plně škálovatelné a skládají se z mnoha položek. Nicméně sledování všech položek není v běžné praxi nutné. Následující položky jsou standardně aktivované ve výchozí šabloně RipEXu:

- RipEX Template
  - Aktivní nastavená položka: 7
  - Výchozí čas aktualizace: 30 minut
    - Lokální jednotka:
      - Modem temperature (°C), RF power (W), TX lost (%), UCC (V), VSWR
    - Vzdálená jednotka:
      - DQ, RSS (dBm)

- RipEX – RFC1213 Template
  - Všechny položky jsou ve výchozím nastavení zakázány
- RipEX – RS232 Template
  - Všechny položky jsou ve výchozím nastavení zakázány
- RipEX – SNMP Trapper Template
  - Všechny SNMP Trap položky a triggery jsou ve výchozím nastavení povoleny s výjimkou DQ a RSS. Tyto triggery musí být pro všechny hosty klonovány, protože nemůžeme předdefinovat IP adresy vzdálených hostů.
- PING Template
  - Aktivní nastavená položka: 1
  - Výchozí čas aktualizace: 30 minut
  - Pouze aktivní položka kontroluje dosažitelnost hostu a v případě, že počítač není dosažitelný, spustí alarm.

Poznámka

Pokud potřebujete sledovat více než jednu vzdálenou stanici RipEX, budete muset "klonovat" existující položky pro sledované hodnoty vzdálené stanice.

Příklad konfigurace **druhé vzdálené stanice** (Data Quality item):

- Přejděte do okna **Template list window** a klikněte na položky z RipEX template.
- Najděte položku s názvem “Remote station 1 wv – Average DQ value” a klikněte na ni.
- Změňte parametr “Key” na hodnotu “2” v závorkách – wvRemDqAvg[2].
- Změňte poslední číslici v SNMP OID ne hodnotu "2" z hodnoty "1" (t.j. 1.3.6.1.4.1.33555.2.4.3.1.7.**2**).
- Klikněte na tlačítko “Clone”.
- Klikněte na tlačítko “Save”.
- Nyní stanice pomocí této šablony bude sledovat hodnoty DQ pro dvě vzdálené stanice.
- Chcete-li definovat tuto položku pouze pro jednu stanici RipEX, je nutné klonovat položku v seznamu "Item list" konfigurace **hostu**. Chcete-li povolit změny nastavení, musíte nejdříve kliknout na tlačítko "Clone"; software vám pak umožní změnit nastavení.

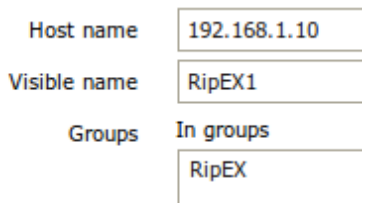
Celková použitá šířka pásma (žádosti, odpovědi) - v případě monitorování pouze hodnot definovaných výše:

- Asi 3 kB / stanici 1 RipEX / 1 hodinu

8.3.3. Jak importovat monitorované stanice RipEX?

Nyní máte funkční šablonu, ale je třeba definovat hosty (stanice RipEX). Každá stanice RipEX má svoji vlastní IP adresu. Následující kroky vás provedou konfigurací hostu.

Chcete-li vytvořit host, přejděte na **Configuration** → **Hosts** a klikněte na tlačítko **Create Host**. Definujte název hostu a jeho IP adresu.

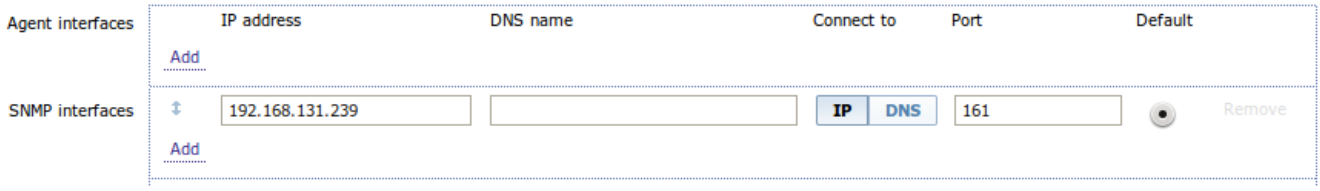


Obr. 8.5: Definování jména hosta a jeho IP adresy

Volitelně lze definovat skupinu (Group) pro hosty. Vytvoření skupiny je jednoduché. Můžete vytvořit novou **Group** při vytváření hostu, nebo to můžete udělat tak, že přejdete na kartu **Configuration** → **Groups** a kliknete na tlačítko **Create Group**.

Propojení šablony a hostu(ů) může být dosaženo ve stejném menu nebo můžete otevřít **Template settings** a propojit k ní libovolný host.

Musíte nastavit IP adresu a číslo portu pro rozhraní SNMP (port 161). V opačném případě nebudete moci používat žádnou položku SNMP.



Obr. 8.6: Definování rozhraní SNMP

Kde mohu vidět monitorované hodnoty RipEXu?

Pro kontrolu sledovaných hodnot přejděte na kartu **Monitoring** → **Latest data** a zvolte požadovaný host z nabídky.

LATEST DATA

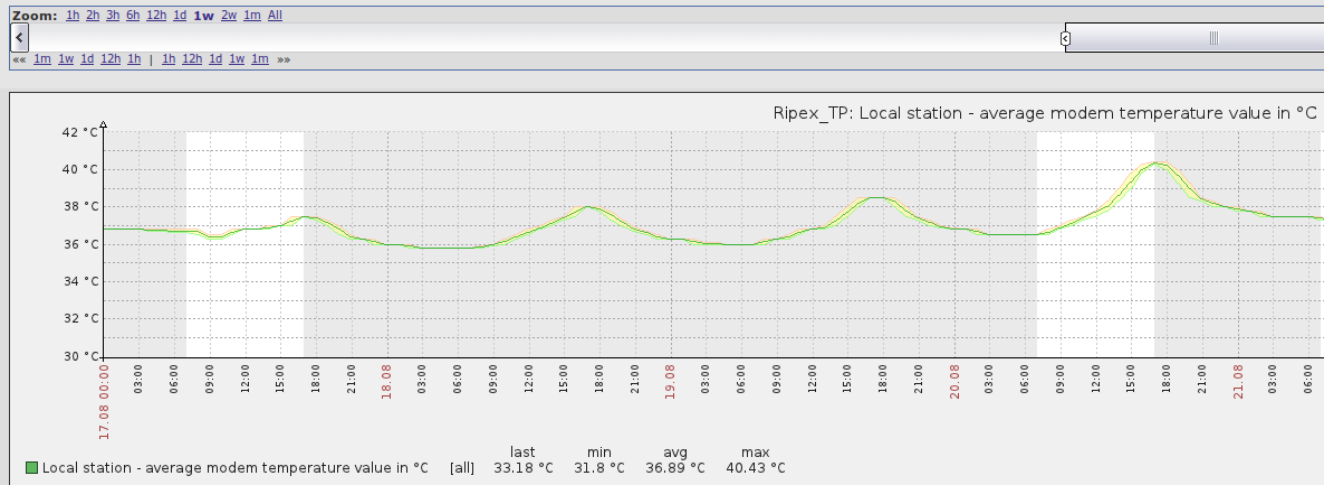
ITEMS — Group: Ripex — Host: Ripex_TP

Filter

Description	Last check	Last value	Change	History
COM ports (18 Items)				
Ethernet (5 Items)				
Local Station (11 Items)				
Station working mode	10 Sep 2012 10:46:34	router (2)	-	Graph
Station name	10 Sep 2012 10:46:57	RipexTP	-	History
SDDR firmware version	10 Sep 2012 10:47:25	0.16.0.37	-	History
Radio HW version	10 Sep 2012 10:46:42	1.1.50.7	-	History

Obr. 8.7: RipEX latest data

U každé položky můžete zobrazit graf nebo tabulku s její historií. Pokud je trigger nakonfigurován pro položku (Item), graf zobrazuje řádek s Treshohold value (mezní hodnotou).



Obr. 8.8: Graf RipEx

8.3.4. Hodnoty Mappings

Odpovědi některých OID jsou celá kladná čísla ale tyto hodnoty mají svůj speciální význam:

Příklad 8.1. deviceMode

- „1“ znamená **bridge** mód.
- „2“ znamená **router** mod.

Bohužel, ve výchozím nastavení můžete na webovém rozhraní Zabbix vidět pouze číselné hodnoty. Musíte vytvořit ručně **value mappings** pro všechny tyto objekty OID. Hodnota **value mapping** není exportována do šablony RipEX.

Vytvořte hodnoty **value mappings** ještě před importem šablony RipEX. V opačném případě budete muset propojit všechny hodnoty value mappings ručně s příslušnými položkami (items).

Nezapomeňte, že pro Zabbix od verze 2.2.1 je nutné vytvořit položky **value mappings** před importem šablony.

Poznámka

Tato syntaxe funkce je používána ve všech MIB tabulkách, nejen v tabulkách **RipEX MIB**.

Chcete-li přidat nové hodnoty *value mappings*, přejděte na Administration → General → Value Mapping. Klikněte na tlačítko **Create value map** a vložte hodnoty, které jsou uvedeny na následujících řádcích. Uvedený je seznam **Item list**, který využívá těchto **value mappings** (ať už jsou propojeny ručně nebo automaticky pomocí importu šablony).

Poznámka

Existuje také několik **value mappings** používaných v RFC1213 a RS232.

Value Mappings List / Seznam Value Mappings

RipEX.AlmState	**Items:**
-1 ⇒ unknown	Alarm state - COM1 interface Rx to Tx packets ratio

RipEX.AlmState	**Items:**
0 ⇒ inactive	Alarm state - COM2 interface Rx to Tx packets ratio
1 ⇒ active	Alarm state - Device temperature
	Alarm state - DQ
	Alarm state - ETH interface Rx to Tx packets ratio
	Alarm state - HW Input
	Alarm state - RF Power
	Alarm state - RSS
	Alarm state - Tx lost
	Alarm state - UCC
	Alarm state - Unit ready
	Alarm state - VSWR

RipEX.BackupPathsState	**Items:**
0 ⇒ unknown	Backup Paths 1 - Alternative Paths - Currently passive paths State
1 ⇒ up	Backup Paths 2 - Alternative Paths - Currently passive paths State
2 ⇒ down	Backup Paths 1 - Alternative Paths - Currently used path State
	Backup Paths 2 - Alternative Paths - Currently used path State

RipEX.comProtocol:	**Items:**
0 ⇒ none	COM1 - Protocol
3 ⇒ AsyncLink	COM2 - Protocol
4 ⇒ Modbus	TS 1 COM user protocol type
5 ⇒ IEC101	TS 2 COM user protocol type
6 ⇒ DNP3	TS 3 COM user protocol type
7 ⇒ UNI	TS 4 COM user protocol type
8 ⇒ Comli	TS 5 COM user protocol type
9 ⇒ DF1	
10 ⇒ Profibus	
12 ⇒ C24	
13 ⇒ RP570	
14 ⇒ Cactus	
15 ⇒ ITT Flygt	
16 ⇒ SLIP	
16 ⇒ Siemens 3964 (R)	

RipEX.deviceMode	**Items:**
1 ⇒ bridge	Station working mode

RipEX.deviceMode **Items:**

2 ⇒ router

RipEX.eDhcp **Items:**

0 ⇒ off Ethernet interface DHCP mode

1 ⇒ server

2 ⇒ client

RipEX.eSpeed **Items:**

0 ⇒ auto Ethernet interface bit rate and duplex settings

1 ⇒ s-100baseTX-Full

2 ⇒ s-100baseTX-Half

3 ⇒ s-10baseT-Full

4 ⇒ s-10baseT-Half

RipEX.ifTmATM **Items:**

0 ⇒ mask TCP Modbus COM protocol address translation mode

1 ⇒ table

RipEX.IOState **Items:**

-1 ⇒ unknown HW alarm input contact state

0 ⇒ off

1 ⇒ on

RipEX.RelayContactType **Items:**

0 ⇒ off HW alarm input contact type

1 ⇒ normally-closed

2 ⇒ normally-open

RipEX.rEncryption **Items:**

0 ⇒ off Radio interface encryption method

1 ⇒ aes256

RipEX.rRfPwr **Items:**

0 ⇒ mE-100mW Radio interface RF power

1 ⇒ mEr-200mW

2 ⇒ mE-500mW

3 ⇒ mE-1W

4 ⇒ mE-2W

5 ⇒ mE-3W

6 ⇒ mE-4W

7 ⇒ mE-5W

8 ⇒ mE-10W

RipEX.rRfPwr	**Items:**
9 ⇒ mE-8W	
17 ⇒ mL-200W	
18 ⇒ mL-500mW	
19 ⇒ mL-1W	
20 ⇒ mL-2W	

RipEX.SettingState	**Items:**
0 ⇒ off	Ethernet interface broadcast and multicast status
1 ⇒ on	Ethernet interface shaping status
	Terminal server status
	TCP Modbus COM protocol broadcast accept
	Radio interface FEC
	TS 1 on/off
	TS 2 on/off
	TS 3 on/off
	TS 4 on/off
	TS 5 on/off

RipEX.tsEthProtType	**Items:**
0 ⇒ tcp	TS 1 Ethernet protocol type
1 ⇒ udp	TS 2 Ethernet protocol type
	TS 3 Ethernet protocol type
	TS 4 Ethernet protocol type
	TS 5 Ethernet protocol type

RFC1213.ifType	**Items:**
1 ⇒ other	RFC1213 - Interface 1 - The type of interface (physical/link protocol)
2 ⇒ regular1822	RFC1213 - Interface 2 - The type of interface (physical/link protocol)
3 ⇒ hdh1822	
4 ⇒ ddn-x25	
5 ⇒ rfc877-x25	
6 ⇒ ethernet-csmacd	
7 ⇒ iso88023-csmacd	
8 ⇒ iso88024-tokenBus	
9 ⇒ iso88025-tokenRing	
10 ⇒ iso88026-man	
11 ⇒ starLan	
12 ⇒ proteon-10Mbit	
13 ⇒ proteon-80Mbit	

RFC1213.ifType	**Items:**
14 ⇒ hyperchannel	
15 ⇒ fddi	
16 ⇒ lapb	
17 ⇒ sdlc	
18 ⇒ ds1	
19 ⇒ e1	
20 ⇒ basicISDN	
21 ⇒ primaryISDN	
22 ⇒ propPointToPointSerial	
23 ⇒ ppp	
24 ⇒ softwareLoopback	
25 ⇒ eon	
26 ⇒ ethernet-3Mbit	
27 ⇒ nsip	
28 ⇒ slip	
29 ⇒ ultra	
30 ⇒ ds3	
31 ⇒ sip	
32 ⇒ frame-relay	

RFC1213.ipForwarding	**Items:**
1 ⇒ forwarding	RFC1213 - The indication of whether this entity is acting as an IP gateway
2 ⇒ not-forwarding	

RFC1213.snmpEnableAuthenTraps	**Items:**
1 ⇒ enabled	RFC1213 - SNMP - Indicates whether the SNMP agent process is permitted to generate authentication-failure traps
2 ⇒ disabled	

RS232.rs232AsyncPortParity	**Items:**
1 ⇒ none	RS232 port 1 - The port's sense of a character parity bit
2 ⇒ odd	RS232 port 2 - The port's sense of a character parity bit
3 ⇒ even	
4 ⇒ mark	
5 ⇒ space	

RS232.rs232AsyncPortStopBits	**Items:**
1 ⇒ one	RS232 port 1 - The port's number of stop bits
2 ⇒ two	RS232 port 2 - The port's number of stop bits
3 ⇒ oneAndHalf	

RS232.rs232AsyncPortStopBits	**Items:**
4 ⇒ dynamic	

RS232.rs232PortInFlowType	**Items:**
1 ⇒ none	RS232 port 1 - The port's type of input flow control
2 ⇒ ctsRts	RS232 port 2 - The port's type of input flow control
3 ⇒ dsrDtr	RS232 port 1 - The port's type of output flow control
	RS232 port 2 - The port's type of output flow control

RS232.rs232PortType	**Items:**
1 ⇒ other	RS232 port 1 - The port's hardware type
2 ⇒ rs232	RS232 port 2 - The port's hardware type
3 ⇒ rs422	
4 ⇒ rs423	
5 ⇒ v35	
6 ⇒ x21	

ICMP ping - Accessibility	**Items:**
0 ⇒ ICMP ping fails	ICMP ping - Accessibility
1 ⇒ ICMP ping successful	

Poznámka

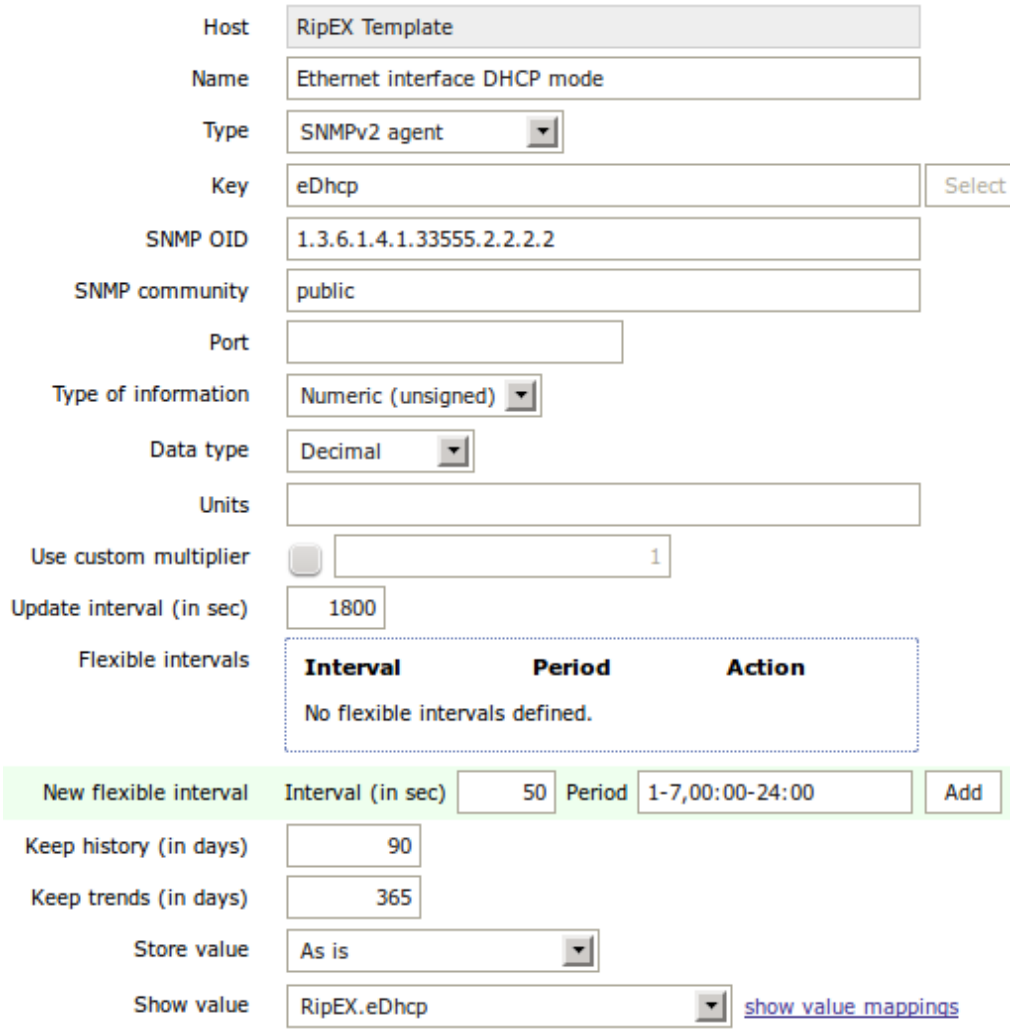
Dvě hodnoty **value mappings** by měly být zahrnuty již v samotném monitorovacím sw Zabbix, viz část "stav SNMP rozhraní (ifAdminStatus)" a "stav SNMP rozhraní (ifOperStatus)" v menu Value mapping. Čtyři položky ze šablony RFC1213 používají toto mapování.

Jak mohu změnit položku Item na odkaz s Value Map?

Přejděte na **Configuration** → **Templates** a zvolte jednu z importovaných šablon. Otevřete okno konfigurace položky a klikněte na vybranou položku pro prohlížení a upravení jejího nastavení.

Vyberte příslušnou hodnotu **value map** v menu **Show value** a uložte změny.

Příklad: RipEX.eDhpc

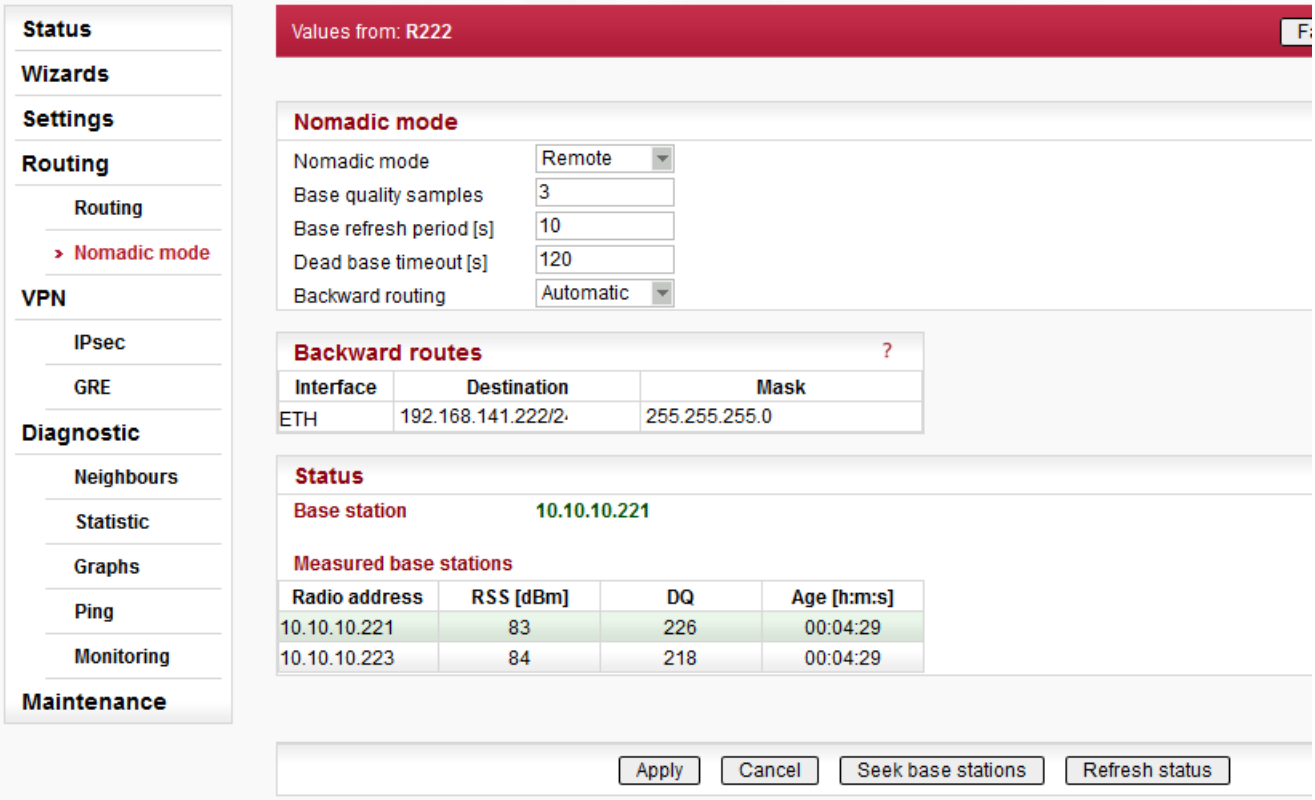


Obr. 8.9: Propojení Value map a položky Item

8.4. Tabulka RipEX MIB

Tabulku MIB pro RipEX najdete v dokumentu Application notes na odkazu *http://www.racom.eu/eng/products/m/ripex/app/snmp/MIB.html*, nebo na webu Racom na odkazu *http://www.racom.eu/download/hw/ripex/free/eng/3_fw/RACOM-RipEX-MIB.zip*.

9. Nomadický mód



Obr. 9.1: Menu Nomadický mód

9.1. Základní popis

Nomadický mód je metoda výstavby sítě, která nabízí snadné přidání nové vzdálené (remote) stanice k rádiové síti nebo jednoduché přemístění vzdálených (remote) stanic mezi různými Nomadickými bázemi. Přepínání mezi Nomadickými bázemi není rychlý proces, trvá v řádu minut.

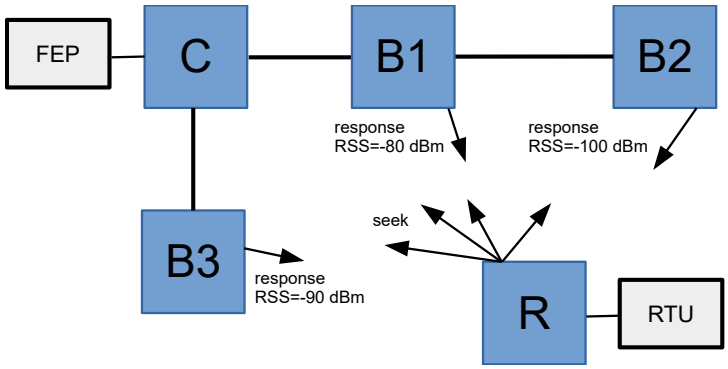
Nomadický mód je dostupný pouze v Router módu, který je součástí Flexibilního rádiového protokolu.

Jsou tři druhy stanic v síti Nomadického módu:

- Centrum: V Nomadické síti může být pouze jedna centrální stanice. Veškerá komunikace s Remote musí Centrem procházet. Centrum se chová i jako Báze.
- Báze: Stanice ke které se Remote připojuje
- Remote: Připojena jedním rádiovým skokem k Bázi.. Nomadický mód vytváří nomadické tunely mezi Remote jednotkami a Centrem, těmito tunely prochází veškerý uživatelský provoz.

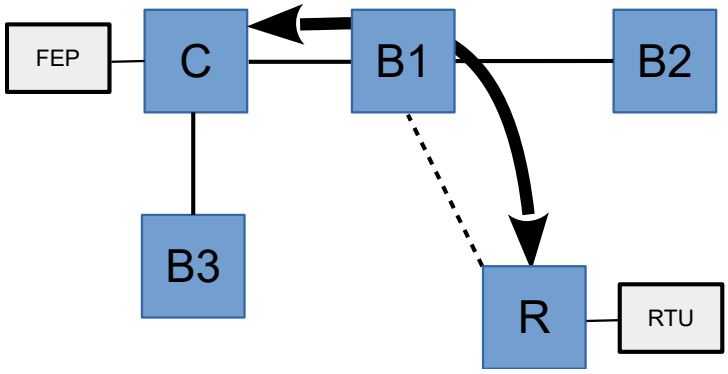
Všechny obrázky níže reprezentují zjednodušené příklady Nomadické sítě, jsou použity následující zkratky:

- C - Centrum
- B - Báze
- R - Remote
- FEP - Front End Processor - aplikační centrum pro uživatelská data
- RTU - Remote Terminal Unit - aplikační koncový bod



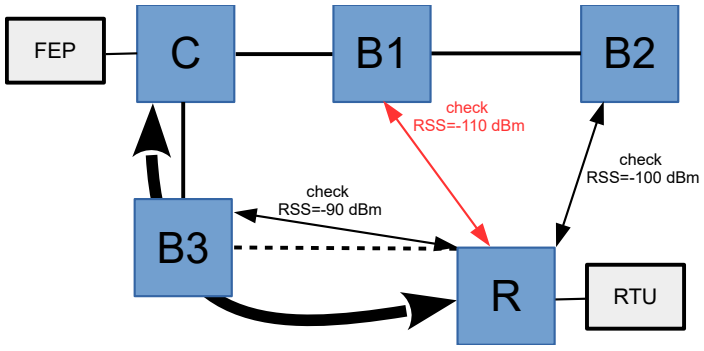
Obr. 9.2: Ustanovení spojení

- Remote stanice vysílá "seek" paket - Báze v rádiovém pokrytí odpovídají
- Spojení je automaticky ustanoveno přes Bázi s nejsilnějším signálem
- Pravidla routování do a z Remote do Centra jsou vytvořena automaticky
- K jedné Bázi může byt připojeno maximálně 64 Remote stanic.
- Pokud není spojení mezi Bází a Centrem, Remote stanice spojené s Bází automaticky spustí nové vyhledávání Báze.



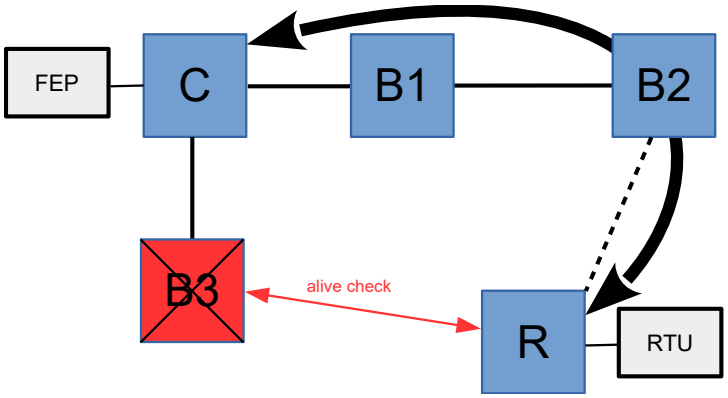
Obr. 9.3: Připojený Remote

Remote stanice je připojená k Bází s nejlepší signálem. Uživatelský provoz z RTU je přesměrován do nomadického tunelu a předán do FEP, to platí I pro opačný směr.



Obr. 9.4: Periodická kontrola nejlepší báze

- V nastaveném intervalu se kontroluje, která Báze poskytuje nejsilnější signál.
- Aby došlo ke změně Báze, musí být signál musí být silnější než 5 dBm.



Obr. 9.5: Periodická kontrola neaktivní Báze

Báze pravidelně kontroluje své spojení s Centrem. Pokud spojení není, informuje Remote stanice a ty se přepojí k jiné Bázi s nejsilnějším signálem.

9.2. Konfigurace

- **Nomadic mode**
  List box: Off, Remote, Base, Center
  Default = Off
  Výběr funkce jednotky v Nomadickém módu

Centrum - Konfigurace

- **Base stations**
  - Všechny bázové stanice v síti jsou zobrazeny v této tabulce
  - Maximální počet aktivních Bází je 256
  - Stejná IP adresa nesmí být použita více než jednou.
  - Záznamy z tabulky " Unknown Base stations" (Neznámé Báze) mohou být přesunuty jako nové Báze do tabulky “Base stations”.

- **IP address**
  Default = 0.0.0.0

  IP adresa Báze. Může být použita buď primární ETH adresa nebo rádiová IP adresa. Typ použité IP adresy (Eth nebo radio) musí odpovídat IP adrese použité v nastavení Báze.

- **Active**

  Zaškrkněte políčko pro aktivaci/deativaci pravidla

- **Note**
  Můžete přidat poznámku o délce až 16 znaků (UTF8). Následující znaky nejsou povoleny:
  " (dvojitá uvozovka)
  ` (akcent)
  \ (zpětné lomítko)
  $ (dolar)
  ; (středník)

- **Modify**

Tlačítka “Delete” a “Add” umožňují odebírat a přidávat záznamy (posunování mezi záznamy šipkami nahoru a dolů).

Báze - Konfigurace

- **IP address of the Center**
  Default = 0.0.0.0
  Může být použita rádiová nebo ETH adresa, stejný typ adresy musí být použit i při konfiguraci Centra (v tabulce "Base stations").

- **Báze - Pokročilá konfigurace**

  Center refresh period [s]
  Default = 300 s [1 - 86400]
  Obnovovací perioda spojení s Centrem.

Remote - Konfigurace

- **Backward routing**
  List box: Manual, Automatic
  Default: Automatic
  Metoda, jak jsou vytvářena pravidla zpětného routování
  - Automatic: Je použit rozsah primární ETH addresy. Pokud je na COM1 a/nebo COM2 použit SLIP protokol, je přidán i tento rozsah IP adres.
  - Manual: Pravidla se zadají do tabulky "Backward routes".

- **Backward routes**
  Routovací pravidla pro routování veškerého provozu z Centra do Remote prostřednictvím nomadického tunelu.
  Pravidla jsou přenesena do Centra po registraci Remote. Počet pravidel je omezen na 8. Stejná IP adresa smí být v rámci celé sítě požita jen jednou.

- **Destination**
  Default = 0.0.0.0/0
  Destination IP adresa. Pakety odpovídající této adrese/masce budou poslány do Remote.

  POZNÁMKA: Jak ETH, tak i rádiová adresa může být použita pro přístup k COM1 a COM2 při použití SCADA púrotokolů (Modbus, DNP3 apod.). Defaultní ETH adresa může být použita.

- **Mask**
  Default = 0.0.0.0
  Maska destinace IP adresy

- **Active**
  Zaškrkněte políčko pro aktivaci/deativaci pravidla

- **Note**
  Y Můžete přidat poznámku o délce až 16 znaků (UTF8). Následující znaky nejsou povoleny:
  " (dvojitá uvozovka)
  ` (akcent)
  \ (zpětné lomítko)
  $ (dolar)
  ; (středník)

■ **Forward rules**
Nakonfigurované v tabulce “Routing – Routes”.
Pravidla routování provozu z Remote do Centra
Parametr "Mode" každého pravidla “Routing – Routes” musí být nastavený na "Nomadic", aby se vytvořil nomadický tunel.
Pravidlo "Default GW" musí být nakonfigurováno také. Pokud je RTU jednotka napojena přímo do Ethernet portu, není třeba dalších routovacích pravidel.

■ **Remote - Pokročilá konfigurace**

Base quality samples
Default = 3 [3 - 8]
Počet paketů použitých k určení kvality signálu mezi Remote a Bází. Vyšší číslo znamená delší proces, ale lépe změřenou kvalitu signálu. Přenos uživatelských dat může být ovlivněn tímto procesem..

Base refresh period [s]
Default = 3600 s [10 - 86400]
Perioda obnovování registrace Remote k Bázi. Při tomto procesu mohou být ovlivněna uživatelská data.

Dead Base timeout [s]
Default = 120 s [5 - 120]
Používá se k nastavení periody ověření dostupnosti Báze. Pokut neprobíhá žádný jiný provoz, je po tomto intervalu poslán servisní paket. Pokud Báze nereaguje, spustí se nový proces vyhledávání Báze.

9.3. Diagnostika Nomadického módu

Remote stanice jsou přístupné přes “Fast remote access” při použití stejné adresy jako byly nakonfigurovány v jejich zpěných routovacích tabulkách. Nomadický protokol používá UDP datagramy s defaultním portem 8905.

Centrum - Status

■ **Base stations**
Seznam nakonfigurovaných Bází dává následující stavové informace:
- Báze připojené k Centru jsou označeny zeleně
- Báze nepřipojené k Centru jsou označeny červeně

■ **Unknown Base stations (Neznámé Bázové stanice)**
Poskytuje seznam Bází, které jsou nakonfigurovány jako nomadické Báze, ale nejsou přidány do seznamu Bází (“Base stations” v Centru.

■ **Remotes**
Jsou uvedeny všechny Remote stanice připojené k síti s uvedením následujících informací:
- Rádiová a ETH adresa Remote
- Výrobní číslo Remote
- Adresa Báze, ke které je Remote jednotka připojena. Pokud je připojena přímo k Centru, pak je "Centrum" umístěno v seznamu místo IP adresy.
- Doba od poslední registrace
- Záznam Remote stanice je označen červeně pokud je IP adresa Remote duplicitní.
- Tabulka zpětného routingu

Záznam zpětného routingu není zvýrazněm, pokud je pravidlo akceptováno.
Záznam zpětného routingu je označen světle zeleně pokud je v kolizi, ale pravidlo je použito
Záznam zpětného routingu je označen červeně pokud je v kolizi a pravidlo nebylo akceptováno

■ **Locally connected Remotes**
V tomto seznamu jsou zobrazeny Remote jednotky připojené přímo k Centru s následujícími detaily:
- Rádiová adresa Remote jednotky
- Výrobní číslo Remote jednotky
- Doba od posledního obnovení

■ **Změřené Remote stanice (lokální)**
Tato tabulka poskytuje výsledky měření kvality signálu měřenou mezi Remote a Centrem. Úroveň je měřena když Remote vybírá Bázi s nejlepším signálem.
- Rádiová adresa Remote jednotky
- RSS a DQ měření
- Doba od posledního měření
- Remote jednotky připojené k Centru jsou označeny zeleně

Báze - Status

■ **Spojení s Centrem**
Status zobrazuje, je-li je Báze spojena s Centrem.

■ **Connected Remotes**
Remote stanice připojené k Bázi jsou uvedeny v seznamu s následujícími podrobnostmi:
- Rádiová adresa Remote jednotky
- Výrobní číslo Remote jednotky
- Doba od posledního obnovení.

■ **Measured Remotes**
Tato tabulka poskytuje výsledky měření kvality signálu mezi Remote a Bázemi. Signál je změřen, když Remote stanice vyhledává Bázi s nejlepším signálem.
- Rádiová adresa Remote jednotky
- Měření RSS a DQ
- Doba od posledního měření.
- Připojené Remote stanice jsou vyznačeny zeleně

Remote - Status

■ **Base station Bázová stanice** - IP adresa Báze, ke které je připojena Remote stanice.

■ **Measured Base stations Změřené Bázové stanice**
Tato tabulka poskytuje výsledky měření kvality signálu mezi Remote jednotkou a Bázemi v rádiovém pokrytí. Signál je měřen, když Remote kontroluje Bázi s nejlepším signálem.
- Rádiová adresa Remote jednotky
- Měření RSS a DQ
- Doba od posledního měření
- Aktivní Báze jsou vyznačeny zeleně
- Bázové stanice, které odmítly spojení, jsou vyznačeny červeně

■ **Advanced - Monitoring Pokročilý Monitoring**
- Pro Nomadický mód není specifický monitoring
- Pakety protokolu Nomadického módu mohou být monitorovány na "RADIOVÉM" rozhraní jako UDP rámce s portem 8905

- Nomadický tunel muže být monitorován na "ETH" rozhraní v Centru nebo v Remote jednotce. Uživatelské pravidlo musí být nastaveno jako "-i nomad"

9.4. Nomadický mód a jeho vztahy k dalším RipEX službám

- Pakety vycházející z jednotky do Nomadického tunelu používají jako zdrojovou (source) adresu primární ETH adresu.
- Komunikace mezi rozdílnými Remote stanicemi je možná, ale musí být směrována přes Centrum.
- Komunikace mezi Remote a statickou síťovou stanicí je také možná, ale musí být také směrována přes Centrum

Firewall
- Firewall nejde použít k filtrování paketů mezi Centrem a Remote stanicemi směřující Nomadickým tunelem.
- Pro pravidla založená na rozhraní ("Input device", "Output device"). Je-li použita volba "Radio", může být Nomadický tunel ovlivněn.

Optimization (Optimalizace)
- Optimalizace může být použita jen pro uživatelským a management provoz mezi Remote a Centrem
- Provoz z Remote do jiné jednotky přes Centrum nelze optimalizovat

Proxy ARP
- Proxy ARP funguje správně pro adresu za nomadickým spojením

Terminal servers
- Terminal servery mohou komunikovat přes Nomadický tunel

TCP Proxy
- TCP Proxy může být použito přes Nomadický tunel

IPsec
- IPsec tunel může být uzavřen přes Nomadický tunel (např. mezi Remote stanicí a Centrem)
- Nomadické spojení mezi Centrem a Bází může být uzavřeno přes IPsec tunel.

GRE
- GRE tunel může být použit přes Nomadický tunel
- GRE tunel může být použit pro spojení mezi Centrem a Bází.

Backup routes
- Je možné vytvořit záložní trasu s jednou alternativní cestou za použití Nomadického tunelu. Gateway adresa musí být nastavena na "127.1.1.1". Pravidla záložní trasy v Centru musí být přidána do seznamu zpětných pravidel v Remote jednotce. Tento scénář může být použit k zálohování nomadického rádiového spojení pomocí mobilní sítě.
- Spojení mezi Centrem a Bází lze zálohovat pomocí záložních tras.

HotStandby
- Remote, Bázové a Centrální stanice mohou operovat v Hot-Stand-by konfiguraci.
- Pokud je jednotka hot-swapped, může být ohlášena v Centru jako duplikát. Po nějakém čase zpráva zmizí.

9.5. Tlačítka

Apply - potvrdí a uloží změny

Cancel - obnoví původní hodnoty
Seek Base stations - Remote jednotka – spustí nové vyhledávání Báze
Refresh status - Obnoví všechny Status informace

9.6. Běžné případy použití

Dočasně umístěný RipEX

Při instalaci RipEX jednotky mohou nastat požadavky dočasně někam umístit jednotku a po čase ji přemístit na jinou lokaci. Při použití Nomadického Módu a jednotkou RipEX nastavenou jako Remote, není v takovém případě třeba měnit nastavení. Jednotka se znova zaregistruje k páteřní síti a začne pracovat správně.

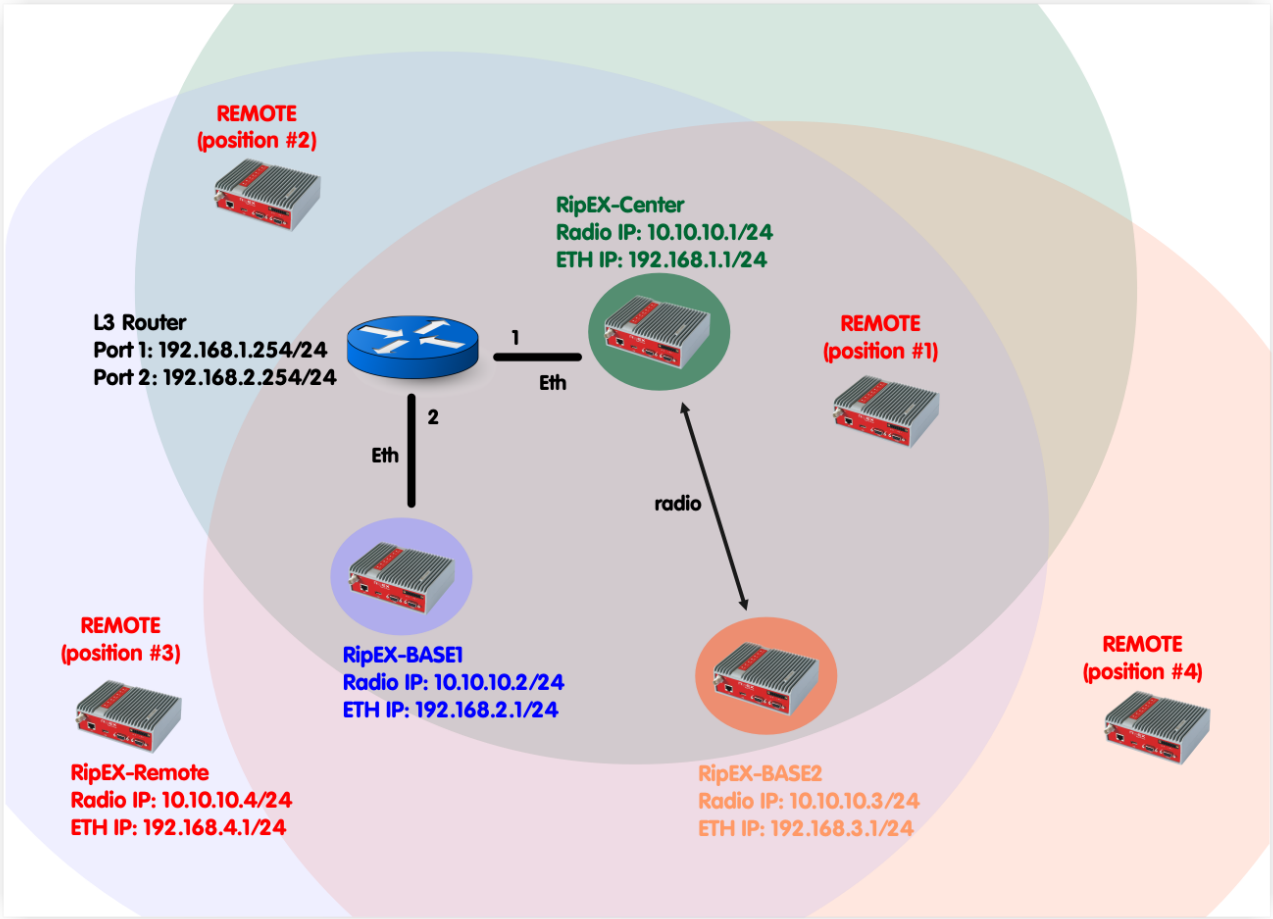
Měřící jednotka

Nomadický mód může být využit pro průzkum sítě. Technik může naistalovat vzdálenou (remote) jednotku v dané lokaci a zařízení automaticky vyhledá nejlepší připojovací bod (nejlepší RipEX bázovou stanici). Po tomto kroku muže být jednotka překonfigurována na statickou. Je doporučeno překonfigurovat jednotku z Nomadického módu na statické řešení kvůli vyšší režii v Nomadickém módu. Pokud jednotku nebudete přemísťovat na jinou lokaci, nenechávejte ji v Nomadickém módu.

“Mobilní použití”

Nomadický mód NENÍ mobilní mód. Není určený k používání jako mobilní síť, ale s jistými omezeními, může takto pracovat. Statická páteř RipEX jednotek s jednou centrální jednotkou a několika Bázovými stanicemi vytvoří základ sítě. V síti můžou pracovat statické vzdálené (remote) jednotky.

9.7. Příklad konfigurace

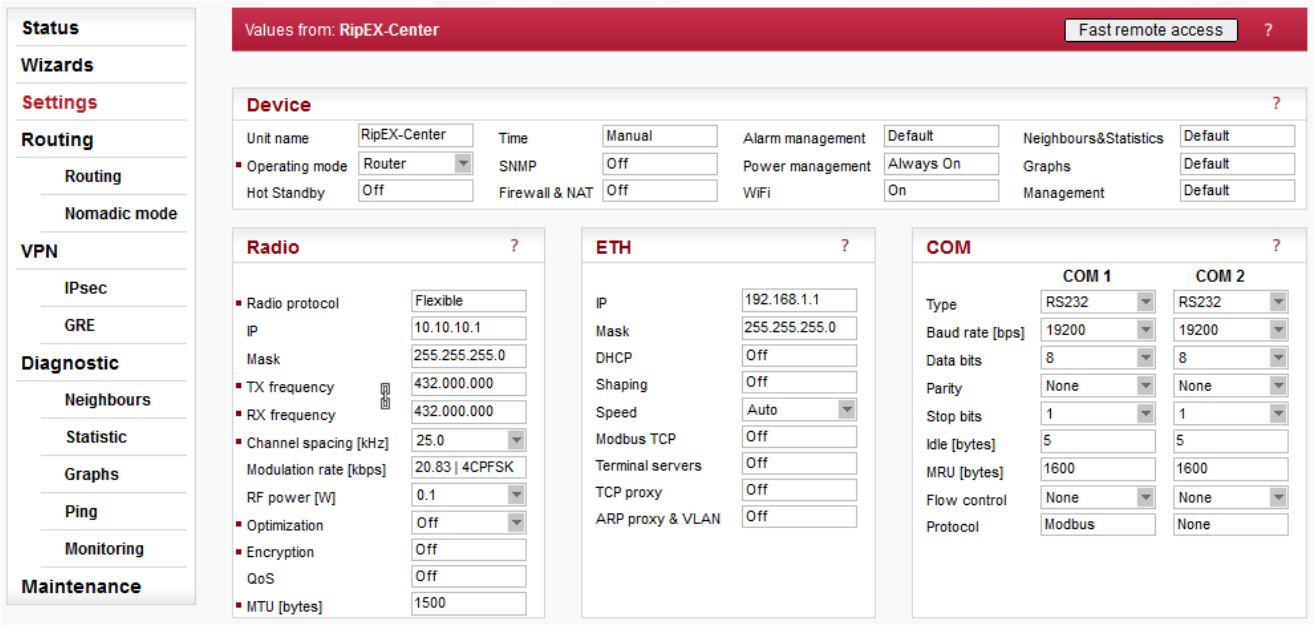


Obr. 9.6: Příklad topologie Nomadického módu

V tomto případě jsou použity 4 RipEX jednotky- RipEX-Center slouží jako centrum Nomadického módu. Dvě jednotky slouží jako báze (RipEX-Base1 a RipEX-Base2)- Čtvrtá jednotka se nazývá RipEX-Remote a slouží jako vzdálená (remote) jednotka. Tato jednotka může být umístěna kdekoli v rádiovém pokrytí alespoň jedné RipEX báze (Center taky operuje jako Báze) a dynamicky navazuje spojení s nejlépe dostupnou Bází. Není třeba překonfigurovávat vzdálenou (remote) jednotku. Nomadický mód zvládne spojení samostatně.

V následující kapitole bude vysvětlena a ukázána individuální konfigurace RipEX jednotek společně s dynamickým routingem. Nezáleží, kde je vzdálená (remote) RipEX jednotka umístěna. Vždycky může komunikovat s ostatními jednotkami v síti.

9.7.1. RipEX-Center Konfigurace

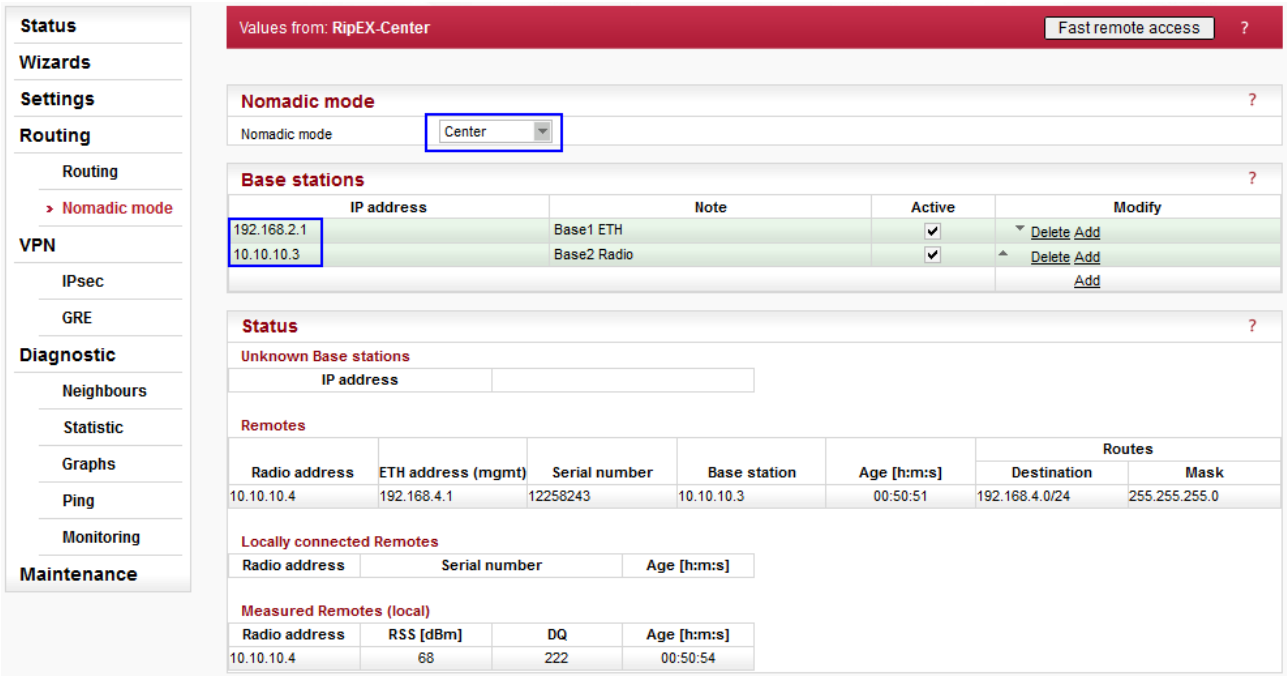


Obr. 9.7: Menu settings-Centrum

Parametry:

Unit name	RipEX-Center
Operating mode	Router
Radio protocol	Flexibilní (Nomadický mód je podporován pouze ve Flexibilním protokolu)
Radio IP/Mask	10.10.10.1/255.255.255.0
Frequency	432.000.000 MHz (nastavte stejnou frekvenci pro celou síť – frekvence mohou být jak simplexní, tak i duplexní)
Channel spacing	25 kHz (nastavte stejnou šířku kanálu pro celou síť)
Modulation rate	20.83 | 4CPFSK (použijte stejný typ modulace pro všechny jednotky, ale hondotu zvolte podle potřeby)
RF power	0.1 W (nastavte minimální možný RF výkon pro test použitím fiktivních záteží na vašem stole - laboratorní testy)
ETH IP/Mask	192.168.1.1/255.255.255.0

Žádná speciální konfigurace není ve Flexibilním Router módu požadována.



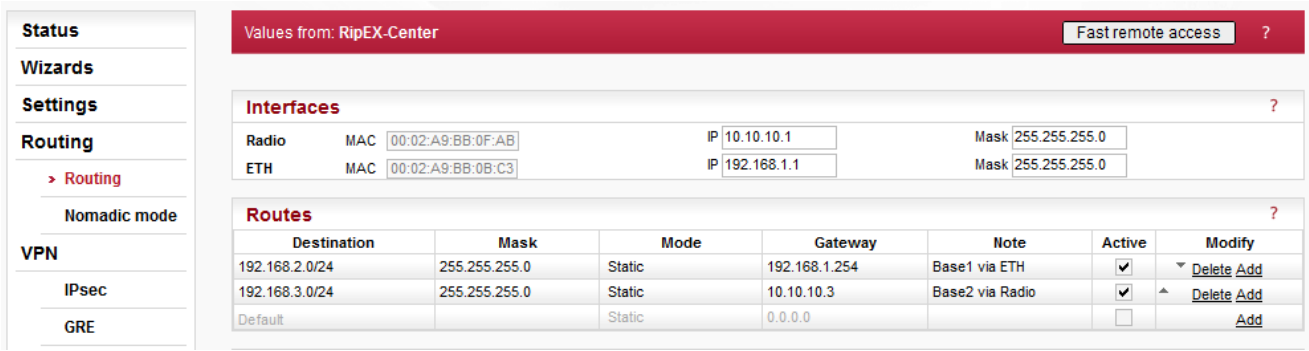
Obr. 9.8: Menu Nomadic Mode - Centrum

Parametry:

Nomadic mode	Center (Centrum)
Base stations (Bázové stanice/Báze)	192.168.2.1, Base1 ETH, Active 10.10.10.3, Base2 Radio, Active

V radiové síti RipEX může být nejvýše jedno Nomadické centrum. To komunikuje a řídí funkci Nomadického módu, v tomto příkladu společně s dvěma Bázemi. Jedna Báze je připojena Ethernetem and druhá rádiovým kanálem. Centrum se také chová jako Báze.

Jakmile se Centrum sesynchronizuje s Bázemi a Remote (vzdálenou jednotkou), jejich status se zobrazí (např. informace o připojené Bázi a Remote (vzdálených jednotkách).



Obr. 9.9: Menu Routing - Centrum

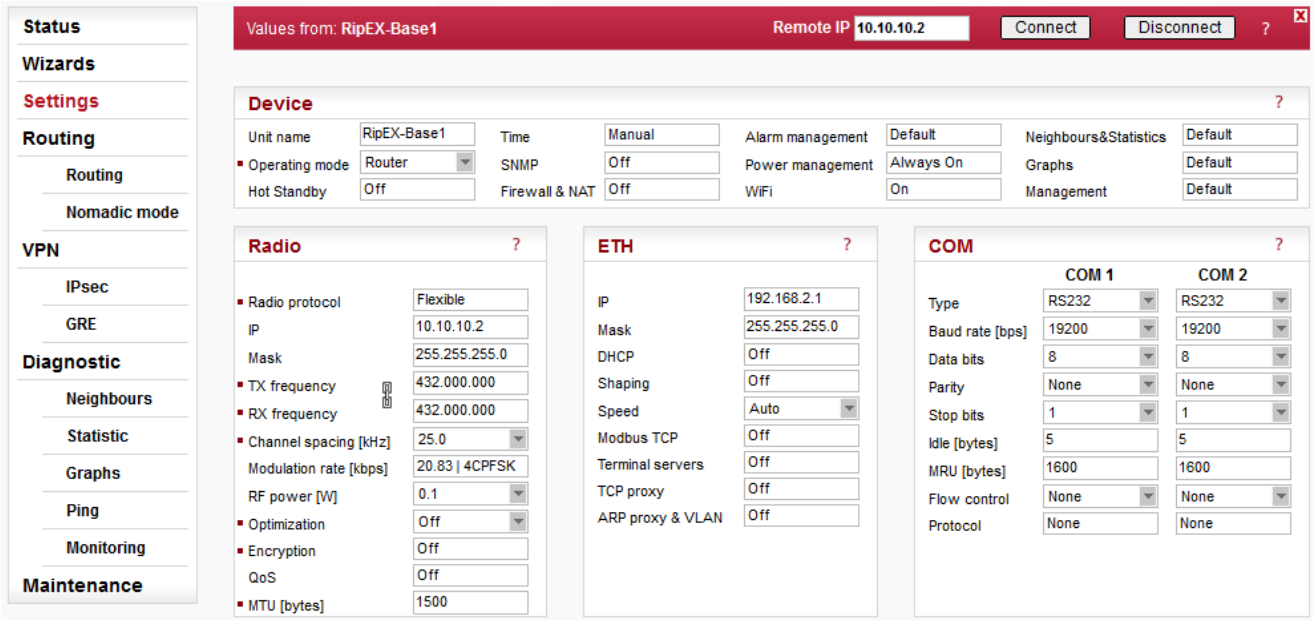
V tomto příkladu jsou nastaveny dva routery.

- 192.168.2.0/24 via 192.168.1.254, Mode: static
- 192.168.3.0/24 via 10.10.10.3, Mode: static

- 192.168.2.0/24 via 192.168.1.254, Mód: statický
- 192.168.3.0/24 via 10.10.10.3, Mód: statický

Kvůli přístupnosti sítí Bází jsou potřebné obě cesty. Síť Remote jednotek není konfigurována, protože je tvořena dynamicky podle místa Remote jednotky. Tento routing je zobrazen v menu Nomadický mód.

9.7.2. RipEX-Base1 Konfigurace



Obr. 9.10: Menu Settings - Base1

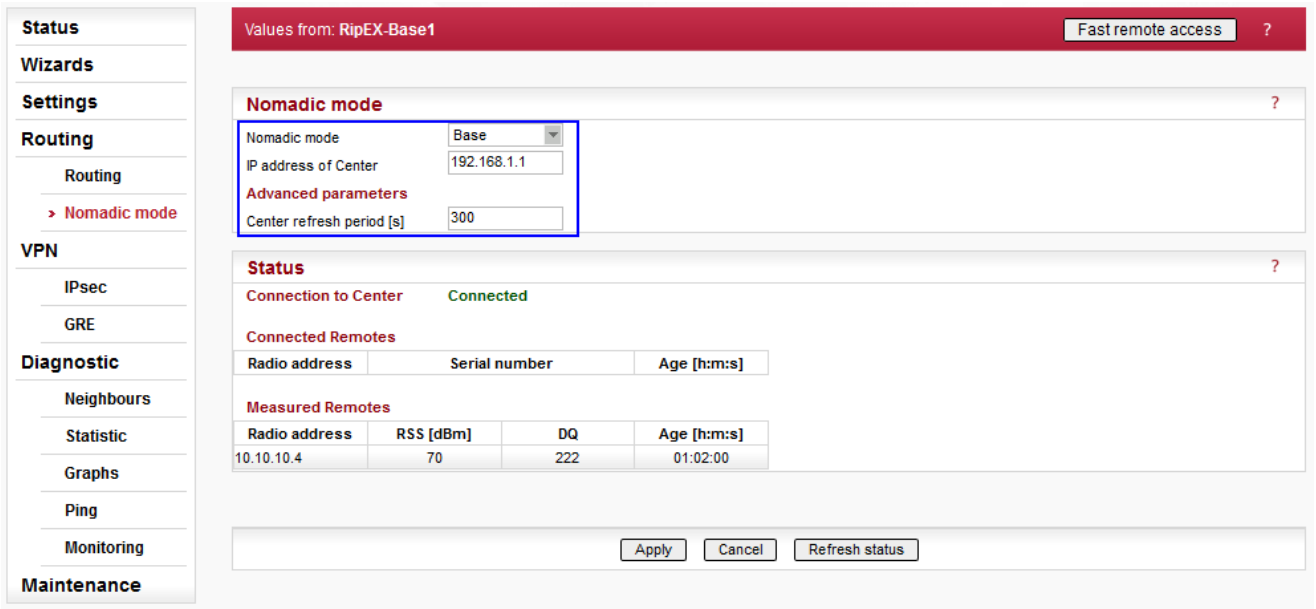
Níže jsou vysvětleny pouze rozdílné parametry v porovnání s Centrem.

Parametry:

Unit name RipEX-Base1

Radio IP/Mask 10.10.10.2/255.255.255.0

ETH IP/Mask 192.168.2.1/255.255.255.0



Obr. 9.11: Menu Nomadic mode - Base1

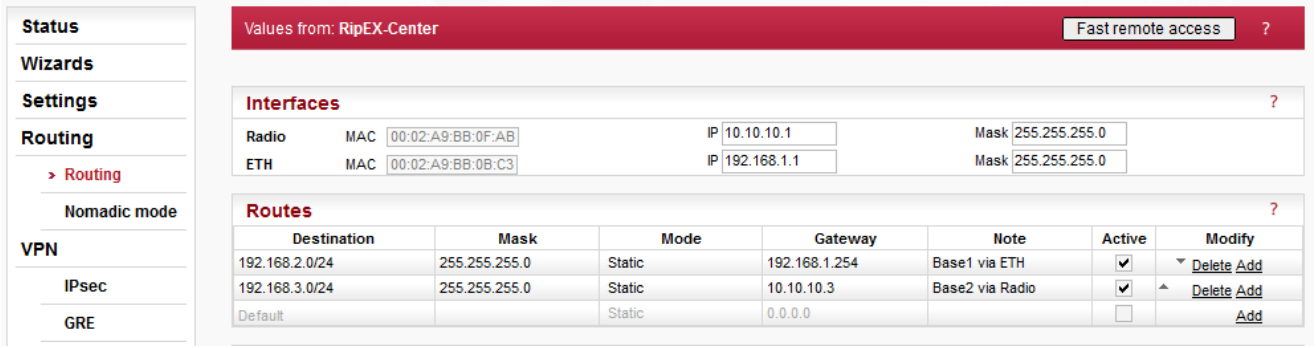
Parametry:

Nomadic mode Base

IP address of Center 192.168.1.1 (RipEX-Center Ethernet IP address – komunikace probíhá přes Ethernet)

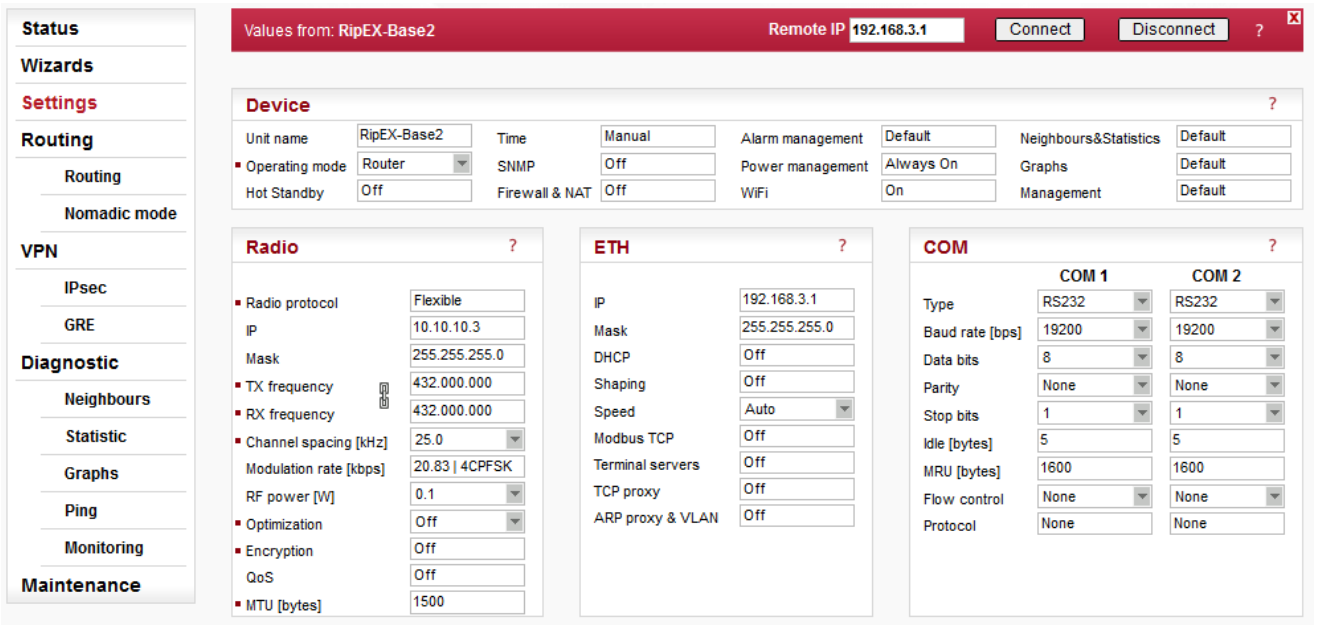
Pokročilé parametry:

Center refresh period [s] 300



Obr. 9.12: Menu Routing - Base1

9.7.3. RipEX-Base2 Konfigurace



Obr. 9.13: Menu Settings - Base2

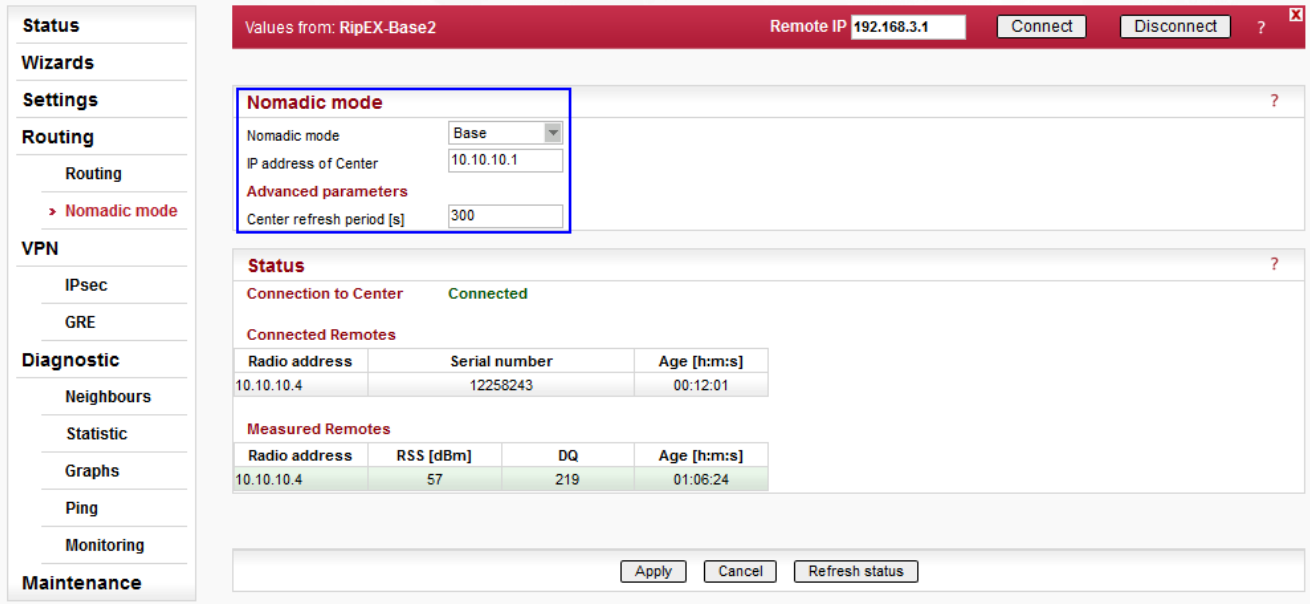
Níže jsou vysvětleny pouze rozdílné parametry v porovnání s Centrem.

Parametry:

Unit name RipEX-Base2

Radio IP/Mask 10.10.10.3/255.255.255.0

ETH IP/Mask 192.168.3.1/255.255.255.0



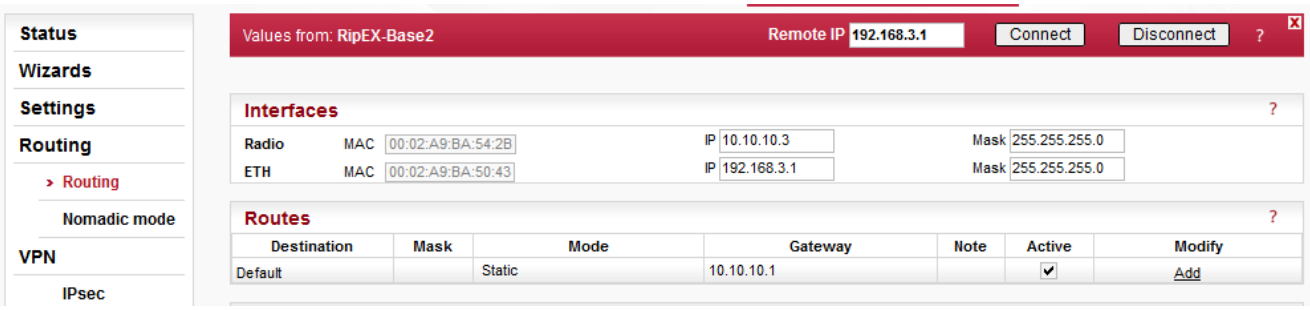
Obr. 9.14: RipEX-Base2 Nomadic mode

Parametry:

Nomadic mode	Base (Báze)
IP address of Center	10.10.10.1 (RipEX-Center Radio IP address – komunikace probíhá přes rádiový kanál)

Advanced parameters:

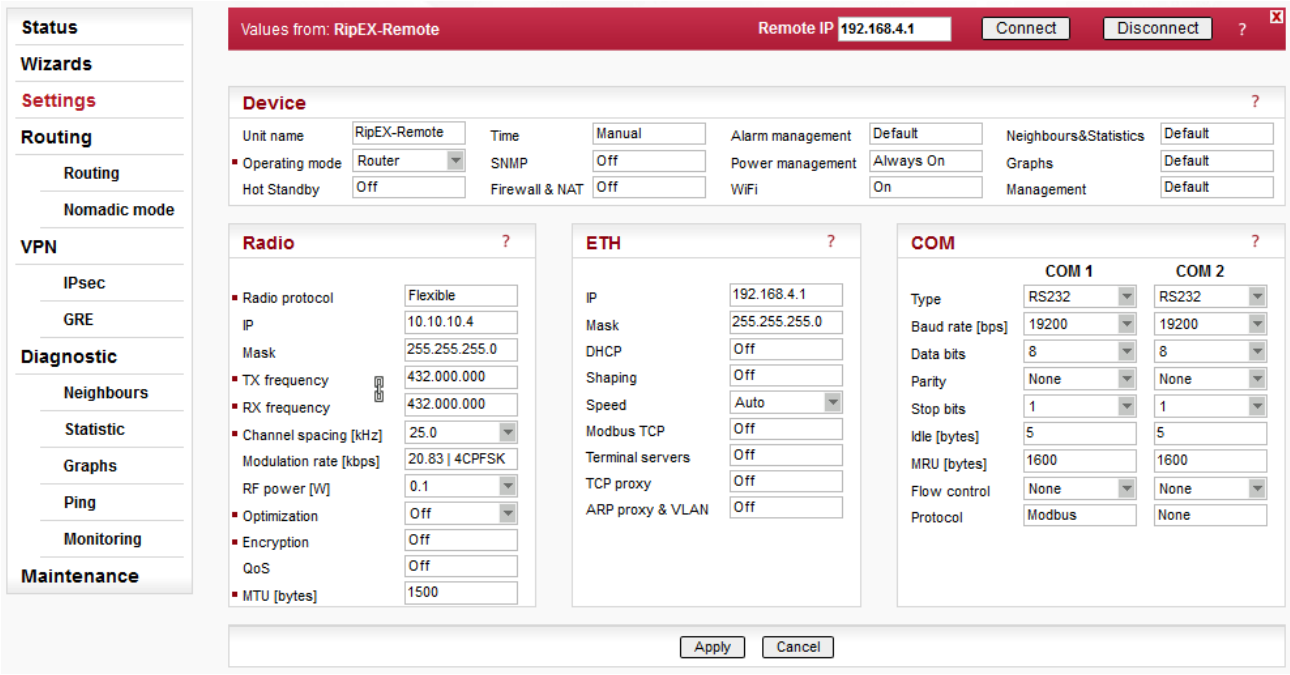
Center refresh period [s]	300



Obr. 9.15: Menu Routing - Base2

Jediný požadovaný routing v tomto příkladě je defaultní (tovární), protože jednotka komunikuje pouze s centrální jednotkou (např. pakety se vysilájí přes centrální jednotku i se vzdálenou (remote) jednotkou napojenou přímo na Bázi.)

9.7.4. RipEX-Remote Konfigurace



Obr. 9.16: Menu Settings - Remote

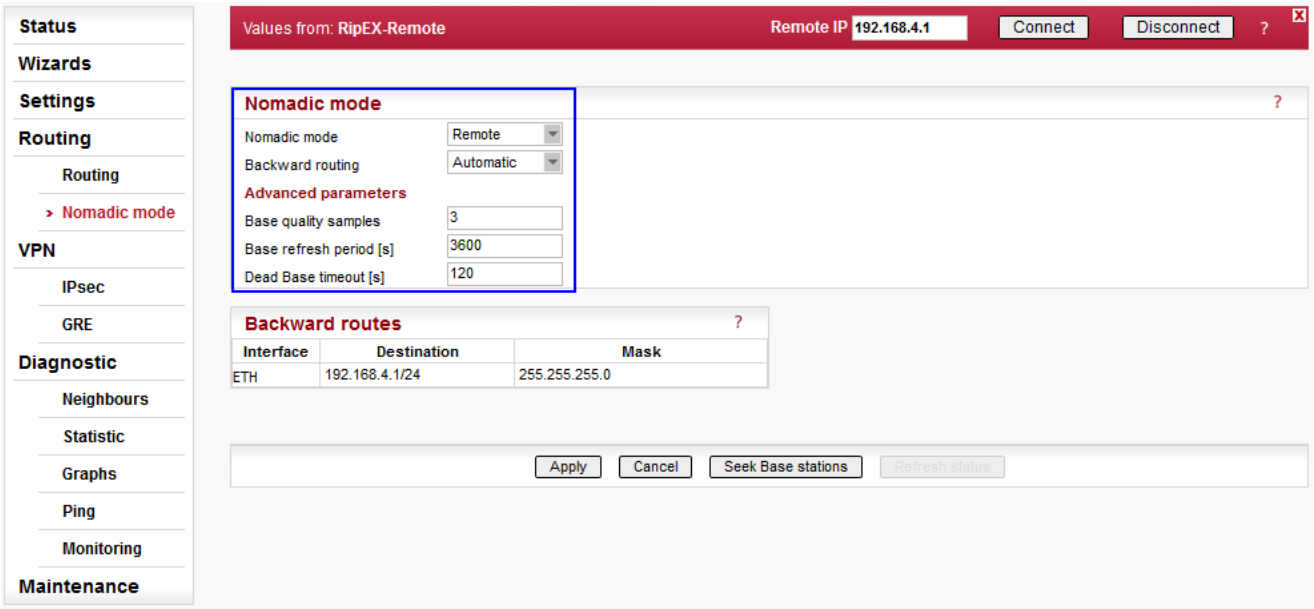
Níže jsou vysvětleny pouze rozdílné parametry v porovnání s Centrem.

Parametry:

Unit name RipEX-Remote

Radio IP/Mask 10.10.10.4/255.255.255.0

ETH IP/Mask 192.168.4.1/255.255.255.0



Obr. 9.17: Menu Nomadic mode - Remote

Parametry:

Nomadic mode remote

Backward routing Automatic

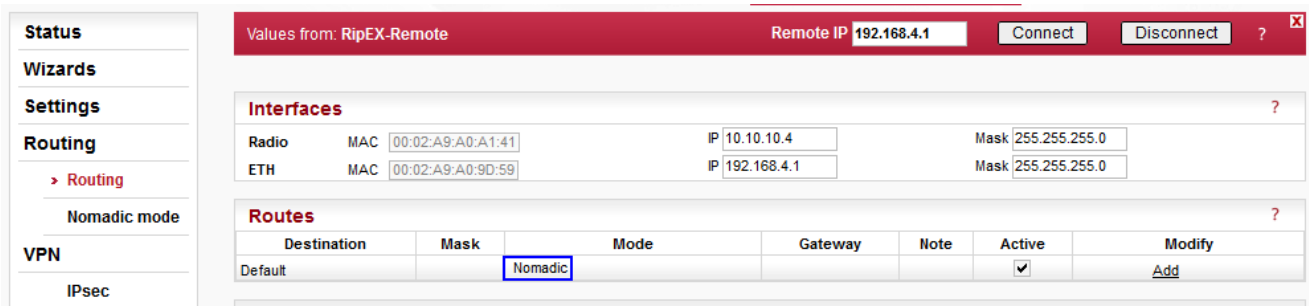
Pokročilé parametry:

Base quality samples 3

Base refresh period [s] 3600

Dead base timeout [s] 120

Zpětné routování může být nastaveno manuálně, ale v námi uvedeném příkladě je mnohem snažší zvolit automatickou volbu, protože automaticky využívá Ethernetovou podsíť nakonfigurovanou v této jednotce. Tato podsíť je jako jediná požadována v našem příkladě.



Obr. 9.18: RipEX-Remote Routing

Routovací tabulka se liší od ostatních jednotek v tomto příkladě. Všechna cesty musí mít nastaven mód Nomadic. V našem příkladu stačí jen defaulní cesta, která bude dynamicky nastavena podle aktuálních podmínek (místo, RSS/DQ atd.).

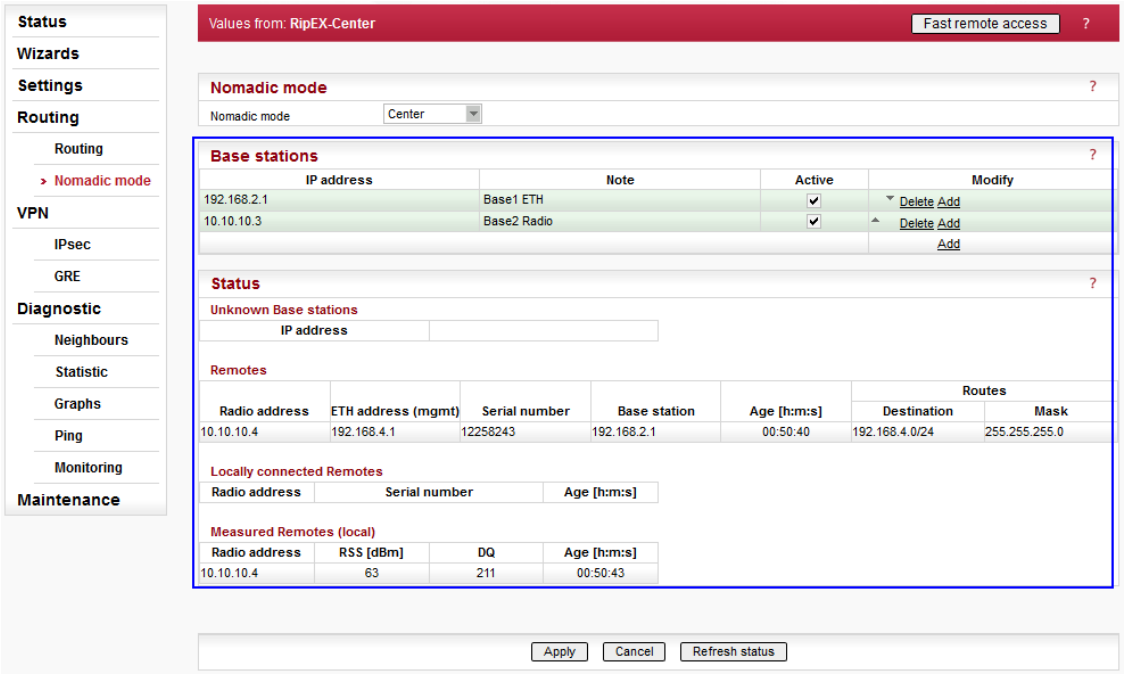
Všechny Remote jednotky muhou být nakonfigurovány stejně, vyžadují se pouze rozdílné rádiové IP adresy a Ethernetové podsítě. Menu Routing zůstává stejné.

9.7.5. Testování a ověření funkčnosti

V této kapitolé jsou popsány statusové tabulky a informace pro rozdílné role v Nomadickém módu. Příklady pro různá umístění Remote jendotky jsou uvedena taktéž.

Menu Nomadic Mode

Central Unit



Obr. 9.19: Menu Nomadic mode - Centrum

Menu zobrazuje stav nakonfigurovaných Bázových stanic. Příklad využívá dvě **Báze** a obě jsou přístupné (např. obě jsou zvýrazněny zeleně. Pokud je nějaká Báze nepřístupná, je zvýraznění červené.

Pod tabulkou nakonfigurovaných Bází jsou zobrazeny **neznámé báze**. To jsou Báze, které se snaží spojit s Centrem, ale nejsou zatím v Centru nakonfigurovány. Pro přidání neznámé bázové stanice do seznamu nakonfigurovaných/aktivních Bází, stiskněte tlačítko "Add"

Další tabulka zobrazuje všechny **Remote** jednotky v síti. Každá z nich je uvedena v seznamu s:

- Rádiová adresa
- ETH address (mgmt) – tuto adresu používejte pro Fast Remote Access
- Výrobní číslo
- Base station – IP adresa Bázeke které je Remote aktuálně připojený.
- Age – čas od posledního přepnutí

- Routes – seznam zpětného routingu

Každá Remote jednotka může být označena červeně, pokud se považuje za "zdvojení" Remote jednotky. Označení “Suspected duplicated Remote” zmizí, jakmile je jednotka obnovena (aktualizována) 8x po sobě beze změny výrobního čísla.

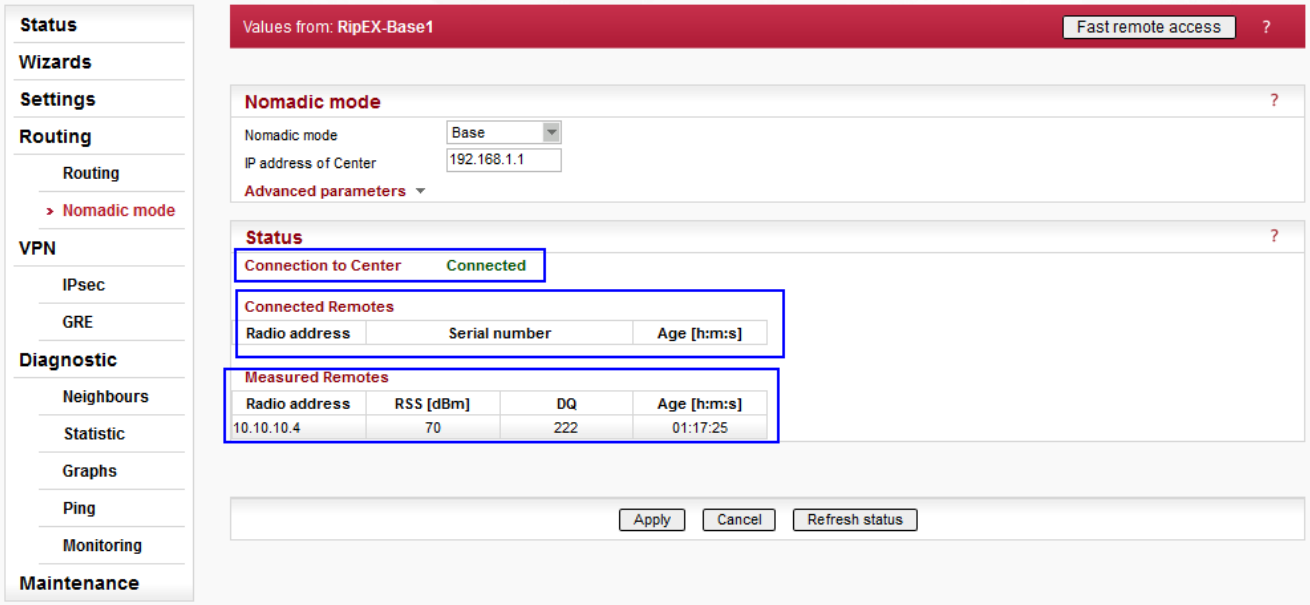
Seznam zpětného routingu je označen:

- “ok” (šedá) – toto pravidlo nekoliduje s jiným a je používáno.
- “ok_coll” (světle zelená) – pravidlo koliduje s jiným pravidlem, ale je používáno.
- “ok_backup” (světle zelená) – pravidlo koliduje s pravidlem záložních tras (Backup routing). To je správně jen tehdy, pokud jsou záložní trasy vybudovány prostřednictvím nomadické cesty, jinak se jedná o konfigurační chybu.
- “coll_rmt” (červená) – Pravidlo koliduje s pravidlem jiného Remote, toto pravidlo je odmítnuto.
- “collision” (červená) – Pravidlo koliduje se statickými pravidly routování nebo se subsítě lokálních rozhraní. Pravidlo je odmítnuto.
- “loop” (červená) – Toto pravidlo by mohlo vytvořit routovací smyčku. Koliduje buď s Bází nebo s adresním rozsahem nebo rádiovým rozhraním. Pravidlo je odmítnuto.

Další tabulka "**Locally connected Remotes**" zobrazuje seznam Remote jednotek, které jsou spojeny přímo s touto centrální jednotkou.

Poslední tabulka "**Measured Remotes**" zobrazuje RSS/DQ hodnoty Remote jednotek, které zkoušely přímo komunikovat s touto centrální jednotkou. Položky starší než 1 den budou smazány.

Base Unit

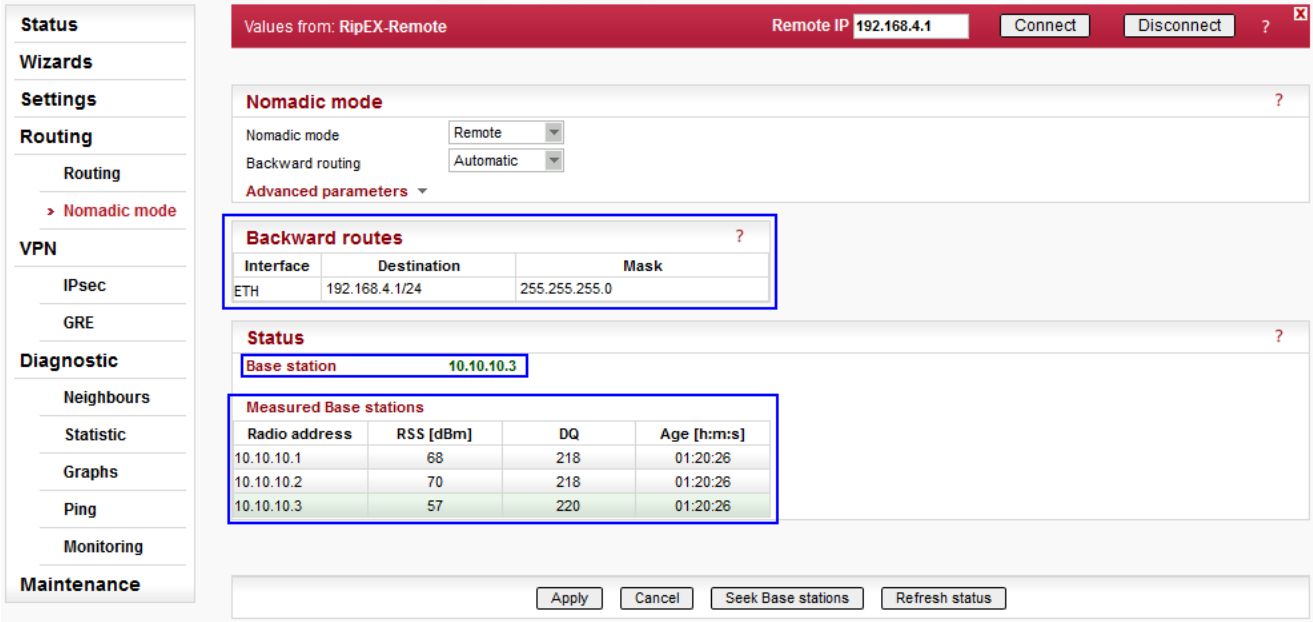


Obr. 9.20: Menu Nomadic mode - Base

V Bázi Nomadického módu jsou tři části. První část zobrazuje, zda je tato Báze připojena k Centru nebo ne.

Tabulky “Connected Remotes” a “Measured Remotes” zobrazují stejnou informaci jako Centrum (viz výše).

Remote Unit



Obr. 9.21: Menu Nomadic mode - Remote

Tabulka “Backward routes” může být vyplněna manuálně nebo automaticky. V tomto příkladě byla nastavena automatická volba a tím pádem byla adresa 192.168.4.1/24 nastavena automaticky (protože tato IP/maska je Ethernetové nastavení lokální jednotky).

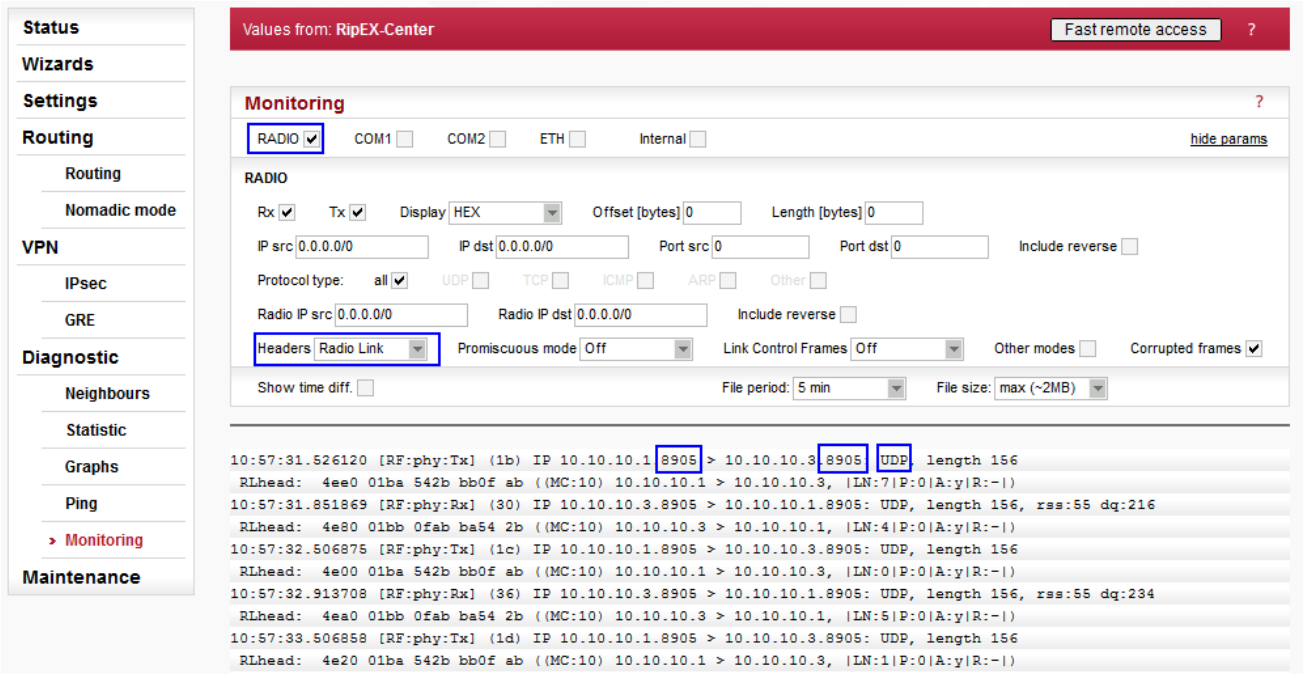
V položce Status je zobrazena Rádiová IP momentálně používané Bázové stanice.

Každá Remote jednotka zobrazuje seznam všech změřených Bází s jejich rádiovými adresami, RSS/DQ hodnoty a čas od posledního měření. Pokud není nějaká Bázova stanice zobrazena, klikněte na “Seek Base stations” pro restart procesu výběru nejlepší Bázové jednotky nebo aktualizujte (obnovte) stránku pro znovuzobrazení informace.

Vybraná Báze je označena zeleně. Ostatní jsou označeny šedě. Pokud Báze odmítne Remote jednotku, bude Báze označena červeně.

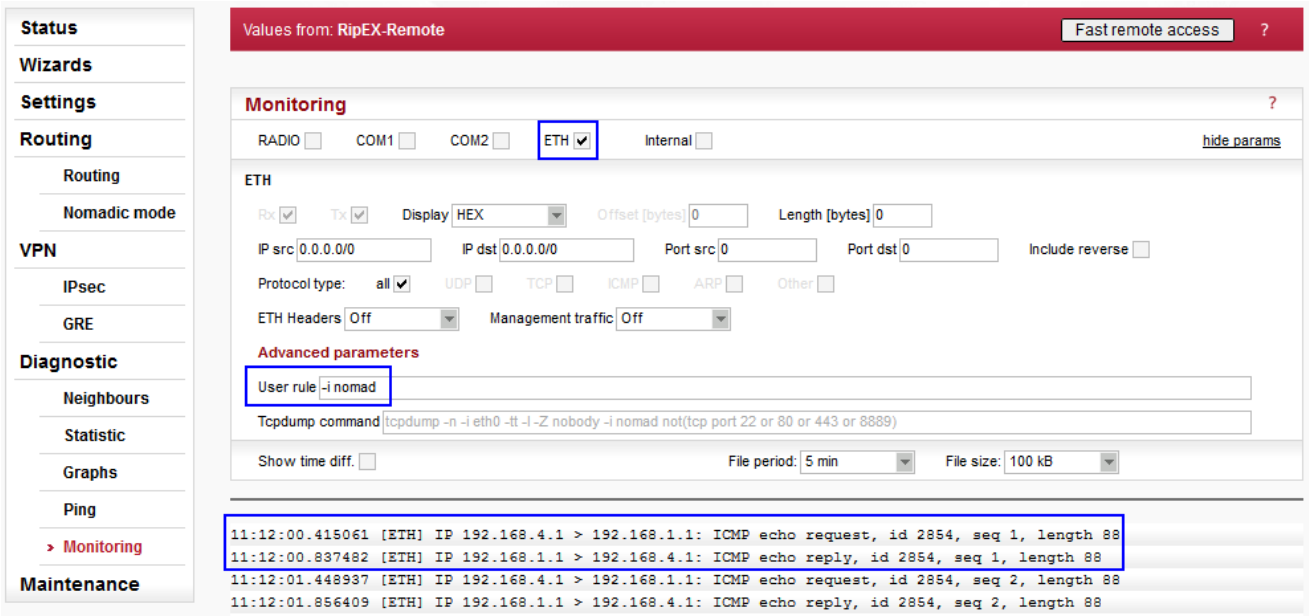
Monitoring

Nomadický provoz používá UDP port 8905. Nomadický mód nemá vlastní monitorovací rozhraní, ale po zadání UPD portu na číslo 8905 může být zachycen na Rádiovém rozhraní.



Obr. 9.22: Monitoring rádiového kanálu v Centru

V Centru a Remote jednotkách může být ETH rozhraní použito i pro monitoring Nomadického provozu. Nastavte pokročilý filtr “-i nomad” jako uživatelské pravidlo a spusťte zachycení provozu.



Obr. 9.23: Monitoring Nomadického provozu v ETH - Remote

9.7.6. Různá umístění Remote

Remote jednotka může být připojena k Centru nebo k jedné z Bází. Pokud je Remote jednotka v pokrytí alespoň jedné z těchto Bází, bude pracovat správně. Na základně změřených RSS/DQ hodnot si Remote jednotka vybere nejlepší Bázi.

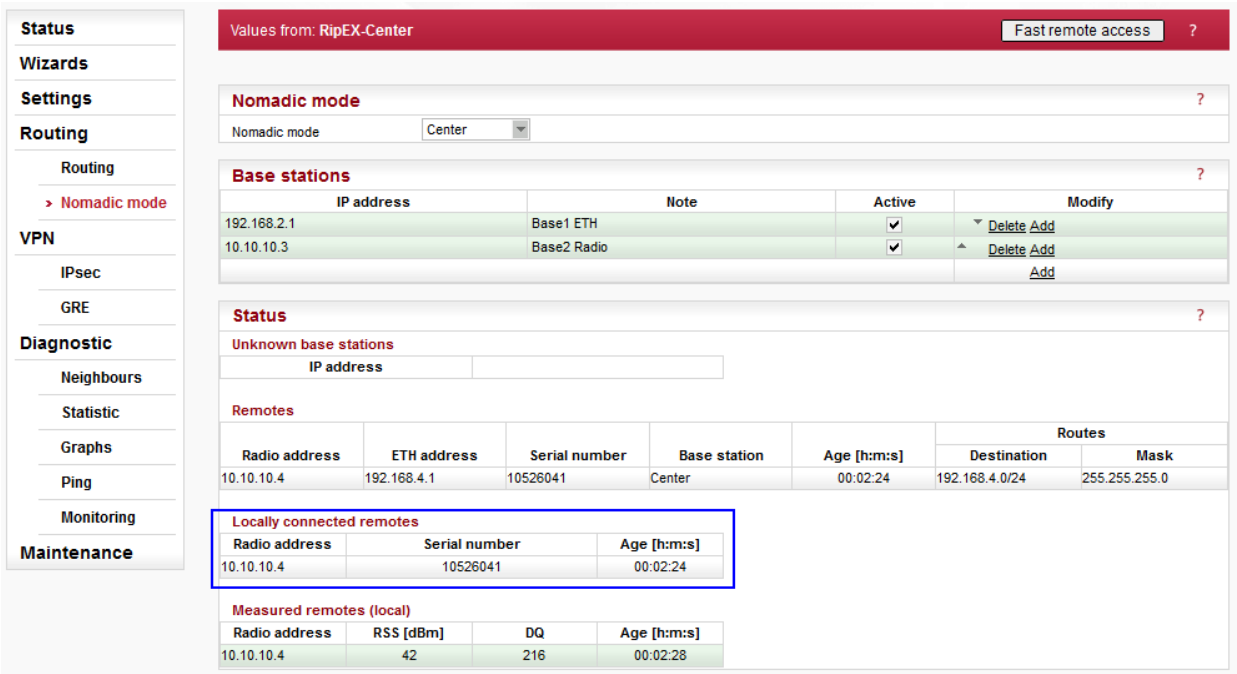
V našem testu, všechny tři možné Báze budou postupně vybrány Remote jednotkou. Jedna z nejjednodušších možností je vypnout a zapnout jednotlivé jednotky. Pokud používáte útlumové prvky a koaxiální kabely pro rádiové pokrytí, můžete stejnou simulaci provést změnou RSS/DQ hodnot. Další možností je odpojení ETH kabelu mezi Centrem a Bází 1. Zmenšení časových limitů v konfiguračních parametrech by taktéž mělo urychlit znovuvybrání Báze.

Pro následující scénáře mohou být aktuální údaje ověřeny v menu Monitoring. Nastavte UDP port 8905 na rádiovém rozhraní nebo použijte parametr '-i nomad' pro Ethernet rozhraní.

Jednotka Central

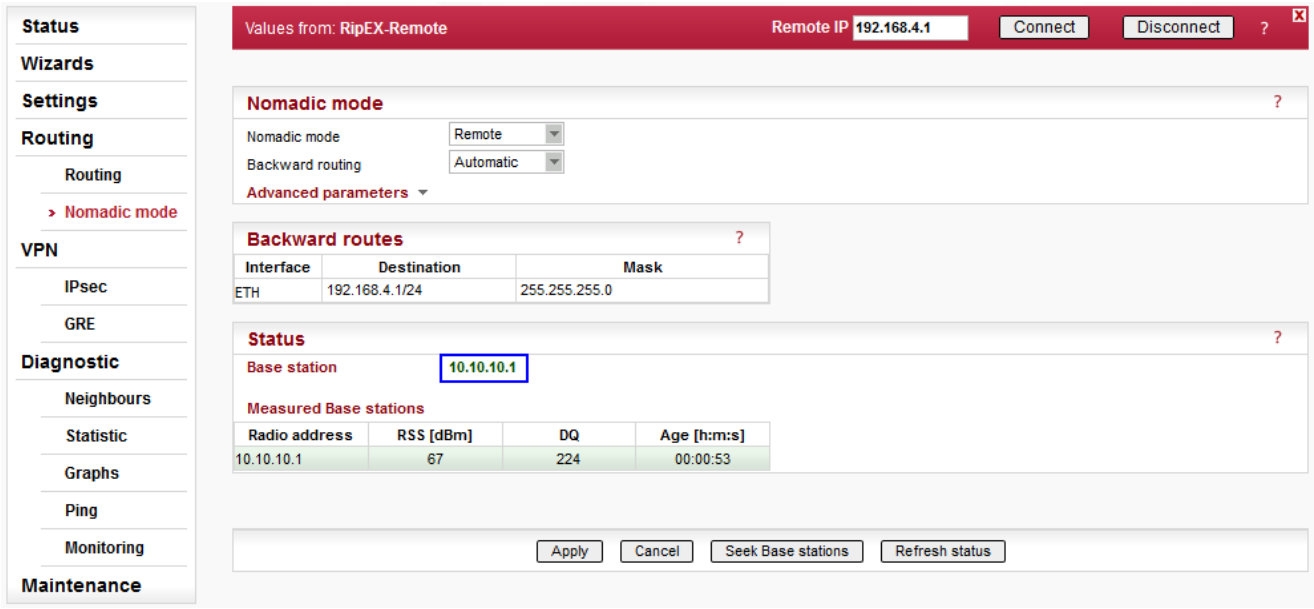
Vypněte všechny RipEX jednotky kromě Centra a poté okamžitě zapněte Remote jednotky. Zkontrolujte, že si Remote jednotka zvolila Centrum a zapněte obě Báze.

V tomto scénáři bude Remote jednotka komunikovat přímo s Centrem jedením rádiovým skokem.



Obr. 9.24: Remote přímo připojený k Centru

V Centru je Remote jednotka 10.10.10.4 zobrazena jako "locally connected Remote".

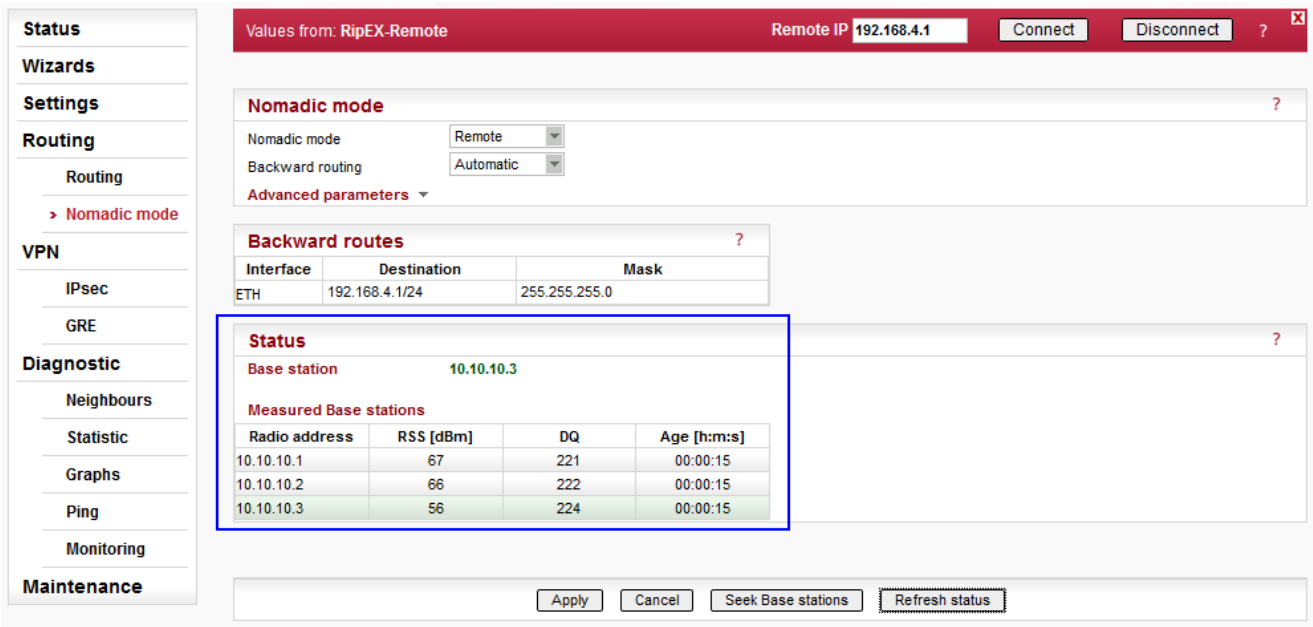


Obr. 9.25: Remote - Centrum je vybráno jako nejlepší Báze

Menu zobrazuje rádiovou IP adresu Centra jako vybranou Bázi. V tabulce “Measured Base stations” je pouze jeden záznam. Momentálně Remote jednotka neví o dalších Bázích.

Pokud aktuální Báze není přístupná po delší dobu, než 120 vteřin (nejsou žádné odpovědi pro data poslané z Remote jednotky do této Báze), začne ověřování dostupnosti Báze. Pokud tato Báze není dostupná, je spuštěn nový “Seek” (vyhledávání) a je vybrána nová Báze.

Klikněte na “Seek Base stations” pro vybrání nejlepší Bázové jednotky. Výsledky mohou záviset na síle vašeho momentální signálu . Obnovte stavovou obrazovku a zkontrolujte menu.



Obr. 9.26: Menu Nomadic mode po vyhledání Bází

Aktuální Báze je jednotka Base2 (10.10.10.3)

POZNÁMKA:
Algoritmus změní aktuální Bázi pouze tehdy, je-li síla signálu (RSS) lepší o více než 5 dBm, jinak bude používat stávající Bázi.

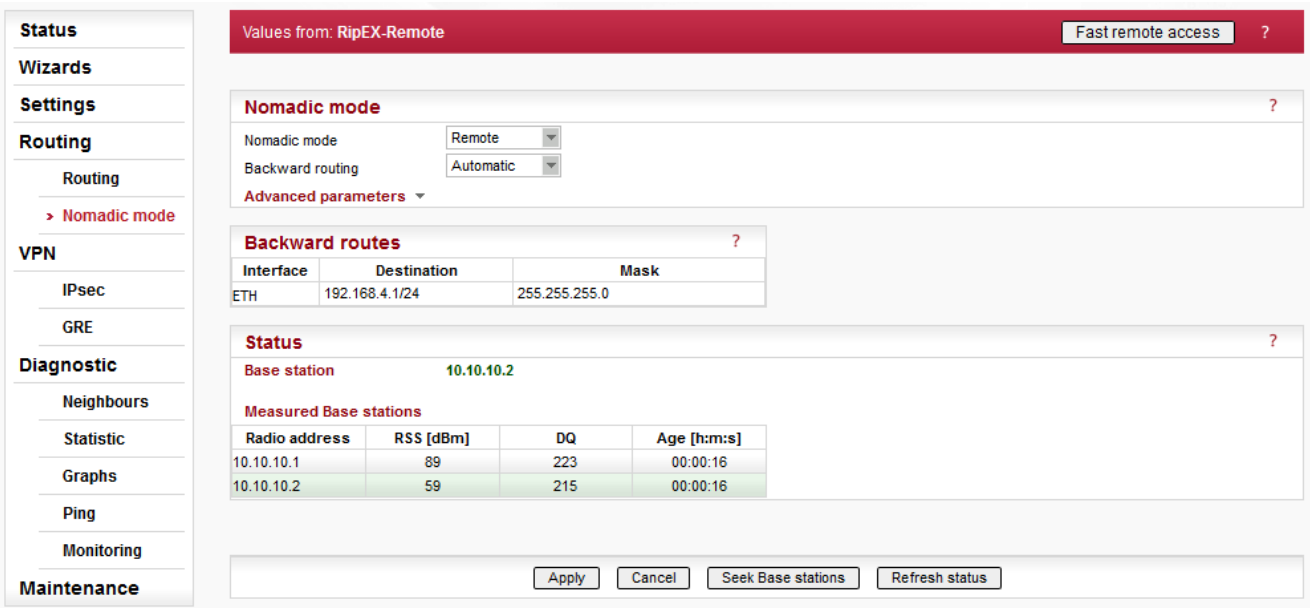
Jednotka Base1

Podobný postup můžete použít I pro Bázi 1. Vypněte jednotky RipEX-Center a RipEX-Base2. Stiskněte "Seek Base stations" v Remote jednotce a zkontrolujte status. Měl by se zobrazit status "Disconnected".

V tomto případě bude Remote jednotka komunikovat přímo s Centrem jedním rádiovým skokem.

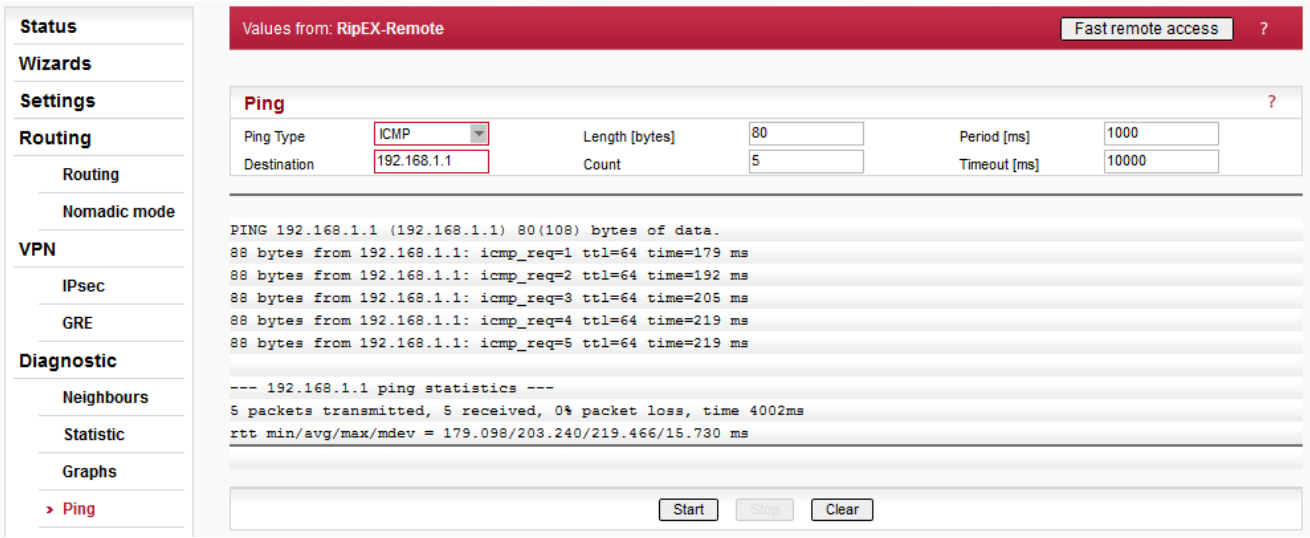
Obr. 9.27: Remote – Disconnected status

Důvod je jednoduchý - v tomto okamžiku není žádné Centrum, pouze jedna Báze. Zapněte centrální jednotku a obnovte status Báze.



Obr. 9.28: Remote – Connected status

Ověřte přístupnost jednotky diagnostickým nástrojem Ping.



Obr. 9.29: Remote unit – Kontrola dostupnosti

POZNÁMKA:
Podobným postupem simulujte RipEX-Base2 jednotku, vybranou jako nejlepší Bázi.

9.8. Režie Nomadického módu a doporučení

Nomadický mód upravuje MTU, vzhledem k nastavenému pro rádiový kanál. Původní hodnota je snížena o 46 B (režie Nomadického módu). Např. pro nastavené MTU 1500 B, se bude používat hodnota 1454 Bytů.

RSS ping pracuje i v Nomadickém módu, ale nezobrazuje změřené RSS/DQ hodnoty. Nezobrazuje aktuální cestu protože každý paket je zapouzdřen v tunelu.

FAQ

Troubleshooting

- Nakonfiguroval jsem Router mód v RipEX jednotce, ale nedaří se mi nakonfigurovat Nomadický mód.

  Pouze "Flexible" protokol podporuje funkci Nomadického módu. Pravděpodobně jste nastavil Base Driven protokol.

- Vidím tři Báze ve Remote jednotce, ale ta vybraná neukazuje RSS/DQ hodnoty. Proč?
- ○ Přemístil jsem Remote jednotku na jiné místo a nedokáže už komunikovat s centrální jednotkou.

  Pokud je Remote jednotka připojena k Bázi, tak se připojí k jiné pouze je-li síla signálu lepší alespoň o 5 dBm. V případě, že síla signálu lepší není, jednotka ne nepřepojí.

  Spusťte manuálně “Seek Base stations” pro vybrání nové Báze nebo počkejte, dokud neskončí “Dead base timeout”. Pak se vyhledávání spustí automaticky.

  Pokud není žádný požadavek na komunikaci, musí vyprchat “Base refresh period” před tím, než je nové vyhledávání spuštěno automaticky.

  Nachází se v pokrytí rádia alespoň jedna Báze?
- Remote jednotka dokáže komunikovat s centrální jen v případě, že jsou spojeny přímo. V případě spojení přes jinou Bázi komunikace neproběhne

  Je tato Baze nakonfigurována v centrální jednotce? Každá Báze se musí přidat manuálně.

  Má Remote jednotka nastavený “nomadic” v routovacích pravidlech? Tj. Mění dynamicky svoje směrování podle aktuálních podmínek připojení, Nejsou routovací pravidla nastavena staticky?

  Je Remote jednotka opravdu připojena k požadováné Bázi? Klikněte na "Seek" Bázových jednotek a ověřte funkčnost.

9.9. CLI příkazy

Rozhraní CLI (Command Line Interface) je alternativa k webovému přístupu. Při použití správného klienta (SSH nebo Telnet) můžete pracovat s CLI rozhraním v textovém módu.

Nomadické CLI příkazy:

- cli_status_nomad_show
  Zobrazí status Nomadického módu

```
CLI(admin):~cli_status_nomad_show
Status of Nomadic mode:
Mode: remote
State: connected
Base: 10.10.10.2
Measured Base stations:
  Radio address: 10.10.10.1  RSS: 89dBm  DQ: 223  Age: 293s  Flag:
  Radio address: 10.10.10.2  RSS: 59dBm  DQ: 215  Age: 293s  Flag: selected
```

- cli_cnf_show_nomad
  Zobrazí konfiguraci Nomadického módu

```
CLI(admin):~$ cli_cnf_show_nomad
Nomadic mode: Remote (r)
Protocol message repeats: 2
Remote - Base quality samples: 3
Remote - Base seek slots: 8
Remote - Base refresh period: 3600 s
Remote - Base re-seek ratio: 24
Remote - Dead Base detection timeout: 120 s
Remote - Backward routing mode: Automatic (a)
```

- cli_cnf_show_nomad_backrts
  Zobrazí zpětné routování Nomadického módu

```
CLI(admin):~$ cli_cnf_show_nomad_backrts
Backward routes:
1. Destination IP: 192.168.4.1    Destination mask: 24    Note:     Rule active: On (n)
```

- cli_cnf_show_nomad_bases
  Zobrazí seznam Bází Nomadického módu

```
CLI(admin):~$ cli_cnf_show_nomad_bases
Base stations:
1. IP address: 192.168.2.1    Note: Base1 ETH    Item is active: On (n)
2. IP address: 10.10.10.3    Note: Base2 Radio    Item is active: On (n)
```

- cli_cnf_set_nomad_backrts
  Změní zpětný routing Nomadického módu
- cli_cnf_set_nomad_bases
  Změní seznam Bází Nomadického módu
- cli_nomad_force_seek
  Donutí Bázovou stanici hledat v Nomadickém módu (Remote).
- cli_nomad_reject_remotes
  Odpojí všechny lokálně připojené Remote jednotky (Báze nebo Centrum) v Nomadickém módu
- cli_cnf_set_nomad
  Změna konfigurace Nomadického módu

Spusťte CLI příkaz s parametrem -h pro podrobnosti příkazů.

9.9.1. Parametry, které jsou přístupné jen přes CLI

Některé pokročilé paramtery mohou být nastaveny jen přes CLI

Centrum

Protocol message timeout

- Default = 5 s [0.1 - 25.5]
- Timeout pro zpávy posílané Bázím
- Příklad příkazu: “cli_cnf_set_nomad -msg-tout 10”

Báze

Protocol message timeout

- Default = 5 s [0.1 - 25.5]
- Timeout pro zprávy posílané do Centra. Není-li žádná jiná komunikace, jsou udržovací pakety posílány po uplynutí tohoto timeoutu.
- Příkaz příkladu: “cli_cnf_set_nomad -msg-tout 10”

Reconnection speedup

- Default = 1 [1 no speedup - 15 max. speedup]
- Hodnota “Center refresh period” je dělena tímto parametrem pro urychlení přepojení.
- Příklad příkazu: “cli_cnf_set_nomad -bs-speedup 2”

Remote

Base seek slots

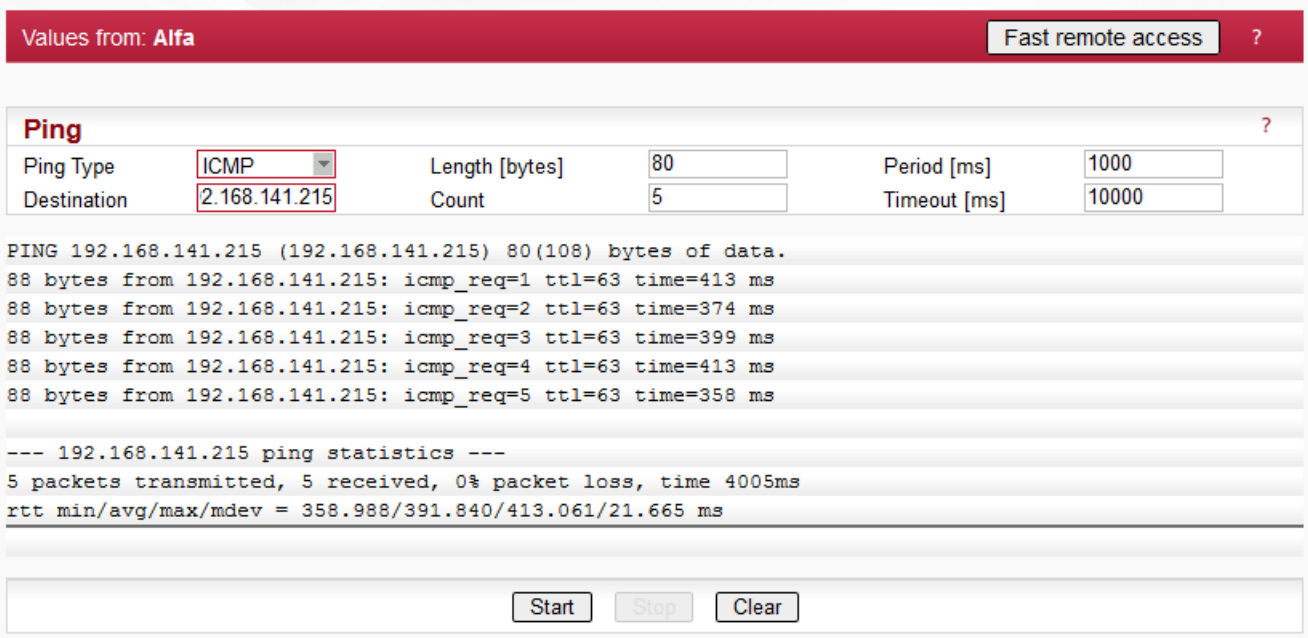
- Default = 8 [3 - 32]
- Definuje periodu (měřenou ve slotech)čekání na odpověď Báze při čekání na Bázi s nejlepším signálem. Vyšší číslo znamená menší pravděpodobnost kolize.
- Příklad příkazu: “cli_cnf_set_nomad -seek-slots 12”

Base re-seek ratio

- Default = 24 [4 - 2047]
- Používá se pro nastavení časové periody mezi hledáními pro zjištění Báze s nejlepší sílou signálu místo (jen) ověření Báze.
- Defaultně je “Base refresh period” 3600s a “base re-seek ratio” je 24, tj. Hledání Báze proběhne jedenkrát za den.
- Příklad příkazu: “cli_cnf_set_nomad -rsk-ratio 48”

10. Diagnostic menu

10.1. Ping



Obr. 10.1: ICMP Ping

Ping (Packet InterNet Groper) se používá pro testování dostupnosti jednotlivých účastníků IP sítě. Vysílá k cílovému účastníkovi pakety echo request a čeká na odpovědi echo response. Přitom měří rtt (round trip time - čas od vyslání do přijetí paketu) a zaznamenává ztráty paketů.

Před používáním pingu se ujistěte, že je nastaven správný routing mezi adresami src a dst. Cílové zařízení musí mít povolen ICMP echo response. RipEX jej má povolen vždy.

POZNÁMKA:
Ping utility generuje on-line report každé 2 sekundy, pokud jste připojeni k jednotce Local a každých 10 sec, pokud je report generován v jednotce Remote a je přenášen rádiovým kanálem.

- **Ping Type**
  List box: ICMP, RSS
  Default = RSS
  - **ICMP**
    Standardní ICMP (Internet Control Message Protocol) ping. Může být použit proti RipEXu nebo libovolnému zařízení připojenému k rádiové síti RipEX.
  - **RSS**
    RSS Ping používá speciální UDP paket a poskytuje další informace:
    - RSS a DQ informace o každém rádiovém skoku každého pingu
    - RSS a DQ statistiku (průměr, min., max.) pro rádiové skoky s nejslabším RSS, v obou směrech
    - Histogram pro rtt (doba odpovědi pingů) rozdělený do 5 intervalů
    - Load a Throughput
    - PER (Packet Error Rate)
    - BER (Bit Error Rate)

- **Destination**

Default = 127.0.0.1
Cílová IP adresa

- **Length [bytes]**
  Default = 80
  Délka uživatelských dat v rozsahu od 8 do 4096 Byte. K této délce je vždy přidána hlavička délky:
  ICMP = 28 Byte
  RSS = 43 Byte pro IP+UDP+RACOM hlavičku + 8 Byte (sledování RSS a DQ) pro každý rádiový skok + 4 bytes (doplněno v serveru)
  RSS ping nemůže být delší než 3/4 MTU.

- **Count**
  Default = 5
  Počet pingů, který bude vyslán. Rozsah od 1 do 1024.

- **Period [ms]**
  Default = 1000
  Po uplynutí této periody je vyslán další Ping. Rozsah od 1000 (1 sec) do 3600000 (1 hodina).

- **Timeout [ms]**
  Default = 10000
  Timeout je od 1000 (1 sec) do 3600000 (1 hodina).
  Jestliže odpověď na ping není přijata během této doby, je ping započítán jako ztracený.

  Pro každý ping je generována zpráva. Po dokončení pingů je zobrazena celková statistika.

- **ICMP Ping report**
  Standardní ping report podle Linuxu, viz *Obr. 10.1 – „ICMP Ping“* :

  Run-time report:

```
88 bytes from 192.168.141.215: icmp_req=1 ttl=63 time=413 ms
```

`88 bytes`	celková délka paketu
`192.168.141.215`	destination IP (cílová adresa)
`icmp_req=1`	pořadové číslo pingu
`ttl=63`	životnost (time to live), max. počet průchodů přes routery v síti, které paket může ještě provést
`time=413 ms`	rtt (round trip time), čas od vyslání paketu ICMP echo request do přijetí odpovědi ICMP echo response

  Statistic report:

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 358.988/391.840/413.061/21.665 ms
```

`time 4005ms`	celkový čas chodu utility ping (od Start do vyčepání Count nebo do stisku Stop)
`rtt min/avg/max/mdev`	doba cyklu (round trip time), minimální / průměrná / maximální / standardní odchylka

■ RSS Ping report

RSS Ping report poskytuje více diagnostických informací:

```
RSS Ping from 192.168.141.213 to 192.168.141.215, size:80+43(+trace)
131 bytes from 192.168.141.215: seq=1 rtt=0.391s
   192.168.141.213-->10.10.10.214 :52/229[RSS/DQ]-->
                     10.10.10.215 :45/220[RSS/DQ]-->192.168.141.215
   192.168.141.215-->10.10.10.214 :45/232[RSS/DQ]-->
                     10.10.10.213 :51/229[RSS/DQ]-->192.168.141.213

131 bytes from 192.168.141.215: seq=2 rtt=0.458s
   192.168.141.213-->10.10.10.214 :52/232[RSS/DQ]-->
                     10.10.10.215 :45/223[RSS/DQ]-->192.168.141.215
   192.168.141.215-->10.10.10.214 :45/229[RSS/DQ]-->
                     10.10.10.213 :51/241[RSS/DQ]-->192.168.141.213

131 bytes from 192.168.141.215: seq=3 rtt=0.431s
   192.168.141.213-->10.10.10.214 :52/220[RSS/DQ]-->
                     10.10.10.215 :45/232[RSS/DQ]-->192.168.141.215
   192.168.141.215-->10.10.10.214 :45/235[RSS/DQ]-->
                     10.10.10.213 :51/232[RSS/DQ]-->192.168.141.213

---RSS Ping from 192.168.141.213 to 192.168.141.215 statistics---
3 packet(s) transmitted, 3 received,  0.00% packet loss (0 corrupted), time 2.44 sec
rtt: min/avg/max/mdev = 0.391/0.427/0.458/0.0277 sec.

Load: 1211 bps
Throughput: 1211 bps

PER: 0.00% round trip, 0.00% one-way
BER: 0.00% round trip, 0.00% one-way

Radio hop with lowest RSS - direction to Destination
RSS:     52.0/52.0/52.0/0.0      min/avg/max/mdev
DQ :     220.0/221.0/223.0/1.4   min/avg/max/mdev

Radio hop with lowest RSS - direction from Destination
RSS:     51.0/51.3/52.0/0.5      min/avg/max/mdev
DQ :     229.0/230.0/232.0/1.4   min/avg/max/mdev

rtt histogram (time interval in sec.: %, count)
       0 -      2.5: 100.00%     3      XXXXXXXXXX
     2.5 -        5:   0.00%     0
       5 -      7.5:   0.00%     0
     7.5 -       10:   0.00%     0
      10 -      inf:   0.00%     0
```

Průběžná zpráva:

```
RSS Ping from 192.168.141.213 to 192.168.141.215, size:80+43(+trace)
   131 bytes from 192.168.141.215: seq=1 rtt=0.391s
```

```
 192.168.141.213-->10.10.10.214 :52/229[RSS/DQ]-->
                   10.10.10.215 :45/220[RSS/DQ]-->192.168.141.215
 192.168.141.215-->10.10.10.214 :45/232[RSS/DQ]-->
                   10.10.10.213 :51/229[RSS/DQ]-->192.168.141.213
```

`131 bytes`	velikost paketu RSS (RACOM hlavička + data + trasa)
`10.10.10.214`	repeater IP (adresa retranslace)
`192.168.141.215`	destination IP
`seq`	pořadové číslo pingu
`rtt`	round trip time, čas od vyslání do přijetí paketu

Statistická zpráva:

```
3 packet(s) transmitted, 3 received,  0.00% packet loss (0 corrupted), time 2.44 sec
rtt: min/avg/max/mdev = 0.391/0.427/0.458/0.0277 sec.
```

`corrupted`	počet paketů. které byly přijaty (UDP klavička je OK) ale jejichž data byla porušena (chyba v CRC datové části)
`time`	celkový čas chodu utility ping (od Start do vyčepání Count nebo do stisku Stop)
`rtt min/avg/max/mdev`	doba cyklu (round trip time), minimální / průměrná / maximální / standardní odchylka

```
Load: 1211 bps
Throughput: 1211 bps
```

`Load`	zátěž generovaná utilitou Ping
`Throughput`	propustnost rádiové sítě

```
PER: 0.00% round trip, 0.00% one-way
BER: 0.00% round trip, 0.00% one-way
```

`PER`	Packet Error Rate, to je pravděpodobnost ztráty paketu. Je počítána pro celou trasu i pro jeden směr.
`BER`	Bit Error Rate, pravděpodobnost, že je přijat bit s chybnou hodnotou. V paketové síti může být ztracen celý paket, ne jednotlivý bit. Přijetí špatného bitu tedy způsobí ztrátu celého paketu. Hodnota BER je počítána ze zjištěné hodnoty PER.

```
Radio hop with lowest RSS - direction to Destination
RSS:     52.0/52.0/52.0/0.0      min/avg/max/mdev
DQ :     220.0/221.0/223.0/1.4   min/avg/max/mdev
```

```
Radio hop with lowest RSS - direction from Destination
RSS:     51.0/51.3/52.0/0.5      min/avg/max/mdev
DQ :     229.0/230.0/232.0/1.4   min/avg/max/mdev
```

Informace o RSS (síla přijatého signálu) a DQ (Data Quality) z rádiového skoku s nejslabším RSS, samostatně pro oba směry (do cílového RipEXu a zpět). Je zde i standardní odchylka mdev, která dává představu o homogenitě signálu. Nižší hodnota mdev ukazuje na vyšší spolehlivost linky. Tato "homogenita" vyjadřuje rozptyl hodnot RSS pro jednotlivé pingy.

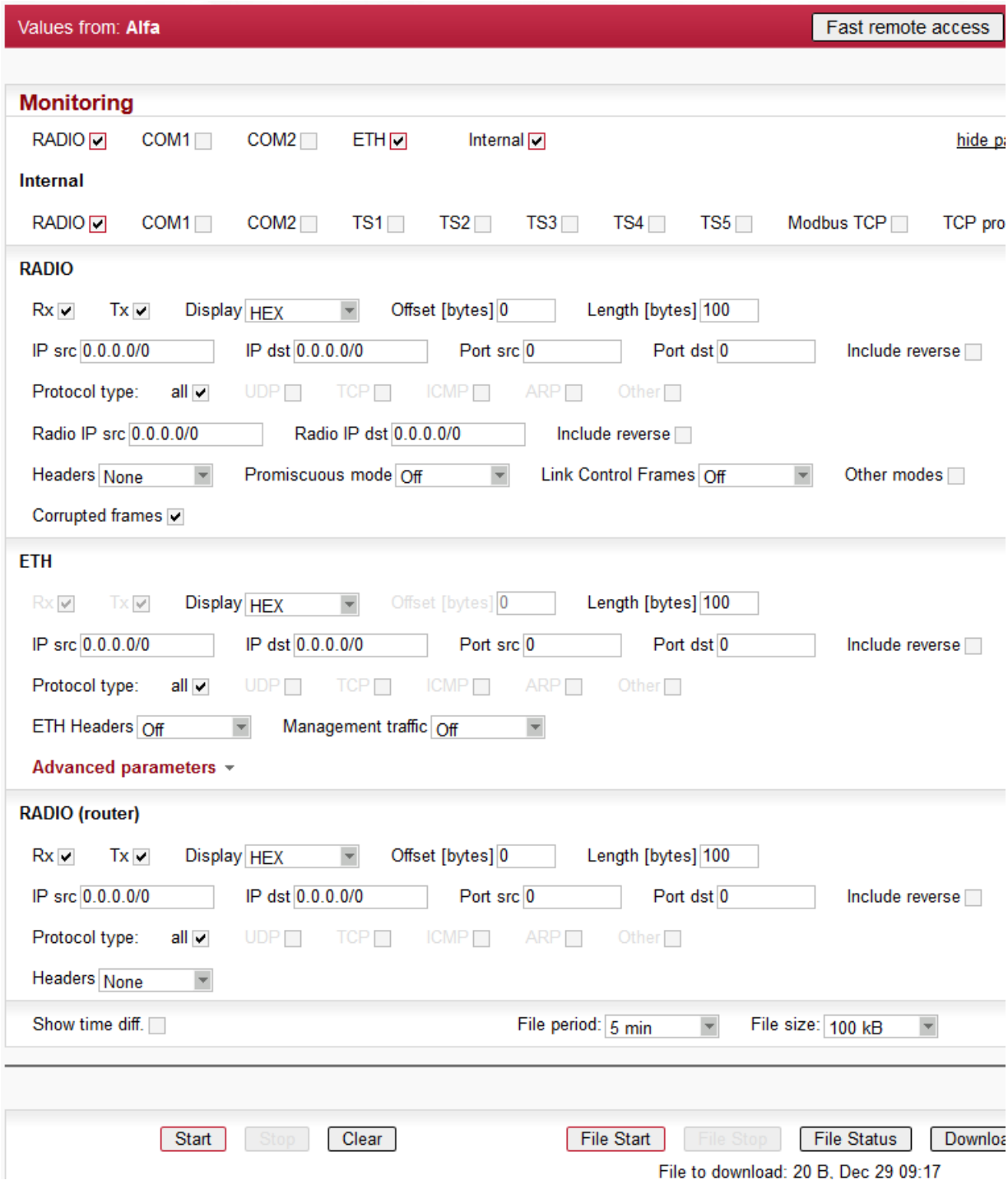
```
rtt histogram (time interval in sec.: %, count)
       0 -      2.5: 100.00%     3      XXXXXXXXXX
     2.5 -        5:   0.00%     0
       5 -      7.5:   0.00%     0
     7.5 -       10:   0.00%     0
      10 -      inf:   0.00%     0
```

Rozložení hodnot rtt (round trip times) pro jednotlivé pingy. Časové intervaly v tabulce jsou 1/4 Timeoutu zvoleného v parametrech pingu. Znaky XXXX... na konci řádku tvoří jednoduchý sloupcový graf.

■ **Buttons**

Start - startuje pingy
Stop - zastaví pingy, poté je zobrazena Statistická zpráva
Clear - smaže zprávu z obrazovky

10.2. Monitoring



Obr. 10.2: Menu Monitoring

Monitoring je pokročilý on-line diagnostický nástroj, který umožňuje podrobnou analýzu komunikace na kterémkoli rozhraní routeru RipEX. Kromě všech fyzických rozhraní (RADIO, ETH, COM1, COM2) mohou být monitorována i další rozhraní mezi softwarovými moduly.

Výstup monitoringu je možno sledovat on-line nebo jej uložit do souboru v RipEXu (nebo ve vzdáleném RipEXu) a stáhnout později.
Popis vnitřních rozhraní je uveden níže.

Krátká ukázka monitorovací zprávy. *Komentované příklady* jsou uvedeny dále.

```
07:55:04.661446 [COM1:phy:Rx] length 2
        0x0000:  aaaa
07:55:04.674861 [RF:phy:Tx] (88) IP 192.168.141.213.8881>192.168.141.214.8882: UDP,length 32
        0x0000:  0800 4500 001e 0000 4000 4011 9dd2 c0a8
        0x0010:  8dd5 c0a8 8dd6 22b1 22b2 000a 72cf aaaa
```

■ **Monitorovaná rozhraní**
Zaškrtávací políčka:
RADIO, COM1, COM2, ETH, Internal
Po zaškrtnutí je možno nastavit příslušná rozhraní (interfejsy). Po zaškrtnutí rozhraní "Internal" se objeví další sada políček pro vnitřní rozhraní:

Internal:
RADIO, COM1, COM2, TS1, TS2, TS3, TS4, TS5, Modbus TCP, TCP proxy
Po jejich zaškrtnutí se objeví konfigurační parametry příslušných rozhraní (viz jejich *popis níže*).

■ **Společné parametry pro všechna rozhraní:**

Rx Tx
Zaškrtávací políčka.
Po zaškrtnutí jsou monitorovány pakety (rámce, hlášení) procházející v příslušném směru. Paket je považován za Tx, jestliže odchází ven z příslušného softwarového modulu (např. RADIO nebo Terminal Server) a naopak. Při monitorování vnějšího rozhraní (např. COM:phy), představuje Tx také paket vysílaný z RipEXu přes příslušné rozhraní (Rx znamená "přijímaný"). Představa směrů na vnitřních rozhraních nemusí být zcela zřejmá, pro objasnění nahlédněte prosím na dále uvedené *schéma*.
Oddělení směrů pro monitorování RX nebo Tx rámců není možné na rozhraní ETH.

Display
List box: HEX, HEX+ASCII, ASCII
Default = HEX
Formát monitorovacího výstupu.

Offset [bytes]
Default = 0
Počet byte, které nebudou zobrazeny, počítáno od začátku paketu nebo rámce. Následují byte v počtu podle parametru Length.
Tento parametr není možno použít pro rozhraní ETH.

Length [bytes]
Default = 100
Počet byte, které budou zobrazeny z každého paketu nebo rámce.
Příklad:
Offset=2, Length=4 znamená, že budou zobrazeny byte od třetího do šestého včetně:
Data (HEX): `01AB3798A28593CD6B96`
Monitorovací výstup: `3798A285`

■ **Filtrování IP/ARP paketů**
(dostupné pro RADIO, ETH a Internal RADIO (router), COMn(router), TSn(router), Modbus TCP(router), TCP proxy (TCP), TCP proxy(router)):

IP src
Rozsah adres IP source ve formátu: aaa.bbb.ccc.ddd/mask

IP dst
Rozsah adres IP destination ve formátu: aaa.bbb.ccc.ddd/mask

Port src
TCP/UDP source port (nebo rozsah) ve formátu: aaaa(-bbbb)

Port dst
TCP/UDP destination port (nebo rozsah) ve formátu: aaaa(-bbbb)

Include reverse
Zaškrtávací políčko.
Pokud je zaškrtnuto, pak rámce definované adresou IP src (nebo IP dst) a Port src (nebo Port dst) budou zobrazeny v obou směrech. Tedy každá hodnota "src" je použita filtrem také jako "dst" a naopak.

Protocol type
(dostupné pro RADIO, ETH a Internal RADIO (router))
Zobrazení pouze označených protokolů. "Other" znamená zobrazení všech protokolů kromě těchto čtyř (zobrazí také ne-IP rámce v případě rozhraní RADIO).

■ **Specifické parametry pro RADIO**

Radio IP src
Adresa rámce Radio IP source musí být v definovaném rozsahu: aaa.bbb.ccc.ddd/mask. Adresa Radio IP je viditelná např. v ARPu nebo v Radio Link Header.

Radio IP dst
Adresa rámce Radio IP destination musí být v definovaném rozsahu: aaa.bbb.ccc.ddd/mask.

Headers:
List box: None, Radio Link, Data Coding, Both
Default = None
- None – zobrazena pouze data z Radio Link Protocol
- Radio Link – zobrazen navíc Radio Link Control Header. Obsahuje např. frame type, No., Radio MAC adresy atd.
- Data Coding – zobrazen navíc Data Coding Header. Obsahuje informace o kompresi dat, fragmentaci a kryptování.
- Both – zobrazeny obě uvedené hlavičky.

POZNÁMKA: Někdy může být obtížné nalézt původní data v rámci Radio Link Protokolu. V závislosti na operačním módu (Bridge nebo Router) a použitém rozhraní (ETH, COM, Terminal Server...) se mohou objevit různé hlavičky protokolu (ETH, IP, UDP...) a celá datová část může být komprimována nebo kryptována.

Promiscuous mode:
List box: On, Off
Default = Off
- Off – monitoring zpracovává pouze rámce, které jsou normálně přijímány jednotkou. Tedy rámce, jejichž Radio IP destination souhlasí s adresou Radio IP této jednotky RipEX, navíc ještě rámce broadcast.
- On – monitoring zpracovává (dále filtruje) všechny rámce detekované rádiovým kanálem.

Link Control Frames
List box: On, Off
Default = Off
- Off – rámce Radio Link Control nejsou zobrazeny (např. rámce ACK).
- On – rámce Radio Link Control jsou zobrazeny, pokud projdou nastavenými filtry monitoringu.

Other modes
Zaškrtávací políčko.
Je-li rozhraní RADIO v módu Promiscuous, pak jednotka může monitorovat na příjmu rámce vysílané v různých operačních módech (Bridge x Router). I když některé rámce nemohou být zcela analyzovány je jejich obsah zobrazen, pokud je zaškrtnuto odpovídající políčko. Viditelná jsou pouze použitelná políčka, tedy v módu Router je k dispozici políčko Bridge a naopak.

Rx stream
Tick box.
Po zaškrtnutí jsou do monitoringu zahrnuty přijímané rámce v módu stream. Platí to pouze pro Bridge mód s uzavíráním rámců ve Stream módu. Upozornění: Provoz v módu Stream typicky obsahuje velký počet krátkých rámců, je tedy generováno nadměrné množství monitorovacích dat. Ve stream módu nejsou monitorovány TX rámce.

Corrupted frames
Zaškrtávací políčko.
Default = zaškrtnuto
Pokud není zvoleno, pak porušené ("header CRC error", "data CRC error", etc.) rámce nejsou zobrazeny. Zobrazení vadných rámců může být užitečné, když je rádiový kanál silně rušený a množství vadných rámců ztěžuje normální čtení monitoringu.

■ **Specifické parametry pro ETH**

ETH Headers
List box: On, Off
Default = Off
Ve stavu ON je hlavička ETH obsažena v monitorovacím výstupu. Jinak je zobrazen pouze IP paket.
Pokud má být zobrazeno VLAN ID paketů VLAN, pak je třeba zapnout ETH Headers = "On".

Management traffic
List box: On, Off
Default=Off
Ve stavu Off nejsou monitorovány vstupní a výstupní datagramy portů HTTPS, HTTP a SSH této jednotky. Tím předejdeme vzniku smyčky za obvyklých podmínek, tedy při on-line monitoringu na PC lokálně připojeném přes ETH rozhraní.

Advanced parameters
User rule
Pro ETH monitoring se používá standardní program ethdump. Do tohoto textového pole lze vložit libovolné další pravidlo v syntaxi tcpdump. Pravidlo je pak připojeno za podmínky filtrů generovaných pro ETH rozhraní na této stránce.
POZNÁMKA: Některá pravidla nejsou podporována. Pokud je použito takové pravidlo, objeví se zpráva (ETH monitoring terminated. Invalid tcpdump parameters?)

■ **Internal - RADIO (router):**
- **Headers:**
  List box: None, Packet (IP), Frame (ETH)

Default: None
- None – Zobrazena jsou pouze data (payload), tedy datová část UDP datagramu.
- Packet (IP) – Doplněny jsou hlavičky paketové vrstvy, je tedy zobrazen celý IP paket.
- Frame (ETH) – Zobrazen je celý rámec Ethernet, tedy včetně ETH hlavičky.

■ **Ovládání výstupu monitoringu**

Show time diff.
Zaškrtávací políčko.
Default = Neoznačeno
Při zaškrtnutém políčku je v monitorovacím výpisu uveden časový rozdíl od předchozího záznamu.

File period
List box: 1 min, 2 min, 5 min, 10 min, 20 min, 30 min, 1 hour, 3 hours, 24 hours, Off
Default = 5 min

File size
List box: 1 KB, 10 KB, 50 KB, 100 KB, 500 KB, 1 MB, max (~2 MB)
Default = 100 KB
Po kliknutí na tlačítko File start je záznam v souboru smazán a bude do něj kopírován monitorovací výstup. Po uplynutí času File period nebo dosažení velikosti záznamu File size (co nastane dříve), je soubor uzavřen a čeká na pozdější stažení Download. Start a stop monitoringu do souboru je nezávislý na on-line monitoringu, výstup je tedy zaznamenáván i když je on-line monitoring zastaven.

■ **Tlačítka**

Tlačítka na spodním okraji obrazovky jsou umístěna do dvou skupin:
vlevo tlačítka **Start**, **Stop**, **Clear** pro ovládání on-line monitoringu,
vpravo tlačítka **File Start**, **File Stop**, **File Status**, **Download** pro řízení záznamu do souboru.

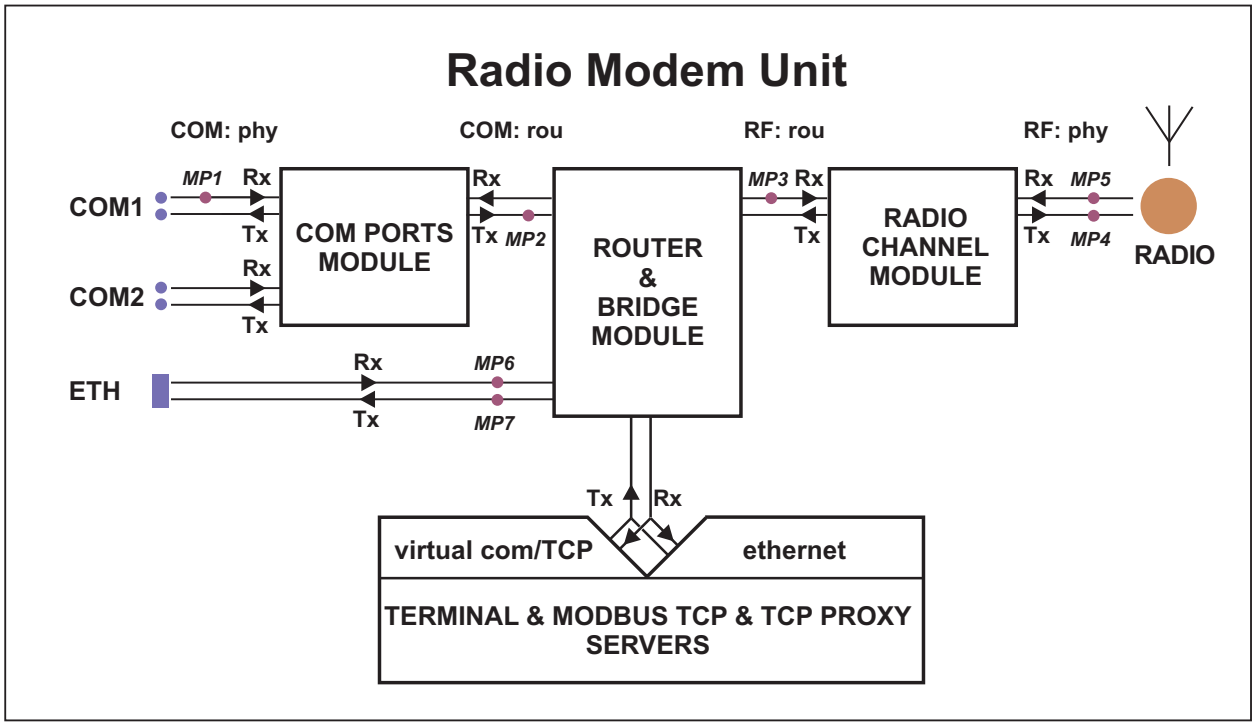
Tyto dva procesy mohou být příslušnými tlačítky kdykoli spuštěny nebo zastaveny. Aktivní je pouze jedno tlačítko z páru **Start**/**Stop** (**File Start**/**File Stop**) podle okamžitého stavu monitorovacího procesu, druhé tlačítko je šedé.

Tlačítko **Clear** smaže obrazovku on-line monitoringu i v případě, že monitoring je právě aktivní.
Tlačítko **File Status** obnoví status souboru, který je v procesu ukládání v RipEXu. Doporučuje se použít toto tlačítko kdykoli si nejsme jisti synchronizací prohlížeče se serverem v RipEXu.
Tlačítko **Download** vyvolá dialog Download File.

Při aktivaci tlačítek **Start** nebo **File Start** je použito momentální nastavení monitoringu na webové stránce. Při změně nastavení na stránce indikují tlačítka Start a File Start, že nastala změna. Zčervenají, pokud je monitoring v klidu nebo se změní v tlačítko Apply, když monotoring běží, tedy když tlačítko Start (File Start) bylo šedé. Klepnutím na Apply provedeme konfigurační změnu (např. přidáme další rozhraní) v běžícím monitorovacím procesu.

■ Popis vnitřních rozhraní

Vnitřní interface jsou rozhraní mezi moduly komunikačních kanálů a modulem centrálního routeru. Vztahy mezi nimi jsou naznačeny na schématu:



Obr. 10.3: Monitorovaná rozhraní

- **Centrální Router & Bridge Modul** pracuje jako standardní IP router nebo bridge, tedy rozhoduje na které rozhraní půjde IP paket v příštím kroku.
- **Moduly COM portů** provádí konverzi zpráv přijímaných sériovými porty na UDP datagramy a naopak.
- **Modul rádiového kanálu** zabalí (rozbalí) IP pakety do rádiového kanálu a zpracovává všechny druhy servisních rámců.
- **Terminal servery** zpracovávají zprávy z (do) virtuálních COM portů a převádí je na (z) stejné UDP datagramy jako to dělá modul COM portu.
- **Modbus TCP server** podobně zpracovává pakety protokolu Modbus TCP(RTU) - podrobnosti viz příslušné aplikační poznámky (Modbus TCP/RTU). Vzhledem k možnosti nezávislého monitorování zpráv z virtual COM a výsledných UDP datagramů, mají TSn a Modbus TCP dvě nezávislá rozhraní - rozlišují se jako (com) a (router).
- **TCP proxy** převádí TCP datagramy na UDP a přitom lokálně provádí TCP komunikaci. Dvě vnitřní rozhraní mohou být použita pro nezávislý monitoring TCP a UDP rozhraní pro (com) a (router).
- MP1, MP2, ... označení monitorovacích bodů v následujících *příkladech monitoringu*.

Příklady monitoringu

Hexadecimální data `aaaa` přicházejí portem COM1 a pak je výsledný rámec odeslám rádiovým kanálem. Monitorováno na IP adrese 192.168.141.213:

```
07:55:04.661446 [COM1:phy:Rx] length 2
        0x0000:  aaaa
07:55:04.674861 [RF:phy:Tx] (88) IP 192.168.141.213.8881>192.168.141.214.8882: UDP,length 32
        0x0000:  0800 4500 001e 0000 4000 4011 9dd2 c0a8
        0x0010:  8dd5 c0a8 8dd6 22b1 22b2 000a 72cf aaaa
```

`07:55:04.661446`	časová značka - doporučuje se synchronizovat čas v síti (např. pomocí NTP serveru) aby bylo možno analyzovat záznamy z různých jednotek
`[COM1:phy:Rx]` `(MP1)`	monitorované rozhraní - port COM1 : fyzická vrstva : zpráva přijatá z vnějšího zařízení
`length 2`	délka monitorované zprávy [byte]
`0x0000:`	pozice monitorovaného Byte, hexadecimálně
`aaaa`	monitorovaná zpráva
`07:55:04.674861`	časová značka
`[RF:phy:Tx]` `(MP4)`	monitorované rozhraní - rádiový kanál : fyzická vrstva : rámec vyslaný do antény
`(88)`	číslování Tx rámců na fyzické vrstvě
`IP 192.168.141.213.8881>`	zdrojová IP adresa a UDP číslo portu
`192.168.141.214.8882:`	cílová IP adresa a UDP číslo portu
`UDP`	typ protokolu Ethernet
`length 32`	délka monitorovaného rámce [byte]
`0x0000:`	pozice monitorovaného Byte, hexadecimálně
`0800 4500 001e 0000 4000 4011 9dd2 c0a8`	obsah monitorovaného rámce

POZNÁMKA: `(MP1)`, `(MP4)` jsou monitorované body označené v *Obr. 10.3 – „Monitorovaná rozhraní“*

Monitoring doplněný o vnitřní rozhraní. Monitorováno na IP adrese 192.168.141.213:

```
12:26:34.700971 [COM1:phy:Rx] length 2
 0x0000:  aaaa
12:26:34.701476 [COM1:rou:Tx] IP 0.0.0.0.8881 > 192.168.141.215.8882: UDP, length 0+2
 0x0000:  aaaa
12:26:34.702074 [RF:rou:Rx] IP 192.168.141.213.8881 > 192.168.141.215.8882: UDP, length 28+2
 0x0000:  4500 001e aa0f 0000 4011 33c2 c0a8 8dd5
 0x0010:  c0a8 8dd7 22b1 22b2 000a 72ce aaaa
12:26:34.734036 [RF:phy:Tx] (84) IP 192.168.141.213.8881 > 192.168.141.215.8882: UDP,len 32
 RLhead:  4e80 01ac c701 ae0f 21 ((MC:10) 10.10.10.213 > 10.10.10.214, |LN:4|P:0|A:y|R:-|)
 0x0000:  0800 4500 001e aa0f 0000 4011 33c2 c0a8
 0x0010:  8dd5 c0a8 8dd7 22b1 22b2 000a 72ce aaaa
12:26:34.748841 [RF:phy:Rx] (84) ACK, rss:52 dq:238
 RLhead:  4000 ae0f 21
```

`[COM1:phy:Rx]`	`(MP1)`	zpráva přicházející z vnějšího zařízení
`aaaa`		vstupní data
`[COM1:rou:Tx]`	`(MP2)`	paket odeslaný z modulu COM PORT do modulu ROUTER
`IP 0.0.0.0.8881 >`		zdrojový port nemá IP adresu, pouze číslo portu 8881
`192.168.141.215.8882:`		cílová IP adresa a port podle konfigurace COM portu
`aaaa`		data ve formátu vstupního protokolu (async. link)
`[RF:rou:Rx]`	`(MP3)`	paket přijatý modulem RADIO od modulu ROUTER
`IP 192.168.141.213.8881>`		zdrojová IP adresa a port
`192.168.141.215.8882:`		cílová IP adresa a port určené protokolem async.link
`length 28+2`		délka hlavičky + délka dat
`[RF:phy:Tx]`	`(MP4)`	rámec odeslaný z modulu RADIO do antény
`(84)`		interní číslování odeslaných rámců
`RLhead:`		hlavička na Rádiové Lince (zapnuto RADIO / Headers = Radio Link)
`10.10.10.213 >`		IP adresa vysílajícího **rádiového kanálu**
`10.10.10.214`		IP adresa přijímajícího **rádiového kanálu** (podle Routingové tabulky)
`[RF:phy:Rx]`	`(MP5)`	příjem potvrzujícího rámce (ACK)
`(84)`		číslo rámce ACK je shodné s číslem potvrzovaného rámce
`ACK, rss:52 dq:238`		síla signálu a kvalita dat rámce ACK

Rámec je přijatý na kanálu ETH a pak vyslaný rádiem. Monitorováno na IP adrese 192.168.141.213:

```
08:23:19.197235 [ETH] ARP, Request who-has 192.168.141.214 tell 192.168.141.212, length 46
 0x0000:  0001 0800 0604 0001 0002 a949 c067 c0a8
 0x0010:  8dd4 0000 0000 0000 c0a8 8dd6 0000 0904
 0x0020:  690f 5600 aaaa 1234 ffff ffff ffff

08:23:19.930106 [ETH] ARP, Reply 192.168.141.214 is-at 00:02:a9:ae:0b:39, length 28
 0x0000:  0001 0800 0604 0002 0002 a9ae 0b39 c0a8
 0x0010:  8dd6 0002 a949 c067 c0a8 8dd4

08:23:20.441093 [ETH] IP 192.168.141.212.8888 > 192.168.141.214.8001: UDP, length 10
 0x0000:  4500 0026 0002 4000 4011 9dc9 c0a8 8dd4
 0x0010:  c0a8 8dd6 22b8 1f41 0012 ae15 0000 0905
 0x0020:  690f 5600 aaaa 0000 0000 0000 0000

08:23:20.443997 [RF:rou:Rx] IP 192.168.141.212.8888 > 192.168.141.214.8001: UDP, length 28+10
 0x0000:  4500 0026 0002 4000 3f11 9ec9 c0a8 8dd4
 0x0010:  c0a8 8dd6 22b8 1f41 0012 ae15 0000 0905
 0x0020:  690f 5600 aaaa

08:23:20.479097 [RF:phy:Tx] (88) IP 192.168.141.212.8888 > 192.168.141.214.8001: UDP,len 40
 RLhead:  4ea0 01ac c701 ae0f 21 ((MC:10) 10.10.10.213 > 10.10.10.214, |LN:5|P:0|A:y|R:-|)
 0x0000:  0800 4500 0026 0002 4000 3f11 9ec9 c0a8
 0x0010:  8dd4 c0a8 8dd6 22b8 1f41 0012 ae15 0000
 0x0020:  0905 690f 5600 aaaa

08:23:20.493823 [RF:phy:Rx] (88) ACK, rss:50 dq:235
 RLhead:  4000 ae0f 21
```

`[ETH] ARP, Request`	`(MP6)`	přijato ARP Request
`[ETH] ARP, Reply`	`(MP7)`	vysláno ARP Reply
`[ETH] IP`	`(MP6)`	rámec přijatý z ETH zařízení
`IP 192.168.141.212.8888>`		zdrojová IP adresa a port rámce ETH
`192.168.141.214.8001:`		cílová IP adresa a port rámce ETH
`[RF:rou:Rx]`	`(MP3)`	paket přijatý modulem RADIO z modulu ROUTER
`[RF:phy:Tx]`	`(MP4)`	rámec vyslaný z modulu RADIO do antény
`IP 192.168.141.212.8888>`		zdrojová IP adresa a port, shodné s rámcem ETH
`192.168.141.214.8001:`		cílová IP adresa a port, shodné s rámcem ETH
`10.10.10.213 >`		IP adresa vysílajícího **rádiového kanálu**
`10.10.10.214`		IP adresa přijímajícího **rádiového kanálu** (podle Routingové tabulky)
`[RF:phy:Rx]`	`(MP5)`	příjem potvrzujícího rámce ACK

Interní zprávy Errors a Warning vypisované při monitoringu

Errors (červené podbarvení)

Zpráva
Význam zprávy
Monitorované rozhraní:

- Requested monitoring data missing
  Požadovaná data pro monitoring jsou nedostupná z neznámé příčiny.
  nezávisle
- RF preheader error
  "RF-preheader" je část hlavičky, která je vysílána 'nejrobustnější' modulací a je vysílána mezi synchronizační směsí a "RL-header"
  RADIO Rx
- RL header CRC error
  "RL-header" je hlavička protokolu Rádiové Linky
  RADIO Rx
- Bridge stream datablock header CRC error
  "Bridge stream DB-header" je hlavička tzv. Data bloku vysílaného ve Stream módu (Bridge).
  RADIO Rx, Bridge
- Data CRC error
  Chyba kontrolního součtu dat.
  RADIO Rx

Warnings (žluté podbarvení)

- Record sequence problem – reconfiguration?
  Detekován problém v pořadí záznamu - pravděpodobně došlo k rekonfiguraci systému (tj. změna v uživatelských konfiguracích - Settings/Routing).
  nezávisle
- Record sequence problem. Some records may be lost.
  Detekován problém v pořadí záznamu - příčina není známá - pravděpodobně došlo ke ztrátě jednoho nebo více záznamů.
  nezávisle
- [x] missing record(s) detected
  Detekce 'x' chybějících záznamů (ve výpisu je [x] nahrazeno konkrétním číslem).
  nezávisle
- Monitoring restarted. Some records may be lost.
  Systém monitoringu byl restartován (např. v důsledku změny konfigurace monitoringu). Některé záznamy se mohly ztratit.
  nezávisle
- ETH monitoring terminated. Invalid tcpdump parameters?
  Bylo předčasně ukončeno monitorování ETH rozhraní. Pravděpodobně z důvodu zadání chybných nebo nepovolených uživatelských parametrů programu 'tcpdump' (položka Advanced parameters/User rule).
  ETH
- Interface not ready!
  RF interface není připraven. Může nastat pri startu systému po bootu, nebo rekonfiguraci, nebo při rekalibraci rádiové části (k té dochází pravidelně po 'x' dnech, nebo při změně teploty o 'y' °C). Rámec je zahozen.
  RADIO Tx
- RF interface not ready!

RF interface není připraven. Může nastat pri startu systému po bootu, nebo rekonfiguraci, nebo při rekalibraci rádiové části (k té dochází pravidelně po 'x' dnech, nebo při změně teploty o 'y' °C). Rámec je zahozen.

Internal RADIO Tx

- Interface not ready - high radio board temperature!
  RF interface není připraven v důsledku vysoké teploty radiomodemu (95 °C). Rámec je zahozen.
  RADIO Tx
- RF interface not ready - high radio board temperature!
  RF interface není připraven v důsledku vysoké teploty radiomodemu (95 °C). Rámec je zahozen.
  Internal RADIO Tx
- Frame reception cancelled
  Byl přerušen proces příjmu rámce.
  RADIO Rx
- Duplicated frame
  Detekován duplikovaný rámec. Rámec je zahozen.
  RADIO Rx
- Queue full
  Fronty 'do vzduchu' jsou zaplněny a byl přijat požadavek na vysílání rámce. Rámec je zahozen.
  RADIO Tx
- Incompatible frame?
  Přijat nekompatibilní rámec. Příčin hlášení může být více - např.: foreign RL-protocol, unknown RLP packet type, unknown RLP packet group, unknown service, incorrect ETH frame, unsupported IP frame type, ...
  RADIO Rx i Tx
- ACK
  Přijat neočekávaný ACK.
  RADIO Rx
- Can't decrypt - configuration problem?
  Nelze provést dekryptování rámce. Pravděpodobně kvůli chybné konfiguraci (chybný AES klíč).
  RADIO Rx i Tx
- Can't decrypt
  Nelze provést dekryptování rámce.
  RADIO Rx i Tx
- Can't decompress
  Nelze provést dekomprimaci rámce. (Komprese se provádí automaticky a může být vypnuta pouze v CLI).
  RADIO Rx i Tx
- Bridge mode frame
  Byl přijat rámec v "Bridge" formátu ale zařízení je nakonfigurováno do "Router" módu.
  RADIO Rx
- Stream mode frame
  Byl přijat rámec v "Bridge-stream" formátu, ale zařízení není nakonfigurováno do "Bridge" módu nebo není nakonfigurovaná položka "Frame closing"=Stream.
  RADIO Rx
- Router mode frame
  Byl přijat rámec ve formátu "Router" ale zařízení je nakonfigurováno do módu "Bridge".
  RADIO Rx

11. Bezpečnost, životní prostředí, licence

11.1. Kmitočet

Rádiový modem musí být provozován na kmitočtech v souladu s platným povolením vydaným národním telekomunikačním úřadem. Všechny rádiové parametry musí být nastaveny přesně podle tohoto povolení.

Důležité

Použití kmitočtů 406.0 až 406.1 MHz je vyhrazeno celosvětově pouze pro Mezinárodní satelitní vyhledávací a záchranný systém (International Satellite Search and Rescue System). Tyto frekvence jsou používány nouzovými majáky a jsou neustále monitorovány pozemním a satelitním systémem Cospas-Sarsat. Jiné použití těchto kmitočtů je zakázáno.

11.2. Bezpečná vzdálenost

Nezdržujte se v těsné blízkosti antény, pokud je radiomodem zapnutý. Bezpečná vzdálenost pro intenzitu elektromagnetického pole je uvedena v následující tabulce. Vzdálenosti platí pro výkon 10 W. Podrobněji v návodu na *http://www.racom.eu/download/hw/ripex/free/cz/ripex-m-en.pdf*

Tab. 11.1: Minimální bezpečná vzdálenost

	Zisk antény		
	5 dBi	10 dBi	15 dBi
160 MHz	2 m	3 m	5 m
300 and 400 MHz	2 m	2 m	4 m

11.3. Vysoká teplota

Jestliže RipEX pracuje v prostředí, kde okolní teplota přesahuje 55 °C, pak RipEX musí být instalován na místě s omezeným přístupem, aby bylo zabráněno kontaktu lidí s povrchem chladiče.

11.4. Dodržení směrnic RoHS a WEEE

Výrobek splňuje směrnici 2011/65/EU o omezení používání některých nebezpečných látek v elektrických a elektronických zařízeních (RoHS 2) a směrnici 2012/19/EU o odpadních elektrických a elektronických zařízeních (OEEZ, WEEE).

RoHS Zákaz nebezpečných látek (RoHS)

Směrnice Předpis RoHS zakazuje v EU prodej elektronických zařízení s obsahem těchto nebezpečných látek: olovo, kadmium, rtuť, šestimocný chróm, polybromované bifenyly (PBBs) a polybromované difenylethery (PBDEs).

Recyklační program (OEEZ)

Směrnice OEEZ se týká obnovy, opakovaného využití a recyklace elektronických a elektrických zařízení. Podle směrnice musí být použité zařízení správně označeno, roztříděno a likvidováno. RACOM inicioval program pro správu recyklace odpadu ekologicky bezpečným způsobem pomocí postupů v souladu se směrnicí OEEZ.

Likvidace baterií

Výrobek může obsahovat baterie. Baterie musí být náležitě likvidovány, nesmí být v EU odkládány jako netříděný komunální odpad. Baterie jsou označeny symbolem, který může obsahovat znaky k označení kadmia (Cd), olova (Pb) nebo rtuti (Hg). Pro správnou recyklaci vraťte baterie vašemu dodavateli nebo na označené sběrné místo.

11.5. Podmínky a instrukce pro bezpečný provoz zařízení

Čtěte pozorně tato bezpečnostní opatření před použitím výrobku:

- Odpovědnost za vady se nevztahuje na výrobek, který byl použit v rozporu s instrukcemi uvedenými v návodu k obsluze, nebo pokud bylo otevřeno pouzdro, v němž je rádiový modem umístěn, nebo když byl proveden neodborný zásah do zařízení.
- Rádiový modem smí být provozován pouze na frekvencích, které jsou k tomu určeny orgánem pověřeným správou rádiového provozu v příslušné zemi a nesmí překročit maximální povolený výstupní výkon. Firma RACOM není zodpovědná za výrobky používané nedovoleným způsobem.
- Zařízení uvedená v tomto návodu k obsluze mohou být použita pouze v souladu s instrukcemi uvedenými v tomto návodu. Bezchybný a bezpečný provoz tohoto zařízení je zaručen pouze při náležité přepravě, skladování, provozu a ovládání těchto zařízení. Totéž platí i pro jejich údržbu.
- Pro prevenci škod na rádiové jednotce a ostatních koncových zařízeních musí být při odpojování nebo připojování kabelu k datovému rozhraní jednotky vždy odpojeno její napájení. Je třeba zajistit, aby různá zařízení byla uzemněna na stejný potenciál.
- Zařízení smí opravovat pouze výrobce.
- Bude-li jednotka RAy použita s jiným než doporučeným příslušenstvím, výrobce nepřijímá odpovědnost za vady, které byly tímto příslušenstvím způsobeny.

11.6. Důležitá upozornění

Výhradním vlastníkem všech práv k tomuto návodu k obsluze je firma RACOM s. r. o. (dále v tomto návodu uváděná pod zkráceným názvem RACOM). Všechna práva vyhrazena. Pořizování písemných, tištěných či kopírovaných kopií tohoto manuálu nebo záznamů na různá média nebo překlad jakékoliv části tohoto manuálu do jiných jazyků (bez písemného svolení vlastníka práv) je zakázáno.

RACOM si vyhrazuje právo na změny v technické specifikaci nebo ve funkci tohoto produktu nebo na ukončení výroby tohoto produktu nebo na ukončení jeho servisní podpory bez předchozího písemného upozornění zákazníků.

Podmínky použití software tohoto produktu se řídí licencí, která je uvedena níže. Program šířený s touto licencí je uvolněn se záměrem, že bude užitečný, ale bez konkrétní záruky. Za žádných okolností

není autor nebo jiná firma či osoba zodpovědná za vedlejší, náhodné nebo související škody, které vyplývají z použití tohoto produktu.

Výrobce neposkytuje uživateli žádnou formu záruky obsahující ujištění o vhodnosti a použitelnosti pro jeho aplikaci.Výrobky firmy RACOM nejsou vyvíjeny, určeny ani zkoušeny pro použití v zařízeních, která přímo ovlivňují zdraví a životní funkce lidí a zvířat, a to ani jako součást jiného důležitého zařízení, a neposkytuje záruky, pokud je výrobek firmy použit v těchto zmíněných zařízeních.

RACOM Open Software License

Verze 1.0, listopad 2009

Každý má možnost kopírovat a šířit doslovné kopie této licence, ale jakákoli změna není povolena.

Program (binární verze) je dostupný zdarma na kontaktech uvedených na http://www.racom.eu. Tento produkt obsahuje open source nebo jiný software pocházející od třetích stran, který podléhá GNU General Public License (GPL), GNU Library / Lesser General Public License (LGPL) a / nebo dalších autorských licencí, prohlášení o vyloučení odpovědnosti a upozornění. Přesné znění GPL, LGPL a některých dalších licencí je uvedeno v balících zdrojového kódu (typicky soubory COPYING nebo LICENSE). Příslušné strojově čitelné kopie zdrojového kódu tohoto softwaru pod GPL nebo LGPL licencemi můžete získat na kontaktech uvedených na http://www.racom.eu. Tento produkt také obsahuje software vyvinutý na University of California, Berkeley a u jejích přispěvatelů.

11.7. Odpovědnost za vady

RACOM s.r.o. odpovídá u svých výrobků za vady po dobu uvedenou v dodací dokumentaci, doba začná plynout od okamžiku doručení výrobku zákazníkovi. Během této doby provede RACOM podle vlastního uvážení opravu nebo výměnu vadného zařízeni, vždy však za předpokladu, že k poruše došlo při běžném používání v souladu s návodem k použití, ne v důsledku nesprávného použití, ať už úmyslného nebo nahodilého, např. pokusem o opravu nebo úpravu neoprávněnou osobou nebo v důsledku působení abnormálních vlivů prostředí, jako je například přepětí, zaplavení nebo úder blesku.

Vadný výrobek, na nějž se vztahuje odpovědnost za vady, bude na náklady zákazníka dopraven do provozovny společnosti RACOM. Opravené zařízení bude zákazníkovi vráceno na náklady společnosti RACOM. V případě, že okolnosti neumožňují výrobek demontovat a doručit do provozovny společnosti RACOM, zákazník uhradí výdaje, které společnosti RACOM vznikly při dopravě a opravě a/nebo výměně na místě.

Tato záruční ustanovení představují plný rozsah záručního krytí firmy RACOM vůči zákazníkovi dohodou, která je mezi oběma stranami dobrovolně uzavřena.

RACOM poskytuje záruku, že zařízení bude fungovat náležitě, jak je popsáno, bez závazku, že se bude hodit pro zákazníkův záměr nebo účel. Za žádných okolností odpovědnost společnosti RACOM nepřesahuje výše uvedené, přičemž RACOM, jeho jednatelé, zaměstnanci nebo zástupci nejsou odpovědni za žádné vzniklé ztráty nebo škody způsobené přímo či nepřímo použitím, zneužitím, provozem či selháním zařízení, vyjma zákonné ochrany, která se může výslovně a nevyhnutelně k věci vztahovat.

11.8. EU prohlášení o shodě

RACOM
www.racom.eu

EU PROHLÁŠENÍ O SHODĚ

Typ rádiového zařízení	**RipEX-160** **RipEX-300** **RipEX-400**	**Rádio SW** SDDR ver. 0.24.0.57 Driver ver. 0.5.19.0
Výrobce	**RACOM s.r.o.** **Mírová 1283, 592 31 Nové Město na Moravě**	

Toto prohlášení o shodě se vydává na výhradní odpovědnost výrobce.

Výše uvedené rádiové zařízení je ve shodě se Směrnicí 2014/53/EU Evropského parlamentu a Rady o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES.

Harmonizované normy použité k prokázání shody:

Spektrum	EN 300 113-2 V1.5.1 EN 302 561 V1.3.2
EMC	EN 301 489-1 V1.9.2 EN 301 489-5 V1.3.1
Bezpečnost	EN 60950-1:2006, A11:2009, A1:2010, A12:2011, A2:2013

Podepsáno za a jménem výrobce:

Nové Město na Moravě, 14. března 2017
Jiří Hruška, generální ředitel

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

ver. 1.1

Obr. 11.1: EU prohlášení o shodě

Rejstřík

U

V

Z

Ž

Příloha A. Přehled revizí

Revize 1.1 2011-09-26
První XML verse podle anglického návodu

Revize 1.2 2013-01-14
Doplnění tabulek pro povolení ČTU

Revize 1.3 2016-02-19
Aktualizace tech param

Revize 1.4 2016-03-07
Přidány kapitoly *5 – „Záložní trasy“* a *7 – „ARP Proxy a VLAN“*

Revize 1.5 2016-05-25
Přidány kapitoly *1 – „RipEX podrobně“*, *4 – „Instalace zařízení“*, *8 – „SNMP“* a *11 – „Bezpečnost, životní prostředí, licence“*
Změna formátu dokumentu na „book“

Revize 1.6 2016-06-20
Přidána kapitola *Konektory*

Revize 1.7 2017-03-15
Doplnění informací o *zabezpečení* a *napájení*.

Revize 1.8 2017-06-13
EU *prohlášení o shodě*

Revize 1.9 2017-06-15
Přidány kapitoly *Ping* a *Monitoring*.

Revize 1.10 2017-08-22
Přidány kapitoly *IPsec* a *GRE*.
Doplněna informace *Base driven* protokol.