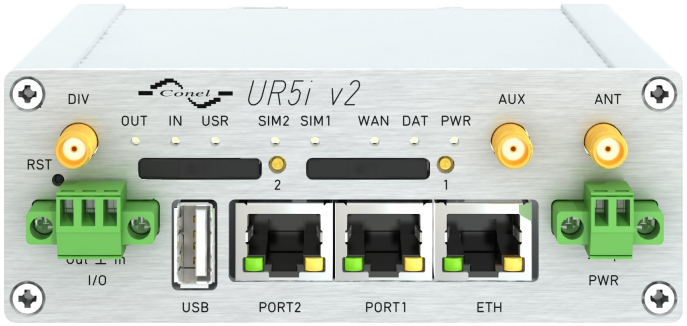
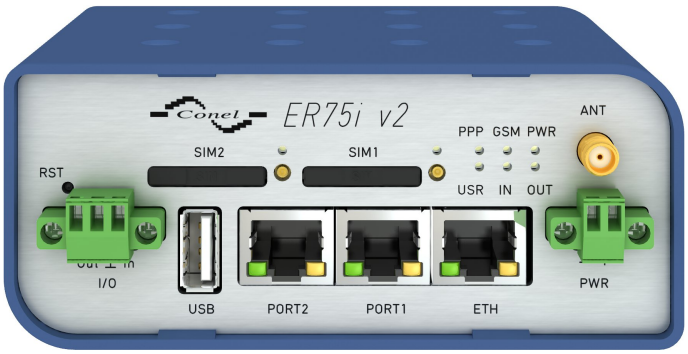
A B&B ELECTRONICS Company

KONFIGURAČNÍ MANUÁL

pro v2 routery





Použité symboly

Nebezpečí – důležité upozornění, které může mít vliv na bezpečí osoby nebo funkčnost přístroje.

Pozor – upozornění na možné problémy, kterým může dojít ve specifických případech.

Informace, poznámka – informace, které obsahují užitečné rady, nebo zajímavé poznámky.

Firmware version

Aktuální verze firmware popsaného v manuálu je 3.0.8 (30.8.2013).

GPL licence

Zdrojové kódy, na které se vztahuje GPL licence, jsou dostupné bez poplatku po zaslání žádosti na adresu:

info@conel.cz.

Verze routerů

Vlastnosti a nastavení routeru spojené s GSM spojením nejsou k dispozici v průmyslovém routeru XR5i v2.

Položka PPPoE configuration je k dispozici pouze u průmyslového routeru XR5i v2, slouží pro nastavení PPPoE spojení po ethernetu.

Conel s.r.o., Sokolská 71, 562 04 Ústi nad Orlicí, Česká Republika
Manuál vydán v ČR, 20. září 2013

Obsah

Seznam obrázků

Seznam tabulek

1. Konfigurace přes webový prohlížeč

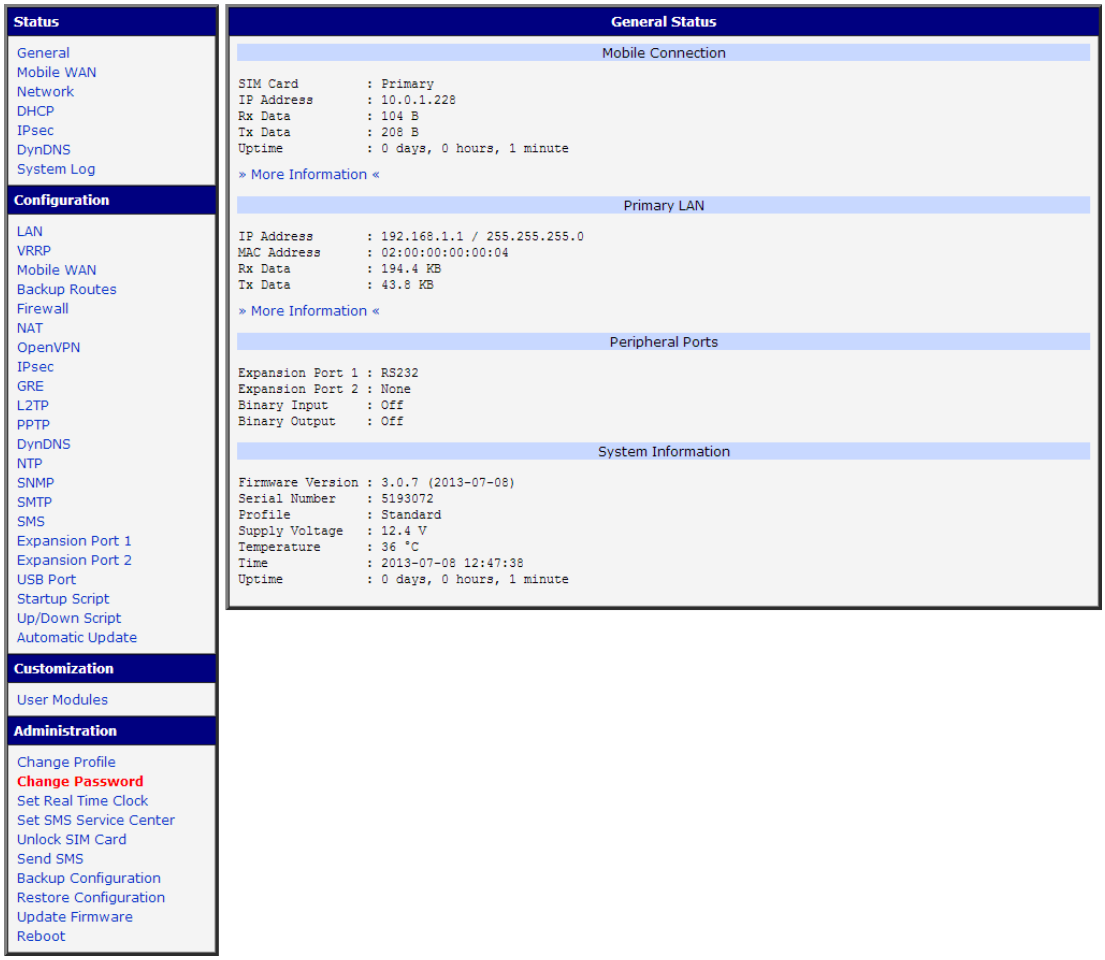
Pozor! Bez vložené SIM karty, nebudou fungovat bezdrátové přenosy. Vložená SIM karta musí mít aktivované přenosy přes technologie používané vašim routerem.

Pro sledování stavu, konfiguraci a správu routeru je k dispozici webové rozhraní, které lze vyvolat zadáním IP adresy routeru do webového prohlížeče. Výchozí IP adresa routeru je 192.168.1.1. Konfiguraci může provádět pouze uživatel „root“ s výchozím heslem „root“.

V levé části webového rozhraní je umístěno menu s nabídkou stránek pro sledování stavu (*Status*), konfiguraci (*Configuration*), správu uživatelských modulů (*Customization*) a správu (*Administration*) routeru. Jednotlivé položky se zobrazují vedle menu.

Název routeru je zobrazen podle typu vašeho routeru. Položky *Name* a *Location* zobrazují jméno a umístění routeru vyplněnou v SNMP konfiguraci (viz SNMP Configuration).

Pro vyšší bezpečnost sítě spravované routerem je nutné změnit výchozí heslo routeru. Je-li v routeru nastaveno výchozí heslo, položka ***Change password*** je červeně zvýrazněná.



Obrázek 1: Webová konfigurace

Po rozblikání PWR LED na předním panelu je možné obnovit výchozí nastavení routeru stisknutím tlačítka RST na předním panelu. Po stisku tlačítka RST se provede reset routeru – obnovení konfigurace a následný reboot routeru (zelená LED se rozsvítí).

1.1 Zabezpečený přístup do webové konfigurace

Do webové konfigurace lze přistoupit i pomocí zabezpečeného protokolu HTTPS.

V případě routeru s výchozí IP adresou se k zabezpečené konfiguraci routeru přistupuje zadáním adresy https://192.168.1.1 do webového prohlížeče. Při prvním přístupu je potřeba nainstalovat bezpečnostní certifikát. Jestliže prohlížeč hlásí neshodu v doméně je k odstranění tohoto hlášení možné použít následující postup.

Jelikož jméno domény v certifikátu je uvedena MAC adresa routeru (jako oddělovače jsou použity pomlčky místo dvojteček), je potřeba přistupovat k routeru pod tímto doménovým jménem. Možnosti tohoto přístupu lze docílit přidáním DNS záznamu do DNS tabulky operačního systému.

- Upravením /etc/hosts (Linux/Unix)
- Upravením C:\WINDOWS\system32\drivers\etc\hosts (Windows XP)
- Nastavením DNS serveru

Dále ke konfiguraci routeru s MAC adresou 00:11:22:33:44:55 se k zabezpečené konfiguraci routeru přistupuje zadáním adresy https://00-11-22-33-44-55 do webového prohlížeče. Při prvním přístupu je potřeba nainstalovat bezpečnostní certifikát.

Při použití vlastního podpisového certifikátu se musí nahrát soubory http_cert a http_key do adresáře /etc/certs v routeru.

1.2 General (Úvodní stránka)

Souhrn základních informací o routeru a jeho činnosti lze vyvolat volbou položky *General*. Tato stránka se také zobrazí po přihlášení do webového rozhraní. Informace jsou rozděleny do několika samostaných bloků dle typu činnosti routeru či oblasti vlastností – *Mobile Connection*, *Primary LAN*, *Peripherals Ports* a *System Information*. Je-li router osazen volitelným portem WIFI, je k dispozici také sekce *WIFI*.

1.2.1 Mobile Connection

Položka	Poips
SIM Card	Identifikace SIM karty (*Primary* nebo *Secondary*)
Interface	Definuje síťové rozhraní
IP Address	IP adresa daného síťového rozhraní

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Poips
MTU	Maximální velikost paketu, kterou je prvek schopen přenášet
Rx Data	Celkový počet přijatých bytů
Rx Packets	Přijaté pakety
Rx Errors	Chybné příchozí pakety
Rx Dropped	Zahozené příchozí pakety
Rx Overruns	Ztracené příchozí pakety z důvodu přetížení
Tx Data	Celkový počet odeslaných bytů
Tx Packets	Odchozí pakety
Tx Errors	Chybné odchozí pakety
Tx Dropped	Zahozené odchozí pakety
Tx Overruns	Ztracené odchozí pakety z důvodu přetížení
Uptime	Doba, po kterou je sestavené spojení na mobilní síti

Tabulka 1: Mobile connection

1.2.2 Primary LAN

Položky zobrazené v této části mají stejný význam jako položky v části předchozí. Navíc je zde informace o MAC adrese daného routeru (položka *MAC Address*).

1.2.3 Peripheral Ports

Položka	Popis
Expansion Port 1	Volitelný port osazený na pozici 1 (pokud je uvedeno *None*, není osazen žádný port)
Expansion Port 2	Volitelný port osazený na pozici 2 (pokud je uvedeno *None*, není osazen žádný port)
Binary Input	Stav binárního vstupu
Binary Output	Stav binárního výstupu

Tabulka 2: Peripheral Ports

1.2.4 System Information

Položka	Poips
Firmware Version	Informace o verzi firmware
Serial Number	Sériové číslo daného routeru (v případě *N/A* není dostupné)

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Poips
Profile	Aktuální profil – standard nebo alternativní profily (využívají se například pro přepínání mezi různými režimy provozu routeru)
Supply Voltage	Napájecí napětí routeru
Temperature	Teplota v routeru
Time	Aktuální datum a čas
Uptime	Doba, po kterou je router v provozu

Tabulka 3: System Information

1.3 Mobile WAN status

U průmyslového routeru XR5i v2 není tato položka k dispozici.

Položka *Mobile WAN* v hlavním menu obsahuje aktuální informace o připojení k mobilní síti. V první části této stránky (*Mobile Network Information*) jsou uvedeny základní informace o mobilní síti, ve které je daný router provozován. K dispozici jsou také informace o modulu osazeném v tomto routeru.

Položka	Poips
Registration	Stav registrace sítě
Operator	Specifikuje operátora, v jehož síti je router provozován
Technology	Přenosová technologie
PLMN	Kód operátora
Cell	Buňka na kterou je router připojen
LAC	Location Area Code – unikátní číslo příslušné základnové stanice
Channel	Kanál na kterém router komunikuje
Signal Strength	Síla signálu vybrané buňky
Signal Quality	Kvalita signálu vybrané buňky: • EC/IO pro technologie UMTS a CDMA (Jedná se o poměr přijímaného signálu z pilotního kanálu – EC – vůči celkové úrovni spektrální hustoty, tj. vůči součtu signálů ostatních buněk – IO.) • RSRQ pro technologii LTE (Definováno jako podíl $\frac{N \times RSRP}{RSSI}$) • Pro technologii EDGE (router ER75i v2) není hodnota dostupná
Neighbours	Kvalita signálu sousedních slyšitelných buněk
Manufacturer	Výrobce modulu
Model	Typ modulu

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Poips
Revision	Verze osazeného modulu
IMEI	IMEI (International Mobile Equipment Identity) modulu
ESN	ESN (Electronic Serial Number) modulu (pro CDMA routery)

Tabulka 4: Mobile Network Information

Červeně zvýrazněné sousední buňky mají blízkou kvalitu signálu, tudíž hrozí časté přepínání mezi aktuální a zvýrazněnou buňkou.

V další části tohoto okna jsou zobrazovány statistiky o kvalitě spojení za jednotlivá období.

Období	Popis
Today	Dnešní den v intervalu 0:00 až 23:59
Yesterday	Včerejší den v intervalu 0:00 až 23:59
This week	Tento týden v intervalu pondělí 0:00 až neděle 23:59
Last week	Minulý týden v intervalu pondělí 0:00 až neděle 23:59
This period	Toto účtovací období
Last period	Minulé účtovací období

Tabulka 5: Popis jednotlivých období

Položka	Popis
Signal Min	Minimální síla signálu
Signal Avg	Průměrná síla signálu
Signal Max	Maximální síla signálu
Cells	Počet přepnutí mezi buňkami
Availability	Dostupnost routeru přes mobilní síť

Tabulka 6: Mobile Network Statistics

Tipy pro tabulku *Mobile Network Statistics*:

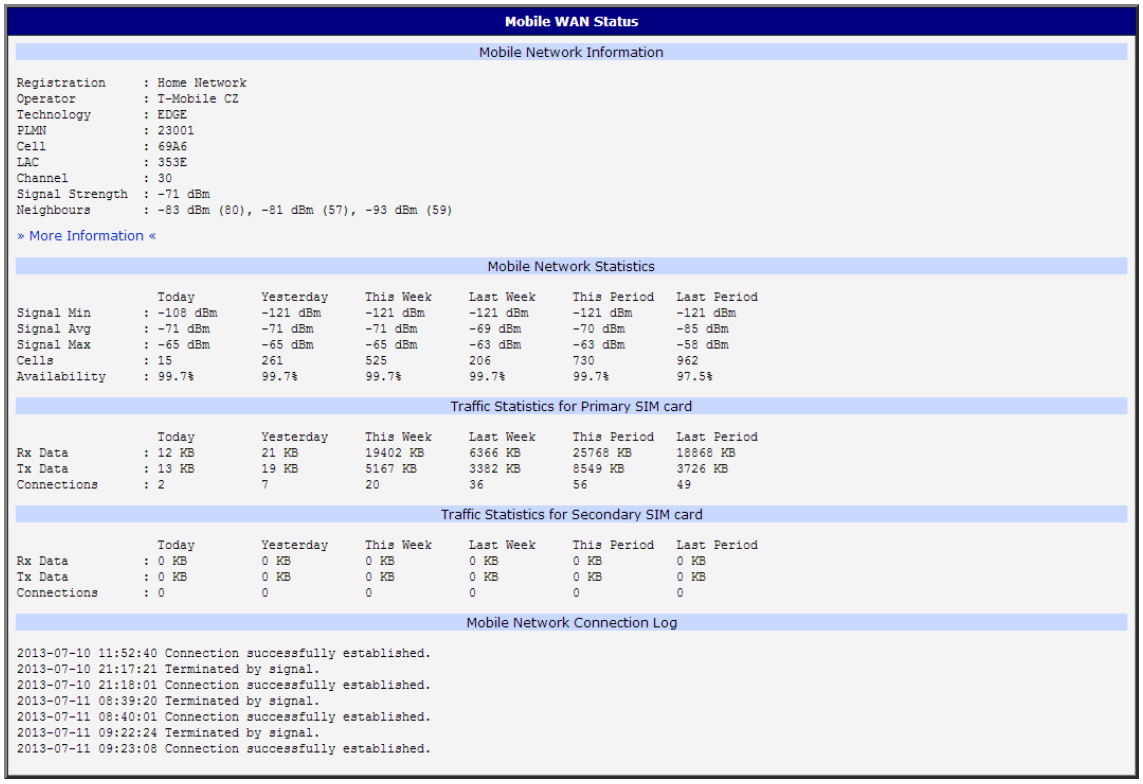
- Dostupnost spojení do mobilní sítě je údaj v procentech, který je počítán poměrem času navázaného spojení do mobilní sítě vůči času, kdy je router zapnutý.
- Po najetí kurzorem na hodnoty maximální nebo minimální síly signálu se zobrazí poslední čas, kdy této síly signálu router dosáhl.

Ve střední části okna jsou zobrazeny statistky popisující stav přenesených dat jednotlivých SIM karet v daných období.

Položka	Popis
RX data	Celkový objem přijatých dat
TX data	Celkový objem odeslaných dat
Connections	Počet sestavení spojení do mobilní sítě

Tabulka 7: Traffic statistics

Ve spodní části okna jsou zobrazovány informace o sestavení spojení a případných problémech při jeho sestavování (*Mobile Network Connection Log*).



Obrázek 2: Mobile WAN status

1.4 Síťové informace

Síťové informace o provozu routeru lze vyvolat volbou položky *Network* v menu. V dolní části okna je zobrazena informace o routovací tabulce. V horní části okna jsou zobrazeny podrobné informace o aktivních síťovéhých rozhraních:

Rozhraní	Popis
eth0, eth1	Síťová rozhraní
ppp0	PPP rozhraní (aktivní připojení do GPRS/EDGE/UMTS)
tun0	Rozhraní OpenVPN tunelu
ipsec0	Rozhraní IPsec tunelu
gre1	Rozhraní GRE tunelu
usb0	Rozhraní konektoru USB

Tabulka 8: Popis rozhranní network status

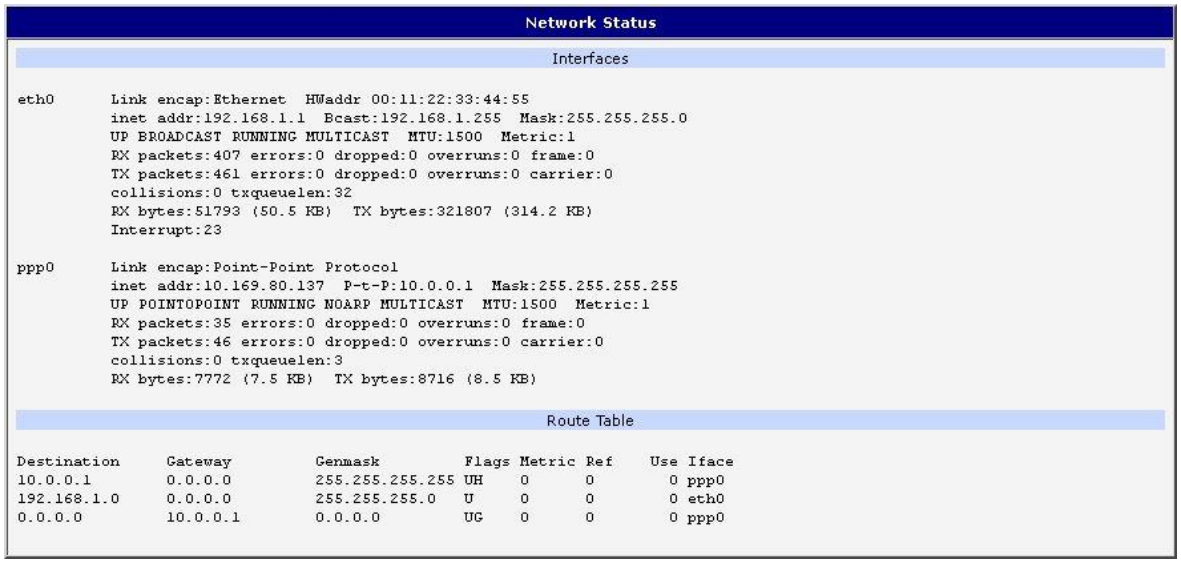
U každého rozhraní jsou pak zobrazeny následující informace:

Položka	Popis
HWaddr	Hardwarová (MAC) adresa síťového rozhraní
inet	Vlastní IP adresa rozhranní
P-t-P	IP adresa druhého konce spojení
Bcast	Všesměrová adresa
Mask	Maska sítě
MTU	Maximální velikost paketu, kterou je prvek schopen přenášet
Metric	Počet směrovačů, přes které musí paket projít
RX	• packets – přijaté pakety • errors – chybné příchozí pakety • dropped – zahozené příchozí pakety • overruns – ztracené příchozí pakety z důvodu přetížení • frame – chybné příchozí pakety z důvodu chybné velikosti paketu
TX	• packets – odchozí pakety • errors – chybné odchozí pakety • dropped – zahozené odchozí pakety • overruns – ztracené odchozí pakety z důvodu přetížení • carrier – chybné odchozí pakety s chybou vzniklou na fyzické vrstvě
collisions	Počet kolizí na fyzické vrstvě
txqueuelen	Délka fronty síťového zařízení
RX bytes	Celkový počet přijatých bytů
TX bytes	Celkový počet odeslaných bytů

Tabulka 9: Popis informací network status

Ze síťových informací je možné vyčíst stav spojení do mobilní sítě. Když je spojení do mobilní sítě aktivní, je v systémových informacích zobrazeno rozhraní ppp0.

U průmyslového routeru XR5i v2 rozhranní ppp0 označuje připojení přes PPPoE spojení.



Obrázek 3: Network status

1.5 DHCP status

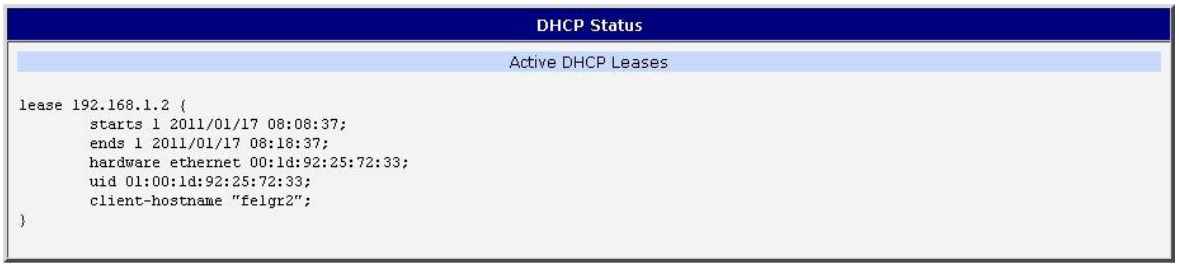
Informace o činnosti DHCP serveru lze vyvolat volbou položky *DHCP status*. DHCP server zajišťuje automatickou konfiguraci zařízení připojených do sítě spravované routerem. DHCP server přiděluje jednotlivým zařízením IP adresu, masku sítě, výchozí bránu (IP adresu routeru) a adresu DNS serveru (IP adresu routeru).

Pro každou konfiguraci jsou v okně DHCP status zobrazeny následující informace.

Položka	Popis
lease	Přidělená IP adresa
starts	Čas přidělení IP adresy
ends	Čas ukončení platnosti přidělené IP adresy
hardware ethernet	Hardwarová (MAC) adresa
uid	Unikátní ID
client-hostname	Název počítače

Tabulka 10: Popis informací DHCP status

V krajním případě může DHCP status zobrazit k jedné IP adrese dva DHCP statusy, příčinou toho může být resetování síťové karty.

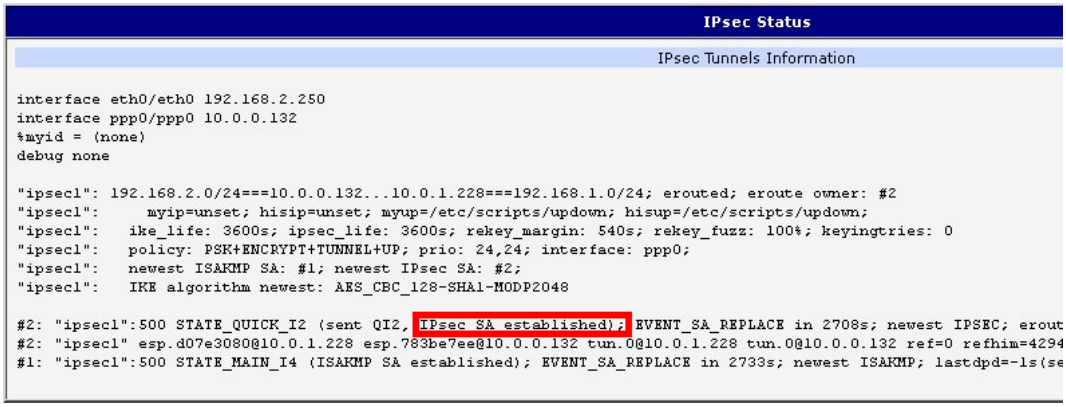


Obrázek 4: DHCP status

1.6 IPsec status

Informace o aktuálním stavu IPsec tunelu lze vyvolat volbou položky *IPsec* v menu.

Po správném sestavení IPsec tunelu se v *IPsec status* zobrazí informace *IPsec SA established* (červeně zvýrazněné). Ostatní informace mají pouze interní charakter.



Obrázek 5: IPsec status

1.7 DynDNS status

Výsledek aktualizace DynDNS záznamu na serveru www.dyndns.org lze vyvolat volbou položky *DynDNS* v menu.

Obrázek 6: DynDNS status

Při zjišťování stavu aktualizace jsou možné následující hlášení:

- DynDNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed yet.
- DynDNS record is already up to date.
- DynDNS record successfully update.
- DNS error encountered.
- DynDNS server failure.

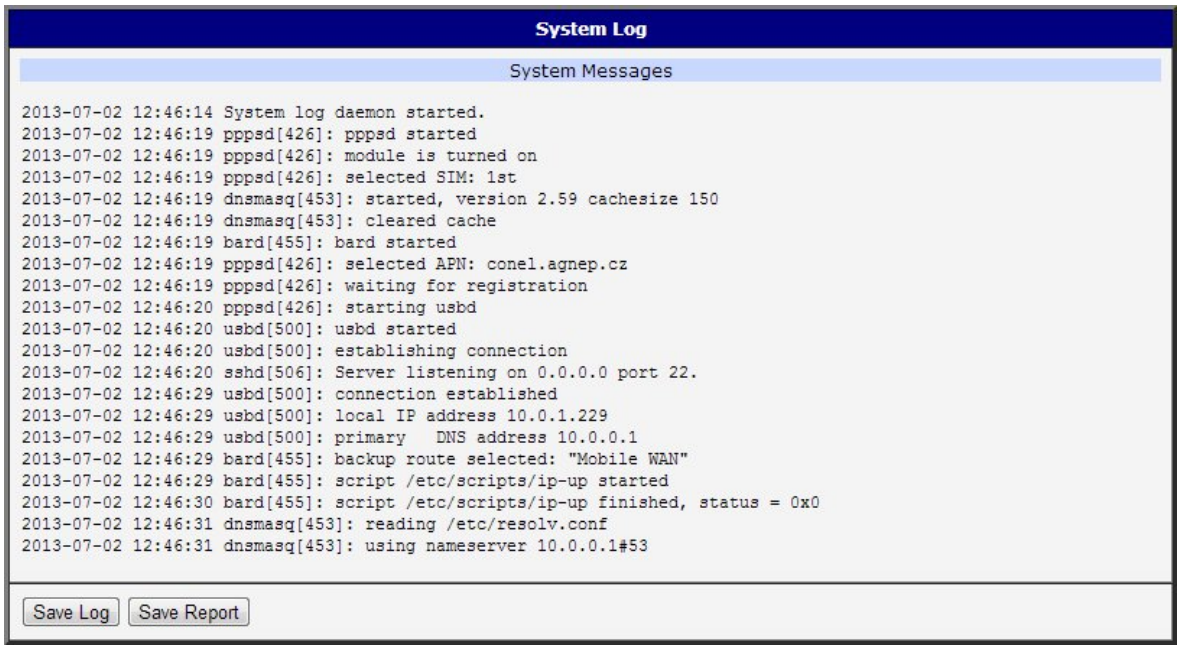
Pro správnou funkci DynDNS musí mít SIM karta routeru přiřazenou veřejnou IP adresu.

1.8 Systémový log

V případě problémů s PPP připojením lze vyvolat systémový log volbou položky *System Log* v menu. V okně jsou zobrazena podrobná hlášení od jednotlivých aplikací běžících v routeru. Pomocí tlačítka *Save Log* je možné systémový log uložit do připojeného počítače. Druhé tlačítko – *Save Report* – slouží k vytvoření reportu (jeden soubor obsahující všechny informace potřebné pro technickou podporu).

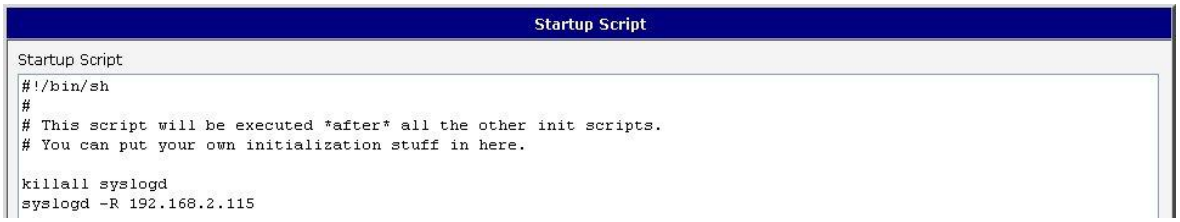
Defaultní velikost systémového logu je 1000 řádků. Po dovršení 1000 řádků se vytvoří nový soubor pro ukládání systémového logu. Po dovršení 1000 řádků v druhém souboru se maže první soubor a vytvoří se místo něho nový.

Program Syslogd může být spuštěn s dvěma volbami, které upravují jeho chování. Volba ve tvaru *-s* následovaná desítkovým číslem nastavuje maximální počet řádků systémového logu. Volba *-r* následovaná IP adresou umožňuje přihlášení do vzdáleného démona syslog. V případě Linuxu musí být na cílovém počítači povoleno vzdálené logování. Typicky spuštěním programu syslogd s volbou -r. Na Windows musí být nainstalován syslog server (např. Syslog Watcher). Aby se program Syslogd spouštěl s těmito volbami, je nutné upravit skript */etc/init.d/syslog* nebo přidat řádky *killall syslogd* a *syslogd <options> &* do startup skriptu (viz konfigurace *Startup Script*).



Obrázek 7: Systémový log

Příklad logování do vzdáleného démona na adrese 192.168.2.115



Obrázek 8: Příklad spuštění programu syslogd s volbou -r

1.9 Konfigurace síťového rozhraní

Konfiguraci síťového rozhraní lze vyvolat volbou položky *LAN* v menu. Síť s označením *Primary LAN* je pro rozhraní routeru ETH, *Secondary LAN* lze použít pouze ve verzi s volitelným ethernetovým portem.

Položka	Popis
DHCP Client	• disabled – Router nemá povoleno automatické přidělení IP adresy od DHCP serveru v síti LAN • enabled – Router má povoleno automatické přidělení IP adresy od DHCP serveru v síti LAN
IP address	Pevně nastavená IP adresa síťového rozhraní ETH routeru
Subnet Mask	Maska sítě
Bridged	• no – Router nemá aktivován režim bridge (výchozí hodnota) • yes – Router má aktivován režim bridge
Media type	• Auto-negation – Router zvolí rychlost komunikace dle možností sítě • 100 Mbps Full Duplex – Router komunikuje rychlostí 100 Mbps v režimu současné obousměrné komunikace • 100 Mbps Half Duplex – Router komunikuje rychlostí 100 Mbps v režimu střídavé obousměrné komunikace • 10 Mbps Full Duplex – Router komunikuje rychlostí 10 Mbps v režimu současné obousměrné komunikace • 10 Mbps Half Duplex – Router komunikuje rychlostí 10 Mbps v režimu střídavé obousměrné komunikace
Default Gateway	Výchozí brána routeru. Při zadání IP adresy výchozí brány se všechny pakety pro které nebyl nalezen záznam ve směrovací tabulce odesílají na tuto adresu.
DNS server	DNS server routeru. Adresa kam jsou přeposlány všechny DNS dotazy na router.

Tabulka 11: Konfigurace síťového rozhraní

Položky *Default Gateway* a *DNS Server* se využívají pouze tehdy, pokud je položka *DHCP Client* nastavena na hodnotu *disabled* a je-li Primary nebo Secondary LAN vybrána systémem Backup routes jako výchozí cesta (algoritmus výběru je popsán v sekci *1.12 Backup Routes*).

Ve stejném okamžiku smí být na routeru aktivní pouze jeden bridge. Ke konfiguraci jsou využívány parametry uvedené v úvodních třech položkách (DHCP Client, IP address, Subnet Mask). Jestliže jsou do bridge přidávána obě rozhraní (eth0 a eth1), má vyšší prioritu primární LAN (eth0). Další rozhraní (wlan0 – wifi) je možné přidat (resp. odebrat) do (ze) stávajícího bridge v jakoukoliv chvíli. Krom toho je také možné vytvořit bridge na žádost těchto rozhraní, není však nakonfigurován příslušnými parametry.

DHCP server přiděluje připojeným klientům IP adresy, IP adresu brány (IP adresa routeru) a IP adresu DNS serveru (IP adresa routeru).

DHCP server podporuje dynamické a statické přidělování IP adres. Dynamický DHCP server přiděluje klientům IP adresy z definovaného prostoru adres. Statický DHCP přiděluje IP adresy, které odpovídají MAC adresám připojeným klientům.

Položka	Popis
Enable dynamic DHCP leases	Zaškrtnutím této položky lze povolit dynamický DHCP server.
IP Pool Start	Začátek prostoru IP, které budou přidělovány DHCP klientům.
IP Pool End	Konec prostoru IP, které budou přidělovány DHCP klientům.
Lease time	Čas v sekundách, po který smí klient IP adresu používat.

Tabulka 12: Konfigurace dynamického DHCP serveru

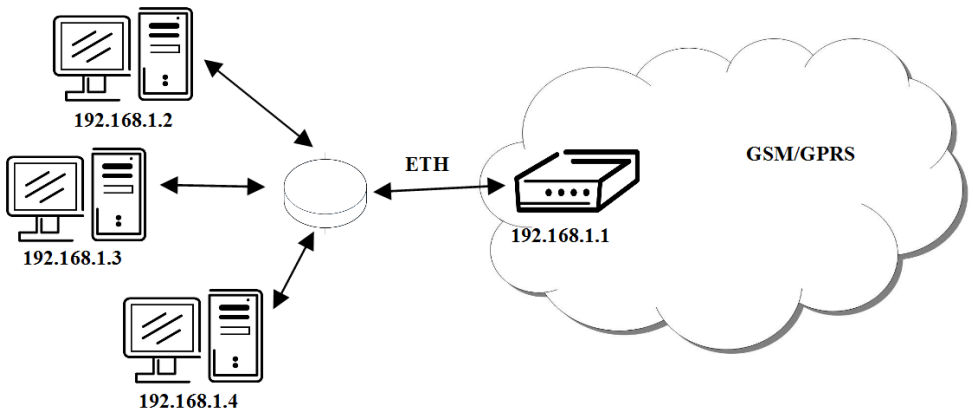
Položka	Popis
Enable static DHCP leases	Zaškrtnutím této položky lze povolit statický DHCP server.
MAC Address	MAC adresa DHCP klienta.
IP Address	Přidělená IP adresa.

Tabulka 13: Konfigurace statického DHCP serveru

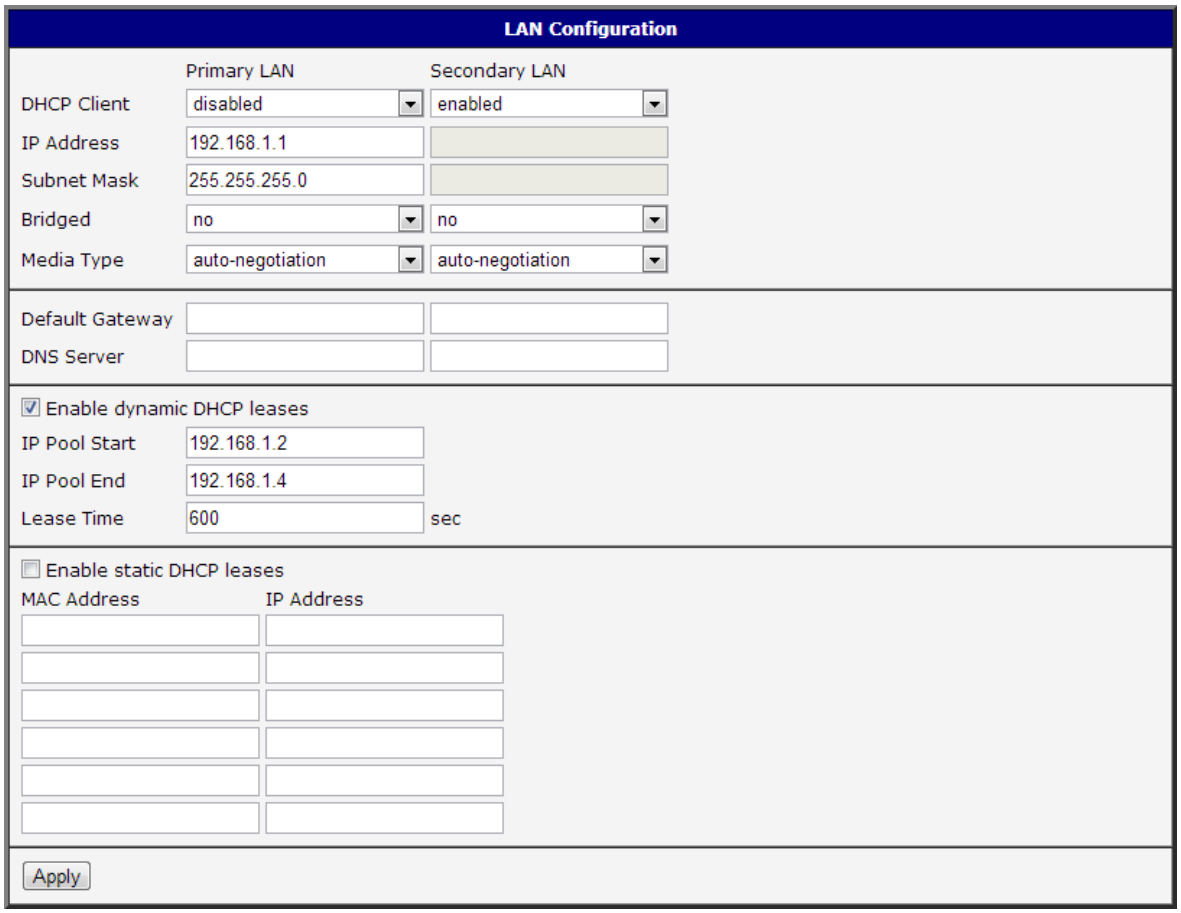
Je důležité, aby se nepřekrývaly rozsahy staticky zadaných IP adres a adres přidělených pomocí DHCP, jinak může dojít ke kolizi adres, a tím k nesprávné funkci sítě.

Příklad nastavení síťového rozhraní s dynamickým DHCP serverem:

- Rozsah přidělovaných adres je 192.168.1.2 až 192.168.1.4.
- Platnost přidělené adresy je 600 sekund (10 minut).



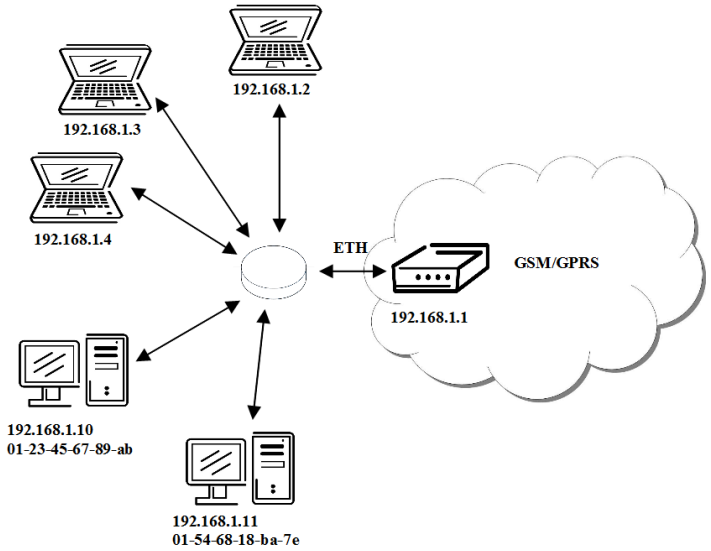
Obrázek 9: Topologie příkladu nastavení LAN 1



Obrázek 10: Příklad nastavení LAN 1

Příklad nastavení síťového rozhraní s dynamickým a statickým DHCP serverem:

- Rozsah přidělovaných adres je 192.168.1.2 až 192.168.1.4.
- Platnost dynamicky přidělené adresy je 600 sekund (10 minut).
- Klientovy s MAC adresou 01:23:45:67:89:ab je přidělena IP adresa 192.168.1.10
- Klientovy s MAC adresou 01:54:68:18:ba:7e je přidělena IP adresa 192.168.1.11



Obrázek 11: Topologie příkladu nastavení LAN 2

LAN Configuration

	Primary LAN	Secondary LAN
DHCP Client	disabled	enabled
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Bridged	no	no
Media Type	auto-negotiation	auto-negotiation
Default Gateway		
DNS Server		

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4
Lease Time	600 sec

☑ Enable static DHCP leases

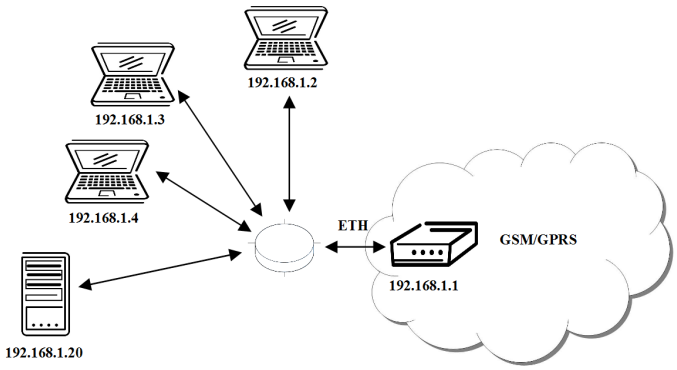
MAC Address	IP Address
01:23:45:67:89:ab	192.168.1.10
01:54:68:18:ba:7e	192.168.1.11

Apply

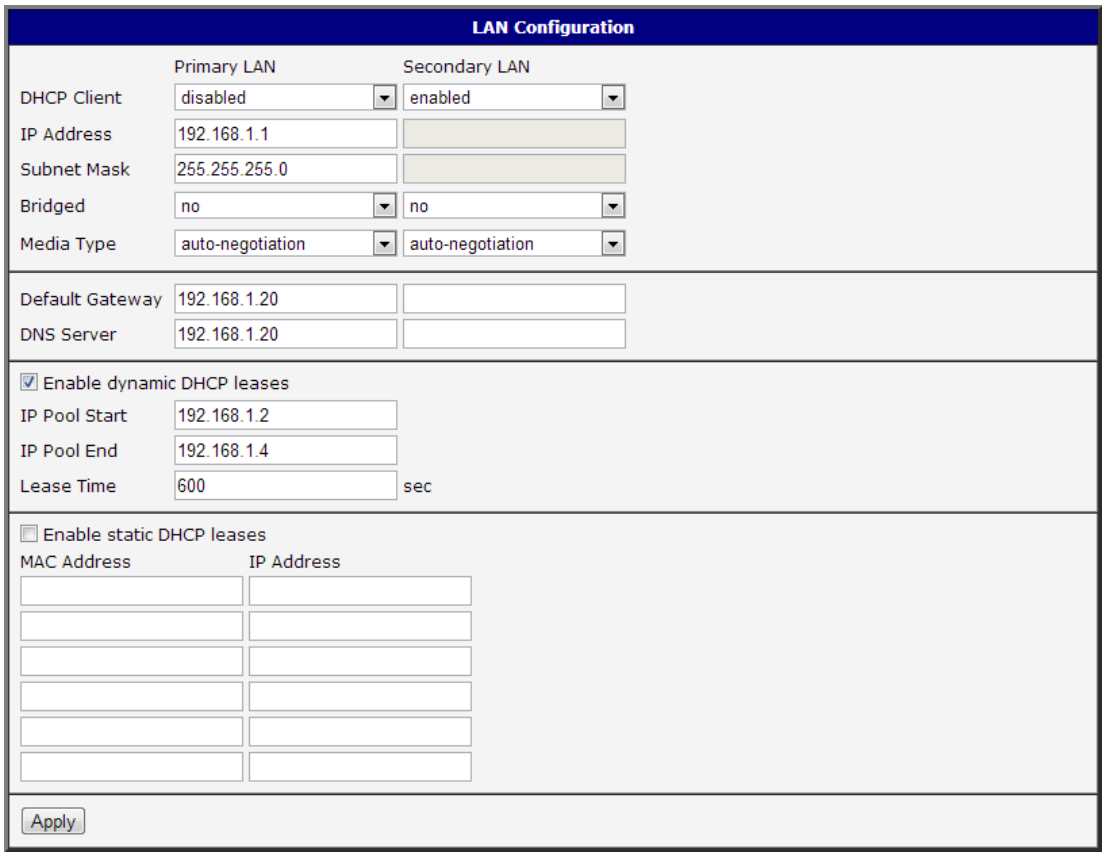
Obrázek 12: Příklad nastavení LAN 2

Příklad nastavení síťového rozhranní s výchozího bránou a DNS serverem:

- Výchozí brána má IP adresu 192.168.1.20
- DNS server má IP adresu 192.168.1.20



Obrázek 13: Topologie příkladu nastavení LAN 3



Obrázek 14: Příklad nastavení LAN 3

1.10 Konfigurace VRRP

Konfiguraci VRRP je možné vyvolat volbou *VRRP* v menu. Protokol VRRP (Virtual Router Redundancy Protocol) je technika, pomocí které lze přenést povinnosti routování z jednoho hlavního routeru na jiný záložní, v případě, že hlavní router vypoví službu. Protokol VRRP lze povolit zaškrtnutím volby *Enable VRRP*.

Položka	Popis
Virtual Server IP Address	Tento parametr nastavuje IP adresu virtuálního serveru, která je stejná pro oba routery. Připojené zařízení posílá svá data přes tuto virtuální adresu.
Virtual Server ID	Pokud by mělo v síti být více virtuálních routerů, tento parametr tyto virtuální routery rozlišuje. Hlavní a záložní router musí mít tento parametr nastavený stejně.
Host Priority	Hlavním routerem se stává ten router, který má nastavenou vyšší prioritu tohoto parametru. Podle RFC 2338 má hlavní router nejvyšší možnou prioritu, a to 255. Záložní router má prioritu v mezích 1 – 254 (výchozí hodnota je 100). Hodnota priority 0 není dovolena.

Tabulka 14: Konfigurace VRRP

V druhé části okna lze navolit kontrolu připojení zaškrtnutím volby *Check connection*. Momentálně aktivní router (hlavní/záložní) bude potom sám posílat ping dotazy. Kontrola spojení je určena k rozpoznání průchodnosti trasy, na jejímž základě dochází k přenosu funkce routeru z hlavního na záložní, popř. naopak.

Položka	Popis
Ping IP Address	Cílová IP adresa ping dotazů. Adresu nelze zadat jako doménové jméno.
Ping Interval	Časové intervaly mezi odesílanými ping dotazy.
Ping Timeout	Doba čekání na odpověď.
Ping Probes	Počet neúspěšných ping dotazů, po kterých se trasa považuje za neprůchodnou.

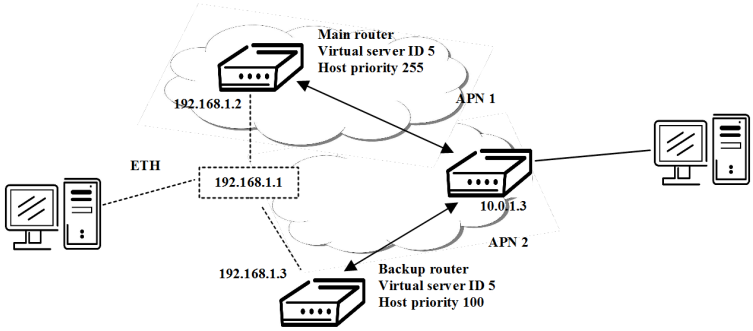
Tabulka 15: Konfigurace kontroly spojení

Jako ping adresu je nutné použít IP adresu, u které je jisté, že bude stále dostupná a bude na ní možné posílat ICMP dotazy (např. DNS server operátora).

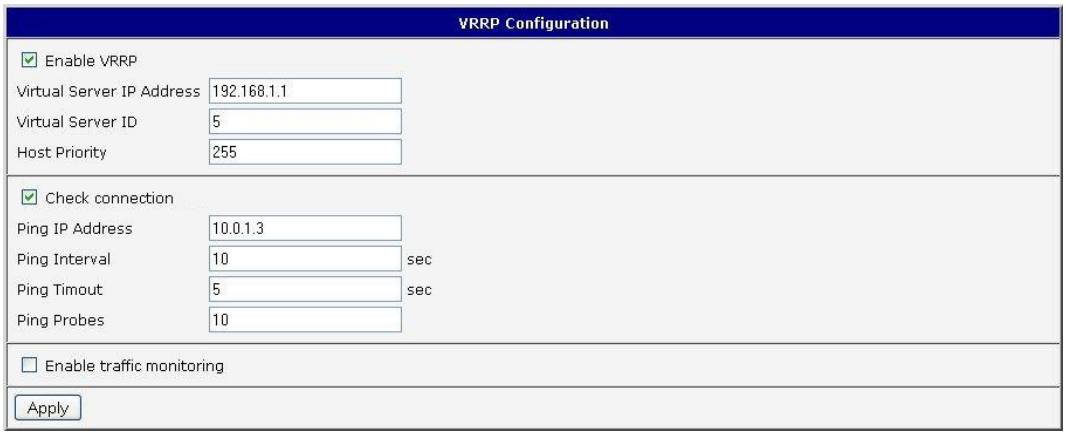
Pro sledování průchodnosti trasy je také možné využít parametr *Enable traffic monitoring*. Je-li tento parametr nastaven, pak se v případě, že je vysílán na sledovanou trasu paket jiný než ping, sleduje, zda do doby *Ping Timeout* přijde nějaká odpověď. Pokud ne, považuje se původní vyslaná zpráva za testovací (jakoby se vyslal ping, na který nepřišla odpověď), a následuje zrychlené testování (s intervalem mezi vysíláním určeným parametrem *Ping Interval*)

zprávami ping s tím, že první vyslaný ping je již považován za druhou testovací zprávu v řadě, která je omezena parametrem *Ping Probes*.

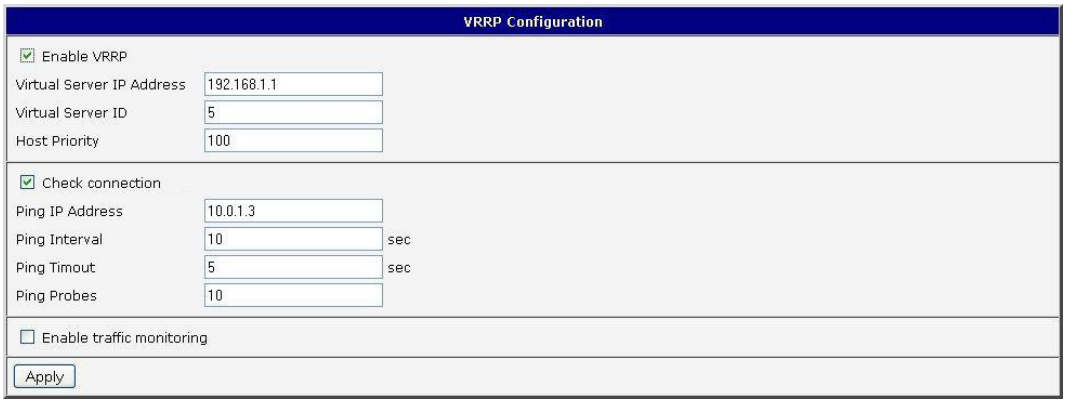
Příklad nastavení protokolu VRRP:



Obrázek 15: Topologie příkladu nastavení VRRP



Obrázek 16: Příklad konfigurace VRRP – Hlavní router



Obrázek 17: Příklad konfigurace VRRP – Záložní router

1.11 Konfigurace připojení do mobilní sítě

U průmyslového routeru XR5i v2 není položka *Mobile WAN Configuration* k dispozici.

Konfiguraci připojení do mobilní sítě lze vyvolat volbou položky *Mobile WAN* v hlavním menu webového rozhraní routeru.

1.11.1 Mobile WAN

Pokud je zaškrtnuta volba *Create connection to mobile network*, pak se router sám po zapnutí pokusí vytvořit spojení.

Položka	Popis
APN	Access point name – přístupový bod sítě
Username	Jméno uživatele pro přihlášení do sítě
Password	Přístupové heslo pro přihlášení do sítě
Authentication	Protokol autentizace v GSM síti: • PAP or CHAP – Routerem je zvolena jedna z autentizačních metod. • PAP – Je použita autentizační metoda PAP. • CHAP – Je použita autentizační metoda CHAP.
IP Address	IP adresa SIM karty. Uživatel nastaví IP adresu, pouze v případě byla mu IP adresa přidělena operátorem.
Phone Number	Telefonní číslo pro vytočení GPRS nebo CSD spojení. Router jako defaultní telefonní číslo používá *99***1 #.
Operator	V této položce lze definovat PLNM kód preferovaného operátora
Network type	Definuje způsob přenosu dat • Automatic selection – Router automaticky vybere konkrétní způsob přenosu dle dostupnosti přenosové technologie. • Furthermore, according to the type of router – Je možné vybrat konkrétní způsob přenosu dat. (GPRS, EDGE, UMTS, . . .).
PIN	Parametrem PIN je třeba nastavit pouze pokud to vyžaduje SIM karta routeru. V případě několika špatných pokusů o zadání PIN dojde k zablokování SIM karty.
MRU	Maximum Receiving Unit – identifikuje maximální velikost paketu, kterou je prvek v daném prostředí schopen přijmout. Z výroby je nastavena velikost na 1500 bytů.
MTU	Maximum Transmission Unit – identifikuje maximální velikost paketu, kterou je prvek v daném prostředí schopen přenášet. Z výroby je nastavena velikost na 1500 bytů.

Tabulka 16: Konfigurace přihlášení do GPRS

Tipy pro práci s konfiguračním formulářem *Mobile WAN*:

- Při nastavení chybné velikosti se nemusí povést přenos dat. Nastavením nižšího MTU dochází k častější fragmentaci dat, což znamená vyšší režii a zároveň možnost poškození paketu při zpětné defragmentaci. Naopak při vyšší hodnotě MTU nemusí daná síť paket přenést.
- Není-li vyplněno pole *IP address*, bude při sestavování spojení automaticky přidělena IP adresa operátorem. Vyplněním IP adresy dodané operátorem se urychlí připojení routeru k síti.
- Není-li vyplněno pole *APN*, router zvolí APN automaticky podle IMSI kódu SIM karty. Pokud PLMN (kód operátora) není v seznamu APN, pak se použije defaultní APN „internet“. APN definuje mobilní operátor.

UPOZORNĚNÍ:

- **Pokud je v routeru zasunuta jedna SIM karta, router přepíná mezi APN. Router se dvěma SIM kartami přepíná mezi SIM kartami.**
- **Zkontrolujte správně zadaný PIN. Pro SIM kartu se dvěma APN bude PIN stejný pro obě APN, jinak může dojít k zablokování SIM karty vícenásobným zadáním špatného PIN kódu.**

Položky označené hvězdičkou je nutné vyplnit pouze pokud jsou tyto údaje vyžadovány operátorem.

V případě neúspěšného sestavení spojení doporučujeme překontrolovat správnost zadaných údajů, případně vyzkoušet jinou autentizací metodu nebo jiný typ sítě.

1.11.2 Konfigurace DNS adres

Položka *DNS Settings* je určená pro snadnější konfiguraci na straně klienta. Při nastavení této položky na hodnotu *get from opertor* se router pokusí od operátora automaticky zjistit IP adresy primárního a sekundárního DNS serveru. Varianta *set manually* pak umožňuje nastavit IP adresu primárního DNS serveru ručně (pomocí položky *DNS Server*).

1.11.3 Konfigurace kontroly spojení s mobilní sítí

Je-li položka *Check Connection* nastavena na variantu *enabled* nebo *enabled + bind* aktivuje se kontrola připojení k mobilní síti. Router bude potom sám posílat ping dotazy na uvedenou doménu nebo IP adresu (položka *Ping IP Address*) v pravidelných časových intervalech (*Ping Interval*). Při neúspěšném pingu se nový odešle za deset sekund. Pokud se nezdaří ping na uvedenou IP adresu třikrát po sobě, pak router ukončí stávající spojení a pokusí se navázat nové. Kontrolu je možné nastavit zvlášť pro dvě SIM karty nebo pro dvě APN. Jako ping adresu lze použít IP adresu, u které je jisté, že je stále funkční a je na ní možné posílat ICMP ping (např. DNS server operátora).

V případě varianty *enabled* jsou ping dotazy posílány na základě routovací tabulky. Mohou tedy chodit přes jakékoliv dostupné síťové rozhraní. Pokud vyžadujeme, aby byl každý ping dotaz posílán přes síťové rozhraní, které bylo vytvořeno při sestavení spojení do sítě mobilního operátora, je nutné položku *Check Connection* nastavit na *enabled + bind*. Varianta *disabled* pak kontrolu připojení k mobilní síti deaktivuje.

Položka	Popis
Ping IP Address	IP adresa nebo doménové jméno pro odesílání kontrolního pingu.
Ping Interval	Časový interval odesílání pingu.

Tabulka 17: Konfigurace kontroly spojení s mobilní sítí

Při zaškrtnutí funkce *Enable Traffic Monitoring* router přestane posílat ping dotazy na *Ping IP address* a bude sledovat připojení k mobilní síti. Při nulovém provozu po dobu delší než *Ping Interval* router vyšle dotaz na adresu *Ping IP address*.

Pozor! Volbu *Check Connection* je třeba aktivovat (nastavit na *enabled* nebo *enabled + bind*) v případě potřeby trvalého provozu routeru.

1.11.4 Konfigurace datového limitu

Položka	Popis
Data limit	Nastavuje maximální očekávané množství přenesených dat (vyslaných i přijatých) přes GPRS v jedné účtovací periodě (měsíc).
Warning Threshold	Udává procentuální hodnotu parametru Data Limit v rozsahu 50% až 99%, po jejímž překročení router pošle SMS zprávu ve tvaru „Router has exceeded *(hodnota parametru Warning Threshold)* of data limit.“.
Accounting Start	Nastavuje den v měsíci, ve kterém začíná účtovací období použité SIM karty. Začátek účtovacího období definuje GSM/UMTS operátor, který dodá uživateli SIM kartu. Od toho dne v měsíci router vždy začíná počítat množství přenesených dat.

Tabulka 18: Konfigurace datového limitu

Pokud není zaškrtnut parametr *Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded* (viz dále) nebo *Send SMS when datalimit is exceeded* (viz konfigurace SMS) datový limit se nebude počítat.

1.11.5 Konfigurace přepínání mezi SIM kartami

V dolní části konfigurace je možné nastavit pravidla pro přepínání mezi dvěma SIM kartami, popřípadě mezi dvěma APN na jediné SIM kartě.

Položka	Popis
Default SIM card	Definuje výchozí APN nebo SIM kartu, z které se bude pokoušet sestavit spojení do mobilní sítě. Při nastavení tohoto parametru na none se router spustí v režimu offline a je nutné sestavit spojení do mobilní sítě pomocí SMS zprávy.
Backup SIM card	Definuje záložní APN nebo SIM kartu na kterou se bude router přepínat při nadefinování jednoho z následujících pravidel.

Tabulka 19: Konfigurace výchozí a záložní SIM karty

Pokud je parametr *Backup SIM card* nastaven na *none*, potom parametry *Switch to other SIM card when connection fails*, *Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected* a *Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded* přepnou router do off-line režimu.

Položka	Popis
Switch to other SIM card when connection fails	Při výpadku spojení do mobilní sítě tento parametr zajistí přepnutí na druhou SIM kartu nebo druhé APN. Výpadek spojení do mobilní sítě může nastat dvěma způsoby. Přistartu routeru, kdy se třikrát po sobě nepodaří navázat spojení do mobilní sítě. Nebo pokud je zaškrtnuta volba *Check connection to mobile network* a je indikována ztráta spojení do mobilní sítě.
Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected	V případě, že je detekován roaming, tento parametr umožní přepnutí na druhou SIM kartu nebo druhé APN. Je-li detekována domací síť, přepne zpět na výchozí SIM kartu.
Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded	Tento parametr zajišťuje přepnutí na druhou SIM kartu nebo druhé APN, v případě překročení datového limitu nastaveného parametrem *Data Limit*. Zároveň umožňuje přepnutí zpět na výchozí SIM kartu, pokud datový limit překročen není.
Switch to backup SIM card when binary input is active switch to default SIM card when binary input isn't active	Tento parametr zajistí přepnutí na druhou SIM kartu nebo druhé APN v případě sepnutí logického vstupu. Jesliže logický vstup sepnut není, přepíná zpět na výchozí SIM kartu.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Switch to default SIM card after timeout	Tento parametrem je možné definovat způsob, jakým se router pokusí přepnout zpět na defaultní SIM kartu nebo defaultní APN.

Tabulka 20: Konfigurace přepínání mezi SIM kartami

Následující parametry definují časy, po kterých se router pokusí přejít zpět na defaultní SIM kartu nebo APN.

Položka	Popis
Initial timeout	První pokus o přepnutí zpět na primární SIM kartu nebo APN se provede za čas definovaný tímto parametrem, povolený rozsah je 1 až 10000 minut.
Subsequent Timeout	Při neúspěšném pokusu o přepnutí se router o druhý pokus pokusí za čas definovaný tímto parametrem – 1 až 10000 minut.
Additive constants	Každý další pokus o přepnutí zpět na primární SIM kartu nebo APN se provede za čas spočítaný jako součet času předchozího pokusu a času definovaného tímto parametrem, rozmezí je 1 až 10000 minut.

Tabulka 21: Konfigurace časů pro přepnutí na výchozí SIM

Příklad:
Pokud je zaškrtnuta volba *Switch to primary SIM card after timeout* a parametry nastavené následovně *Initial Timeout* – 60 minut. *Subsequent Timeout* 30 minut a *Additive Timeout* – 20 minut. První pokus o přepnutí na primární SIM kartu nebo APN se provede po 60 minutách. Při neúspěšném přepnut se druhý pokus provádí po 30 minutách. Třetí po 50 minutách (30+20), čtvrtý po 70 minutách (30+20+20).

1.11.6 Konfigurace Dial-In přístupu

Dial-In access configuration je podporován pouze pro routery ER75i v2 a UR5 v2 (a také pro starší varianty ER75i a UR5).

V dolní části okna lze zaškrtnutím funkce *Enable Dial-In Access* definovat přístup po CSD spojení. Přístup lze zabezpečit použitím přihlašovacího jména a hesla. V případě že je tato funkce povolena a router nemá k dispozici spojení do mobilní sítě je umožněn přístup do routeru přes vytáčené spojení CSD. Router čeká 2 minuty na příjem spojení. Pokud se k routeru během této doby nikdo nepřihlásí, router se opět pokusí o navázání GPRS spojení.

Položka	Popis
Username	Přihlašovací jméno pro zabezpečený přístup.
Password	Heslo pro zabezpečený přístup.

Tabulka 22: Konfigurace Dial-In přístupu

1.11.7 Konfigurace PPPoE bridge mode

V poslední časti okna je možné zaškrtnout mód *Enable PPPoE bridge mode*, kterým aktivujete PPPoE bridge mód. PPPoE (point-to-point over ethernet) je síťový protokol, zapouzdřující PPP rámce do ethernetových rámců. Umožňuje vytvoření PPPoE spojení ze zařízení za routerem. Například z PC připojeného na ETH port routeru. PC bude přidělena IP adresa SIM karty.

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.

Mobile WAN Configuration

☐ Create connection to mobile network

	Primary SIM card	Secondary SIM card	
APN *			
Username *			
Password *			
Authentication	PAP or CHAP	PAP or CHAP	
IP Address *			
Phone Number *			
Operator *			
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator	get from operator	
DNS Server			

(*The feature of check connection to mobile network is necessary for uninterrupted operation*)

Check Connection	disabled	disabled	
Ping IP Address			
Ping Interval			sec

☐ Enable traffic monitoring

Data Limit		MB
Warning Threshold		%
Accounting Start	1	

Default SIM card	primary
Backup SIM card	secondary

☐ Switch to other SIM card when connection fails
☐ Switch to backup SIM card when roaming is detected and switch to default SIM card when home network is detected
☐ Switch to backup SIM card when data limit is exceeded and switch to default SIM card when data limit isn't exceeded
☐ Switch to backup SIM card when binary input is active and switch to default SIM card when binary input isn't active
☐ Switch to default SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

☐ Enable Dial-In access

Username *	
Password *	

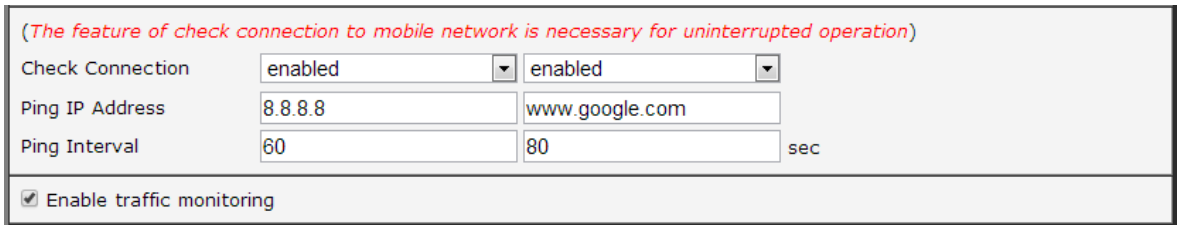
☐ Enable PPPoE bridge mode

* *can be blank*

Apply

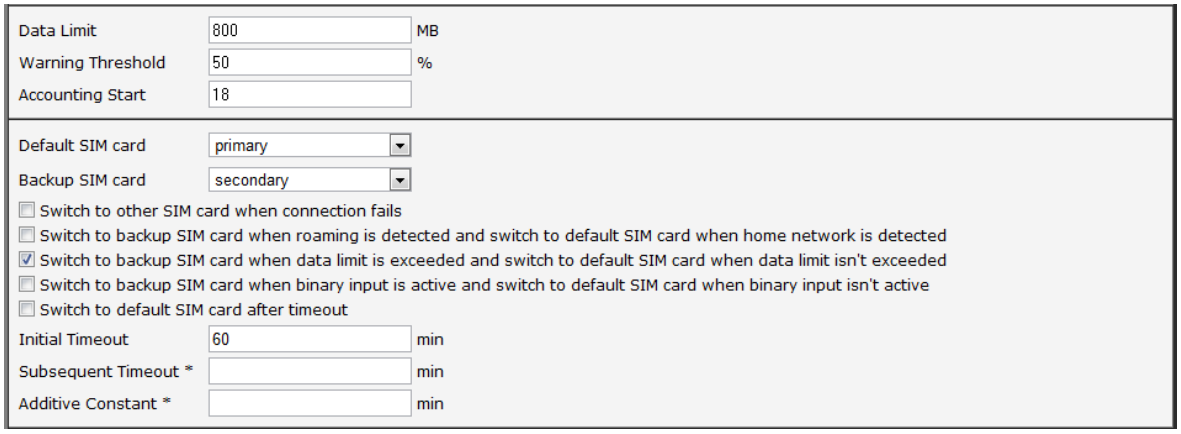
Obrázek 18: Mobile WAN konfigurace

Příklad nastavení kontroly spojení s mobilní sítí primární SIM karty na IP adrese 8.8.8.8 v časovém intervalu 60 s a sekundární SIM karty na doménové adrese www.google.com v časovém intervalu 80 s. V případě provozu na routeru se neposílají kontrolní pingy, ale je sledován provoz:



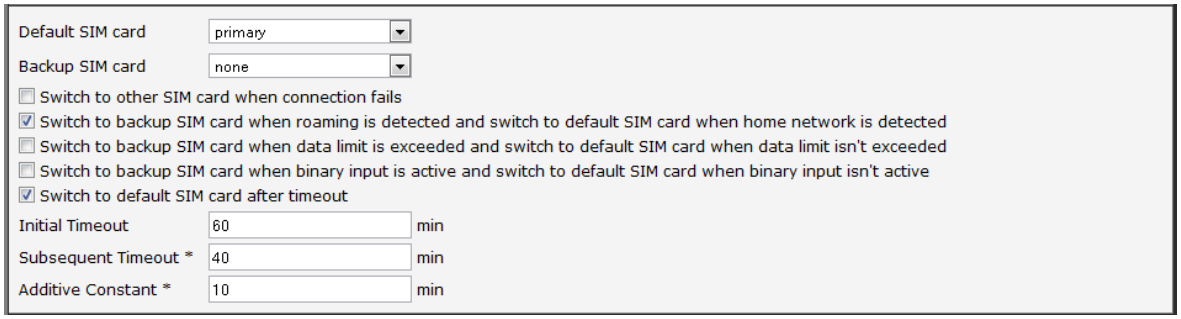
Obrázek 19: Příklad Mobile WAN konfigurace 1

Příklad přepnutí na záložní SIM kartu po překročení datového limitu 800 MB. Odeslání varovné SMS při dosažení 400 MB. S počátkem účtovacího období 18. dne v měsíci:



Obrázek 20: Příklad Mobile WAN konfigurace 2

Příklad přepnutí primární SIM karty do offline režimu po detekci roamingu. První pokus o přepnutí zpět na defaultní SIM kartu je proveden po 60 minutách, druhý po 40 minutách, třetí po 50 minutách (40+10) atd.



Obrázek 21: Příklad Mobile WAN konfigurace 3

1.12 Backup Routes

Pomocí konfiguračního formuláře na stránce *Backup Routes* je možné nastavit zálohování primárního připojení do internetu/mobilní sítě jiným typem připojení. Každému způsobu připojení lze definovat určitou prioritu. Vlastní přepínání se provádí na základě nastavených priorit a stavu kontroly spojení (pro *Primary LAN* a *Secondary LAN*).

Je-li zaškrtnuta volba *Enable backup routes switching*, vybírá se vychozí cesta podle nastavení níže. Konkrétně podle stavu povolení jednotlivých záložních cest (tj. *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for Primary LAN*, *Enable backup routes switching for Secondary LAN*, případně *Enable backup routes switching for PPPoE*), podle jejich explicitně nastavených priorit a podle stavu konroly spojení (pokud je zapnuta). Navíc se u síťových rozhraní, příslušejících k jednotlivým záložním cestám, kontroluje příznak "RUNNING". Tato kontrola řeší např. odpojení ethernetového kabelu.

Pokud volba *Enable backup routes switching* zaškrtnuta není, potom systém Backup routes pracuje v tzv. zpětně kompatibilním módu. Výchozí cesta se vybírá na základě implicitních priorit a podle stavu povolení nastavení jednotlivých síťových rozhraní, popř. povolení služeb, které tato síťová rozhraní nastavují. Názvy záložních cest a jím odpovídajících síťových rozhraní v pořadí podle implicitních priorit:

- Mobile WAN (pppX, usbX)
- PPPoE (ppp0)
- Secondary LAN (eth1)
- Primary LAN (eth0)

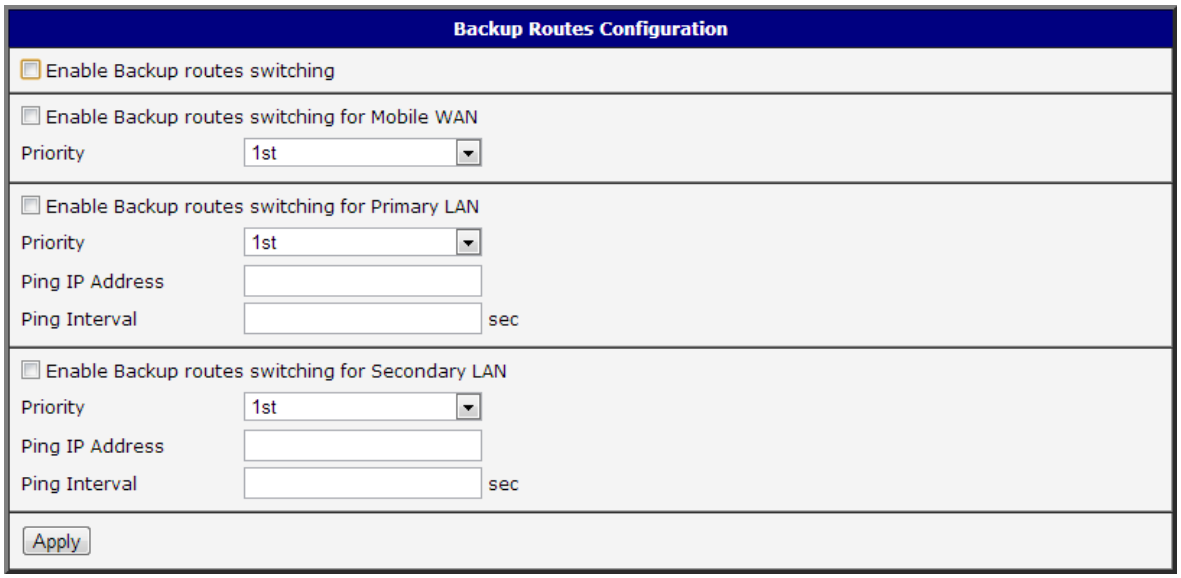
Příklad:

Secondary LAN je jako výchozí cesta vybrána pouze tehdy, pokud není zaškrtnuta volba *Create connection to mobile network* na stránce *Mobile WAN*, příp. není-li zaškrtnuta volba *Create PPPoE connection* na stránce *PPPoE*. Aby byla vybrána Primary LAN, tak ještě navíc nesmí být zadána *IP address* pro Secondary LAN a současně nesmí být zapnut *DHCP Client* pro Secondary LAN.

Položka	Popis
Priority	Priorita pro daný typ připojení
Ping IP Address	Cílová IP adresa ping dotazů pro kontrolu spojení **(adresu nelze zadat jako doménové jméno)**
Ping Interval	Časové intervaly mezi odesílanými ping dotazy

Tabulka 23: Backup Routes

Všechny změny v nastavení se projeví po stisknutí tlačítka *Apply*.

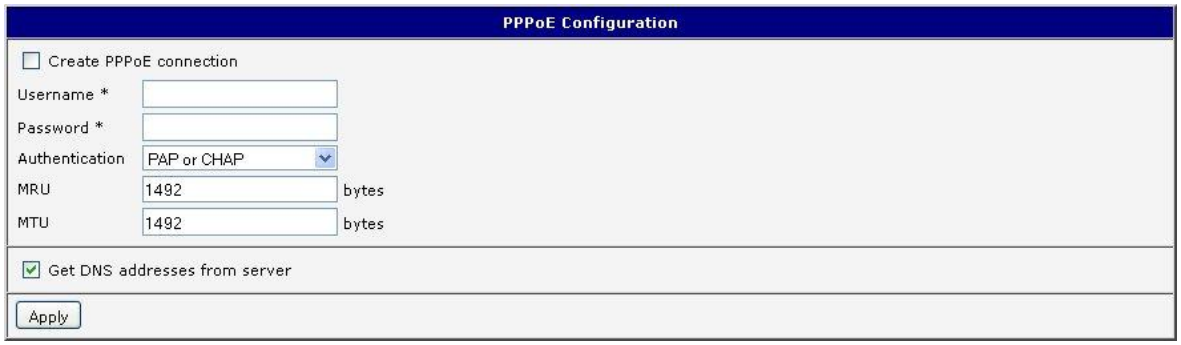


Obrázek 22: Backup Routes

1.13 Konfigurace PPPoE

Položka *PPPoE Configuration* je dostupná pouze u průmyslového routeru XR5i v2, kde funguje v režimu klient. Využívá se tedy k připojení PPPoE serveru nebo PPPoE bridge (např. ADSL modem).

Konfiguraci PPPoE klienta je možné vyvolat volbou *PPPoE* v menu. Pokud je zaškrtnuta volba *Create PPPoE connection*, pokusí se router po startu vytvořit PPPoE spojení. PPPoE (point-to-point over ethernet) je síťový protokol, zapouzdřující PPPoE rámce do ethernetových rámců. PPPoE klient slouží k připojení zařízení podporující PPPoE bridge nebo server (typicky například ADSL router). Po připojení router získá IP adresu zařízení ke kterému je připojen. Všechna komunikace z tohoto zařízení je přeposílána na router.



Obrázek 23: PPPoE konfigurace

Položka	Popis
Username	Jméno uživatele pro zabezpečené připojení do PPPoE
Password	Přístupové heslo pro zabezpečené připojení do PPPoE
Authentication	Protokol autentizace v síti • PAP or CHAP – Routerem je zvolena jedna z autentizačních metod. • PAP – Je použita autentizační metoda PAP. • CHAP – Je použita autentizační metoda CHAP.
MRU	Maximum Receiving Unit – Identifikuje maximální velikost paketu, kterou je prvek v daném prostředí schopen přijmout. Z výroby je nastavena velikost na 1492 bytů.
MTU	Maximum Transmission Unit – Identifikuje maximální velikost paketu, kterou je prvek v daném prostředí schopen přenášet. Z výroby je nastavena na 1492 bytů.

Tabulka 24: Konfigurace PPPoE

Při nastavení chybné velikosti paketu se nemusí provést přenos dat.

1.14 Konfigurace firewallu

Pomocí firewallu je možné nastavit IP adresy, z kterých je možný vzdálený přístup na router a vnitřní síť připojenou za routerem. Volba *Allow remote access only from specified hosts* zapíná/vypíná firewall. Ve firewallu je možné nastavit až osm vzdálených přístupů.

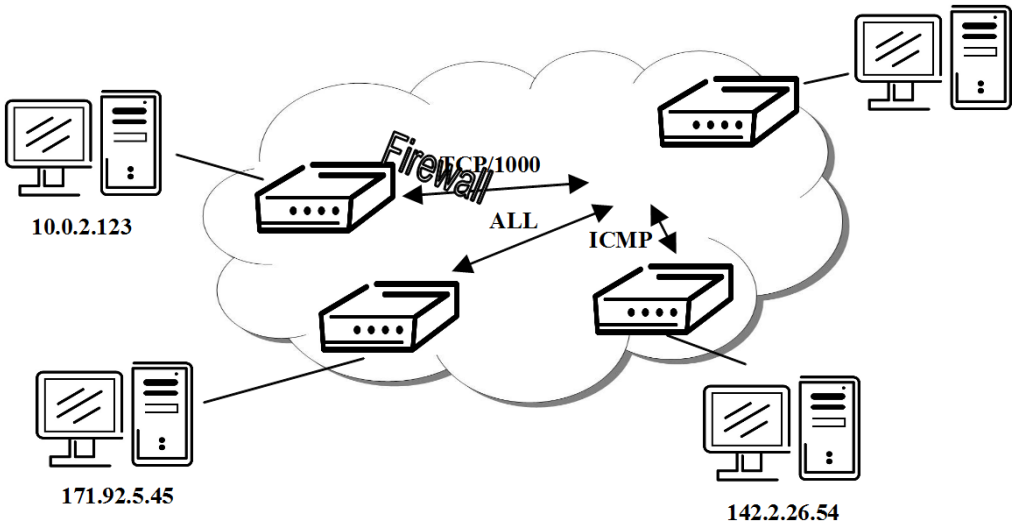
Položka	Popis
Source	• single address – přístup povolen jediné IP adrese definované v Source IP Address, • any address – přístup povolen kterékoliv IP adrese.
Source IP address	IP adresa ze které je povolen přístup na router.
Source Protocol	Protokol kterým je povolen přístup na router: • all – přistup povolen všemi protokoly, • TCP – přístup povolen protokolem TCP, • UDP – přístup povolen protokolem UDP, • ICMP – přístup povolen protokolem ICMP.
Target Port	Číslo portu na kterém je povolen přístup na router.

Tabulka 25: Konfigurace firewallu

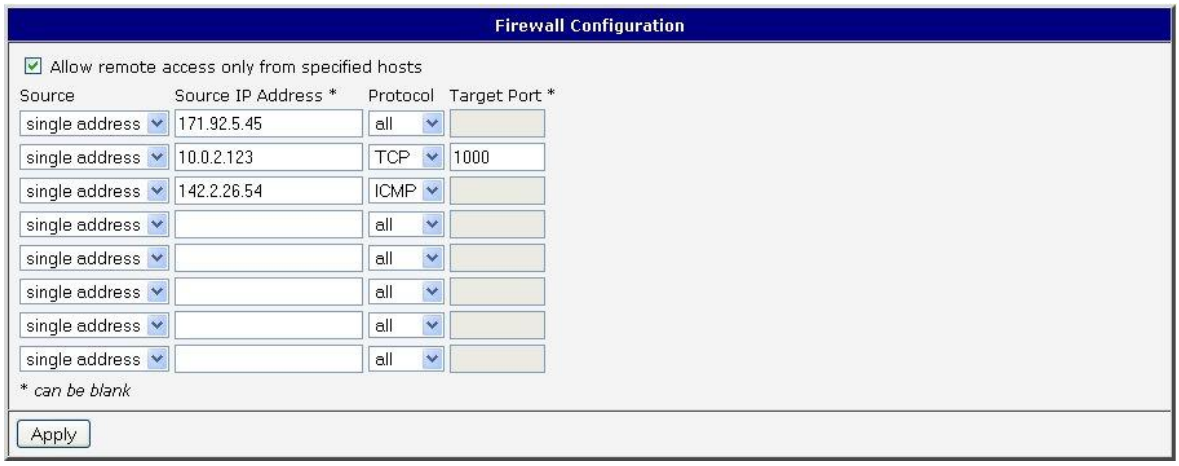
Příklad nastavení firewallu:

Na router jsou povoleny následující přístupy:

- z adresy 171.92.5.45 pomocí jakéhokoli protokolu
- z adresy 10.0.2.123 pomocí protokolu TCP na všech portech
- z adresy 142.2.26.54 pomocí protokolu ICMP



Obrázek 24: Topologie příkladu nastavení firewallu



Obrázek 25: Příklad nastavení firewallu

1.15 Konfigurace překladu adres (NAT)

Konfiguraci překladu adres lze vyvolat volbou položky *NAT* v menu. NAT (Network address Translation / Port address Translation – PAT) je způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů. Okno obsahuje šestnáct položek pro definici překladu adres.

Položka	Popis
Public Port	Vnější port
Private Port	Vnitřní port
Type	Volba protokolu
Server IP address	IP adresa kam budou přeposílány příchozí data

Tabulka 26: Konfigurace překladu adres (NAT)

Pokud je potřeba nastavit více než šestnáct pravidel pro NAT, je možné vložit do start-up script následující skript:

```
iptables -t nat -A napt -p tcp --dport [PORT\_PUBLIC] -j DNAT --to-destination
[IPADDR]:[PORT1\_PRIVATE]
```

kde se místo [PORT_PUBLIC] a [PORT_PRIVATE] vloží konkrétní čísla portů a místo [IPADDR] se vloží IP adresa.

The following items are used to set the routing of all incoming traffic from the PPP to the connected computer.

Položka	Popis
Send all remaining incoming packets to default server	Zaškrtnutím této položky a nastavením položky *Default Server IP Address* lze uvést router do režimu, kdy bude směrovat veškerou příchozí komunikaci z PPP na počítač s definovanou IP adresou.
Default Server IP Address	IP adresa pro směrování veškeré komunikace z PPP.

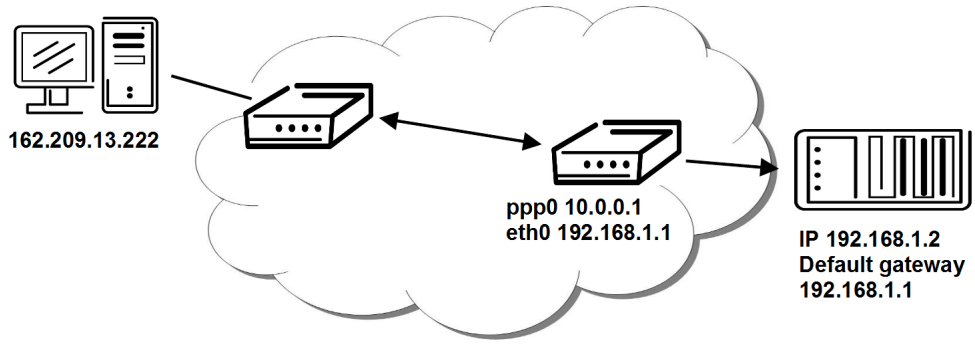
Tabulka 27: Konfigurace jednotného přeposílání

Povolením následujících voleb a zadáním čísla portu, je umožněno vzdálený přístup k routeru z PPP rozhranní.

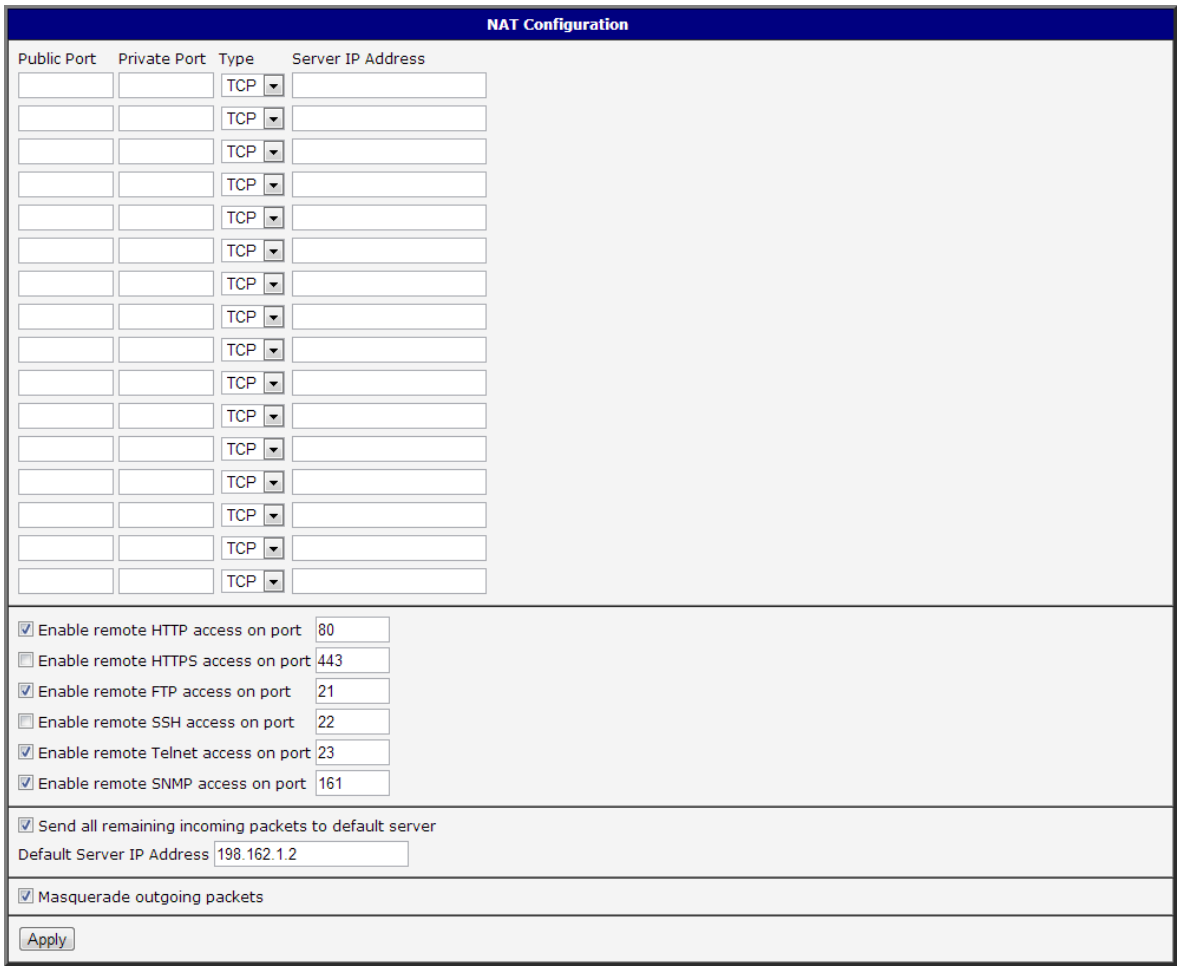
Položka	Popis
Enable remote HTTP access on port	Tato volba umožňuje konfiguraci routeru přes webové rozhraní (ve výchozí konfiguraci zakázáno).
Enable remote HTTPS access on port	Tato volba umožňuje konfiguraci routeru přes zabezpečený webový protokol *HTTPS* (ve výchozí konfiguraci zakázáno).
Enable remote FTP access on port	Tato volba umožňuje přístup přes *FTP* (ve výchozí konfiguraci zakázáno).
Enable remote SSH access on port	Tato volba umožňuje přístup přes *SSH* (ve výchozí konfiguraci zakázáno).
Enable remote Telnet access on port	Tato volba umožňuje přístup přes *Telnet* (ve výchozí konfiguraci zakázáno).
Enable remote SNMP access on port	Umožňuje dotazovat se SNMP agenta.
Masquerade outgoing packets	Volba masquerade (alternativní název pro systém překladu adres NAT) zapíná systém překladu adres NAT.

Tabulka 28: Konfigurace vzdáleného přístupu

Příklad konfigurace s jedním připojeným zařízením na routeru:



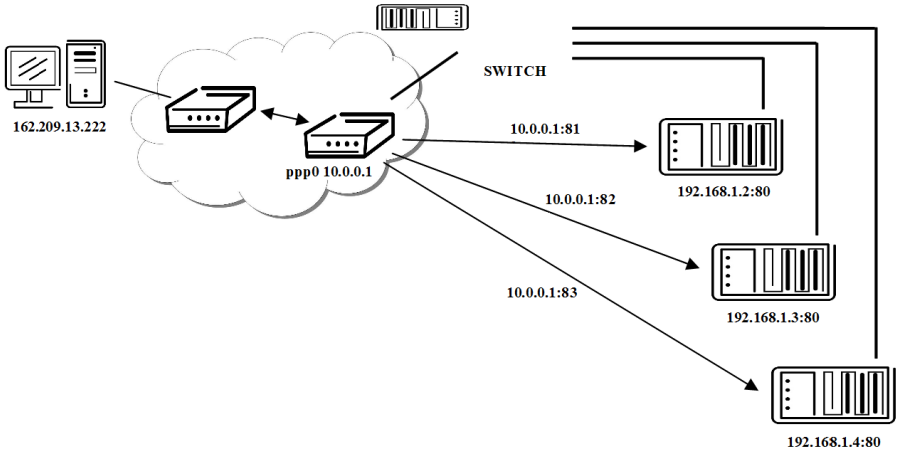
Obrázek 26: Topologie příkladu nastavení NAT 1



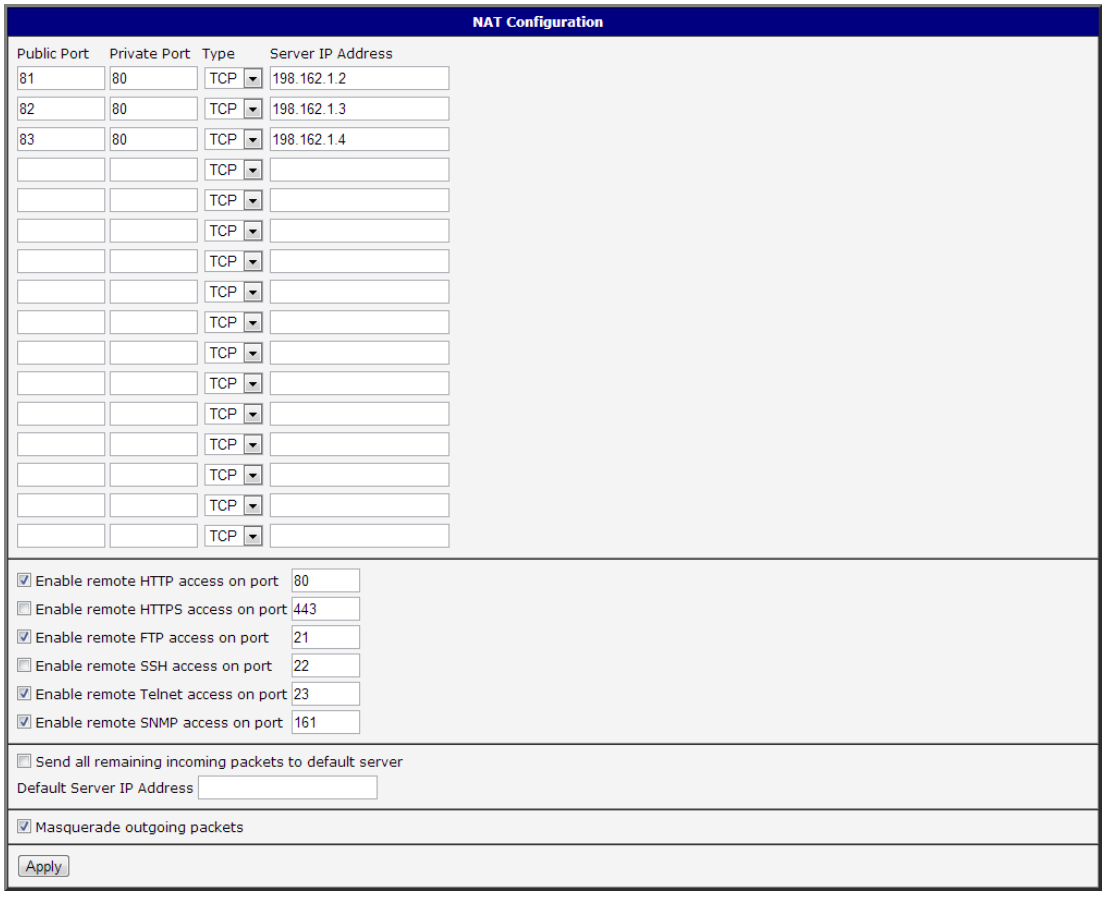
Obrázek 27: Příklad nastavení NAT 1

Při této konfiguraci je důležité mít označenou volbu *Send all remaining incoming packets to default server*, IP adresa v tomto případě je adresa zařízení za routerem. Připojené zařízení za routerem musí mít nastavenou *Default Gateway* na router. Při PINGu na IP adresu SIM karty odpovídá připojené zařízení.

Příklad konfigurace s více zařízeními na routeru:



Obrázek 28: Topologie příkladu nastavení NAT 2



Obrázek 29: Příklad nastavení NAT 2

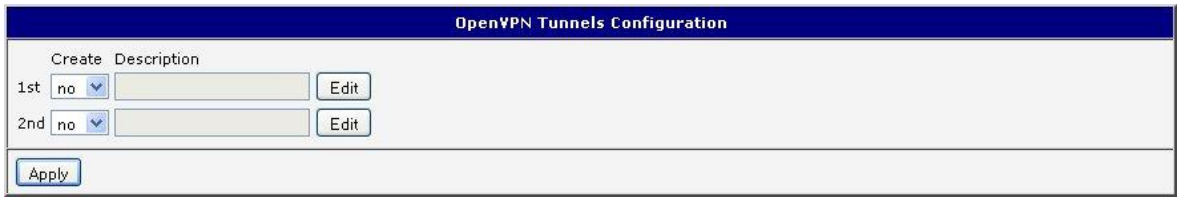
Při této konfiguraci definují adresy *Server IP Address* zařízení zapojené za routerem. Při pingu na IP adresu SIM karty odpovídá router. Přístup na webové rozhraní zařízení za routerem je možné pomocí Port Forwardingu, kdy se za IP adresu SIM udává vnější port, na které chceme přistoupit. Při požadavku na port 80 se zkoumají jednotlivé vnější porty (Public Port), tam tento port není definován, proto při zaškrtnuté volbě *Enable remote http access* se automaticky otevírá webové rozhraní routeru. Pokud tato volba není zaškrtnutá a je zaškrtnutá volba *Send all remaining incoming packets to default server* realizuje se spojení na uvedenou IP adresu. Při nezaškrtnuté volbě webového rozhraní a *Default Server IP address* se žádost neprovede.

1.16 Konfigurace OpenVPN tunelu

OpenVPN tunel umožňuje zabezpečené (šifrované) propojení dvou sítí LAN do jedné, která se tváří jako homogenní. Router umožňuje vytvořit až dva OpenVPN tunely, jejich konfiguraci lze vyvolat volbou položky *OpenVPN* v menu. V okně *OpenVPN Tunnels Configuration* jsou dva řádky, každý řádek odpovídá konfiguraci jednoho tunelu.

Položka	Popis
Create	Tato položka zapíná jednotlivé tunely.
Description	Tato položka zobrazuje název tunelu, zadaný v konfiguraci tunelu.
Edit	Konfigurace OpenVPN tunelu.

Tabulka 29: Přehled OpenVPN tunelů



Obrázek 30: Přehled OpenVPN tunelů

Položka	Popis
Description	Popis tunelu.
Protocol	Protokol pomocí kterého bude OpenVPN komunikovat: • UDP – OpenVPN bude komunikovat protokolem UDP. • TCP server – OpenVPN bude komunikovat protokolem TCP v režimu server. • TCP client – OpenVPN bude komunikovat protokolem TCP v režimu klient.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
UDP/TCP port	Port příslušného protokolu.
Remote IP Address	IP adresa protější strany tunelu. Lze použít i doménové jméno.
Remote Subnet	IP adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Redirect Gateway	Umožňuje přesměrovat všechen provoz na Ethernetu.
Local Interface IP Address	Definuje IP adresu lokálního rozhraní.
Remote Interface IP Address	Definuje IP adresu rozhraní protější strany tunelu.
Ping Interval	Definuje časový interval, po kterém pošle zprávu druhé straně, pro kontrolu správné existence tunelu.
Ping Timeout	Definuje časový interval, po který router čeká na vyslanou zprávu protistranou. Aby se správně ověřoval OpenVPN tunel, musí být parametr *Ping Timeout* větší než *Ping Interval*.
Renegotiate Interval	Nastavuje periodu renegociace (reautorizace) tunelu OpenVPN. Tento parametr je možné nastavit pouze při ověřování username/password nebo při použití certifikátu X.509. Po této časové periodě router mění šifrování tunelu, aby byla zajištěna trvalá bezpečnost tunelu.
Max Fragment Size	Tímto parametrem je možné definovat maximální velikost odesílaného paketu.
Compression	Odesílané data je možné komprimovat • none – Není použitá žádná komprese. • LZO – Je použita bezeztrátová komprese, která musí být nastavená na obou stranách tunelu.
NAT Rules	Tímto parametrem lze aplikovat NAT pravidla na OpenVPN tunel: • not applied – NAT pravidla nejsou aplikována na OpenVPN tunel. • applied – NAT pravidla jsou aplikována na OpenVPN tunel.
Authenticate Mode	Tímto parametrem je možné nastavit autentizaci: • none – Není nastavena žádná autentizace. • Pre-shared secret – Nastavuje sdílený klíč pro obě strany tunelu. • Username/password – Umožňuje autentizaci pomocí *CA Certificate*, *Username* a *Password*.

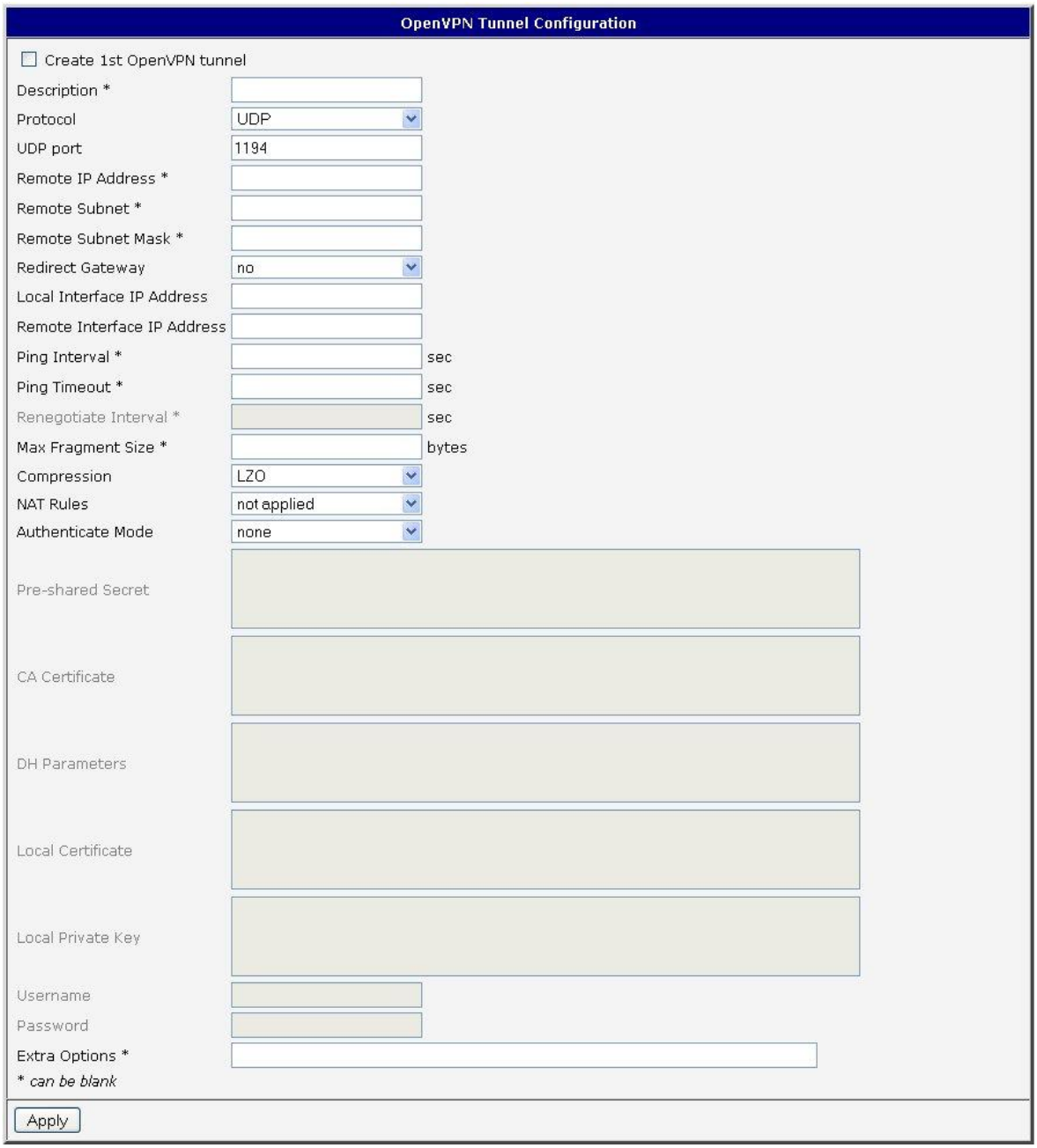
Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
	• X.509 Certificate (multiclient) – Umožňuje autentizaci X.509 v režimu multiclient. • X.509 Certificate (client) – Umožňuje autentizaci X.509 v režimu klient. • X.509 Certificate (server) – Umožňuje autentizaci X.509 v režimu server.
Pre-shared Secret	Autentizace pomocí Pre-shared secret lze použít v autentizacích Pre-shared secret, Username/password a X.509 Certificate.
CA Certificate	Autentizace pomocí CA Certificate lze použít v autentizacích Username/password a X.509 Certificate.
DH Parameters	Protokol pro výměnu klíčů DH Parameters lze použít v autentizaci X.509 v režimu server.
Local Certificate	Tento autentizační certifikát lze použít v autentizaci X.509 Certificate.
Local Private Key	Lokální privátní klíč Local *Private Key* lze použít v autentizaci X.509 Certificate.
Username	Autentizace pomocí přihlašovacího jména a hesla lze použít v autentizaci Username/Password.
Password	Autentizace pomocí přihlašovacího jména a hesla lze použít v autentizaci Username/Password.
Extra Options	Pomocí parametru *Extra Options* je možné definovat doplňující parametry OpenVPN tunelu jako například DHCP options atd.

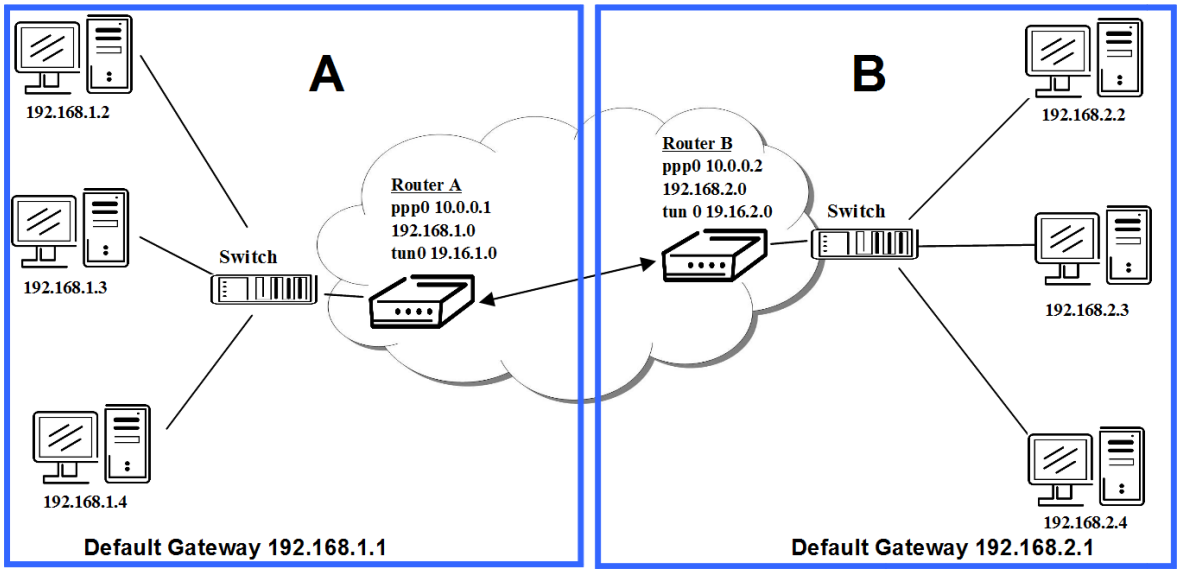
Tabulka 30: Konfigurace OpenVPN tunelu

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 31: Konfigurace OpenVPN tunelu

Příklad konfigurace OpenVPN tunelu:



Obrázek 32: Topologie příkladu konfigurace OpenVPN tunelu

Konfigurace OpenVPN tunelu:

Konfigurace	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Tabulka 31: Příklad konfigurace OpenVPN tunelu

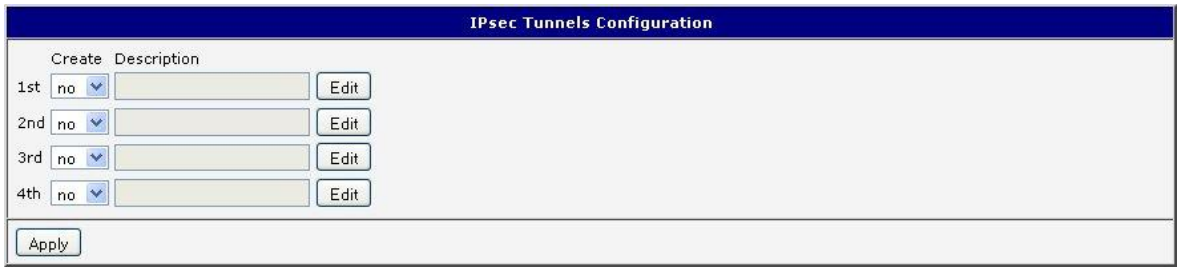
Příklady nastavení všech různých možností konfigurací a autentizací OpenVPN lze nalézt v konfiguračním manuálu OpenVPN tunelu.

1.17 Konfigurace IPSec tunelu

IPsec tunel vytváří zabezpečené (šifrované) propojení dvou sítí LAN do jedné, která se tváří jako homogenní. Router umožňuje vytvořit až čtyři IPSec tunely, jejichž konfiguraci lze vyvolat volbou položky *IPsec* v menu. V okně *IPsec Tunnels Configuration* jsou čtyři řádky, přičemž každý řádek odpovídá konfiguraci jednoho tunelu.

Položka	Popis
Create	Tato položka zapíná jednotlivé tunely.
Description	Tato položka zobrazuje název tunelu, zadaný v konfiguraci tunelu.
Edit	Konfigurace IPsec tunelu.

Tabulka 32: Přehled IPsec tunelů



Obrázek 33: Přehled IPsec tunelů

Položka	Popis
Description	Název tunelu
Remote IP Address	IP adresa protější strany tunelu. Lze zadat i doménové jméno.
Remote ID	ID protější strany. ID se skládají ze dvou částí: *hostname* a *domain-name*.
Remote Subnet	IP adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Local ID	ID lokální strany tunelu. ID se skládají ze dvou částí: *hostname* a *domain-name*.
Local Subnet	IP adresa lokální sítě.
Local subnet mask	Maska lokální sítě.
Encapsulation Mode	Režim IPsecu (dle způsobu zapouzdření) – zvolit lze tunnel (zapouzdřen celý IP datagram) nebo transport (pouze IP hlavička).
NAT traversal	Pokud se mezi dvěma koncovými body IPsec tunelu používá překlad adres, je nutné povolit NAT Traversal (*Enabled*).

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
IKE Mode	Definuje mód při sestavování spojení (*main* či *aggressive*). Je-li zvolen agresivní mód, spojení je sestaveno rychleji, ale šifrování je nastaveno striktně na 3DES-MD5.
IKE Algorithm	Způsob volby algoritmu: • *auto* – šifrovací a hashovací algoritmus je zvolen automaticky • *manual* – šifrovací a hashovací algoritmus nadefinuje uživatel
IKE Encryption	Šifrovací algoritmus – 3DES, AES128, AES192, AES256
IKE Hash	Hashovací algoritmus – MD5 nebo SHA1
IKE DH Group	Číslo Diffie-Hellman skupiny. Skupina určuje sílu klíče použitého v procesu výměny klíčů. Vyšší číslo skupiny zajišťuje větší bezpečnost, ale vyžaduje více času pro výpočet.
ESP Algorithm	Způsob volby algoritmu: • *auto* – šifrovací a hashovací algoritmus je zvolen automaticky • *manual* – šifrovací a hashovací algoritmus nadefinuje uživatel
ESP Encryption	Šifrovací algoritmus – DES, 3DES, AES128, AES192, AES256
ESP Hash	Hashovací algoritmus – MD5 nebo SHA1
PFS	Zabraňuje ohrožení dat v případě vyzrazení hlavního klíče
PFS DH Group	Číslo Diffie-Hellman skupiny (viz *IKE DH Group*)
Key Lifetime	Životnost klíče datové části tunelu. Minimální hodnota tohoto parametru je 60 s. Maximální hodnota je 86400 s.
IKE Lifetime	Životnost klíče řídící části tunelu. Minimální hodnota tohoto parametru je 60 s. Maximální hodnota je 86400 s.
Rekey Margin	Čas před vypršením platnosti klíčů, kdy se generují nové klíče. Maximální hodnota musí být menší než polovina parametrů IKE a Key Lifetime.
Rekey Fuzz	Procentuální prodloužení času Rekay Margin.
DPD Delay	Čas, po kterém se zkouší funkčnost IPsec tunelu.
DPD Timeout	Doba, po kterou se poté čeká na odpověď.
Authenticate Mode	Tímto parametrem je možné nastavit autentizaci: • Pre-shared key – Nastavuje sdílený klíč pro obě strany tunelu. • X.509 Certificate – Umožňuje autentizaci X.509 v režimu multiclient.
Pre-shared Key	Sdílený klíč pro obě strany tunelu pro autentizaci Pre-shared key.
CA Certificate	Certifikát pro autentizaci X.509.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Remote Certificate	Certifikát pro autentizaci X.509.
Local Certificate	Certifikát pro autentizaci X.509.
Local Private Key	Privátní klíč pro autentizaci X.509.
Local Passphrase	Privátní klíč pro autentizaci X.509.
Extra Options	Pomocí tohoto parametru je možné definovat doplňující parametry OpenVPN tunelu jako například šifrování atd.

Tabulka 33: Konfigurace IPsec tunelu

Certifikáty a privátní klíč musí být ve formátu PEM. Jako certifikát lze použít pouze takový, který je uvozen začátkem a koncem certifikátu.

Náhodný čas, po kterém dojde k opětovné výměně nových klíčů se definuje:

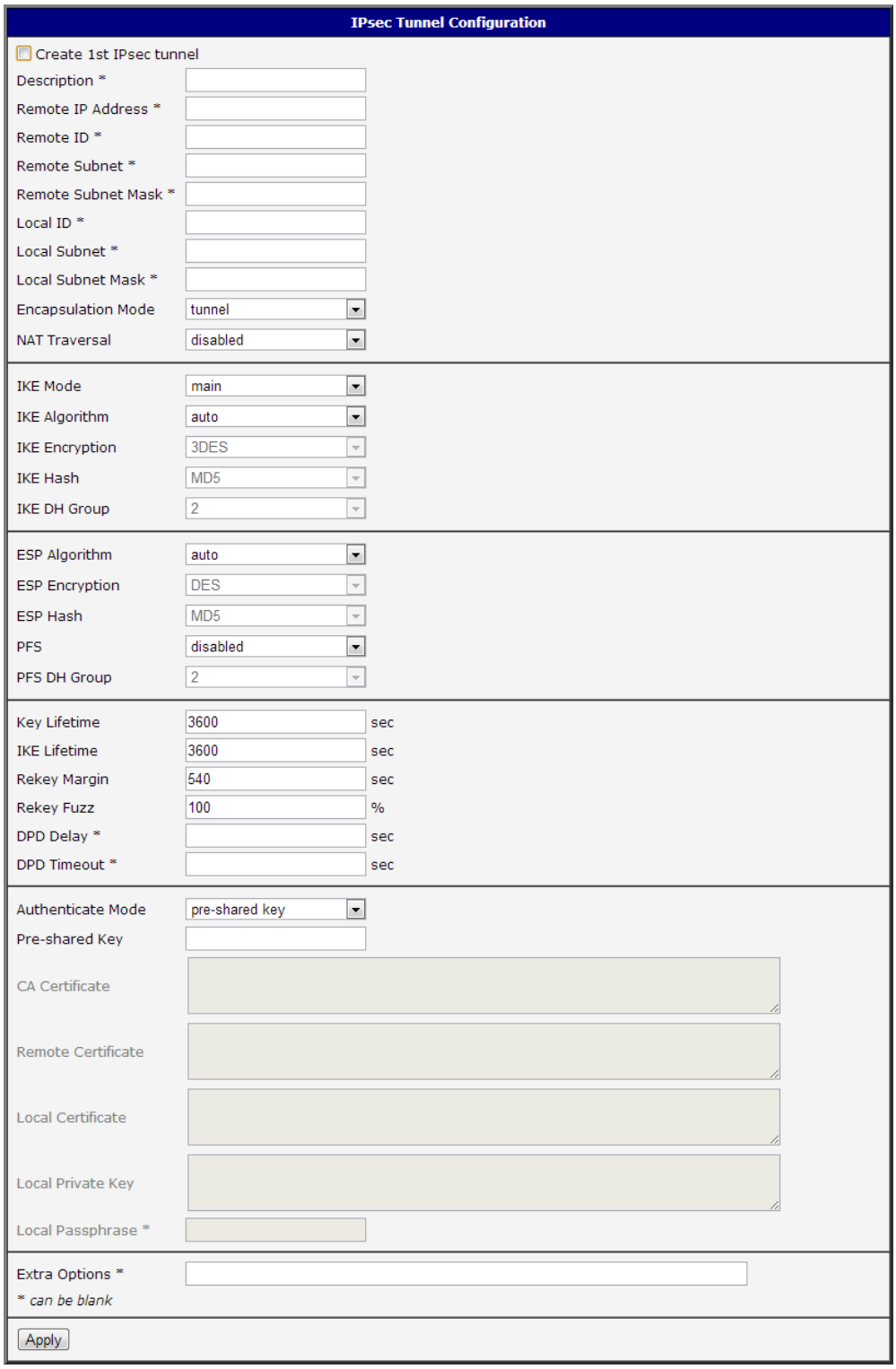
*Lifetime - (Rekey margin + náhodná hodnota v rozmezí (0 až Rekey margin * Rekey Fuzz/100))*

Při výchozím nastavení bude opětovná výměna klíčů probíhat v časové rozmezí:

- Minimální čas: 1 h - (9 m + 9 m) = 42 m
- Maximální čas: 1 h - (9 m + 0 m) = 51 m

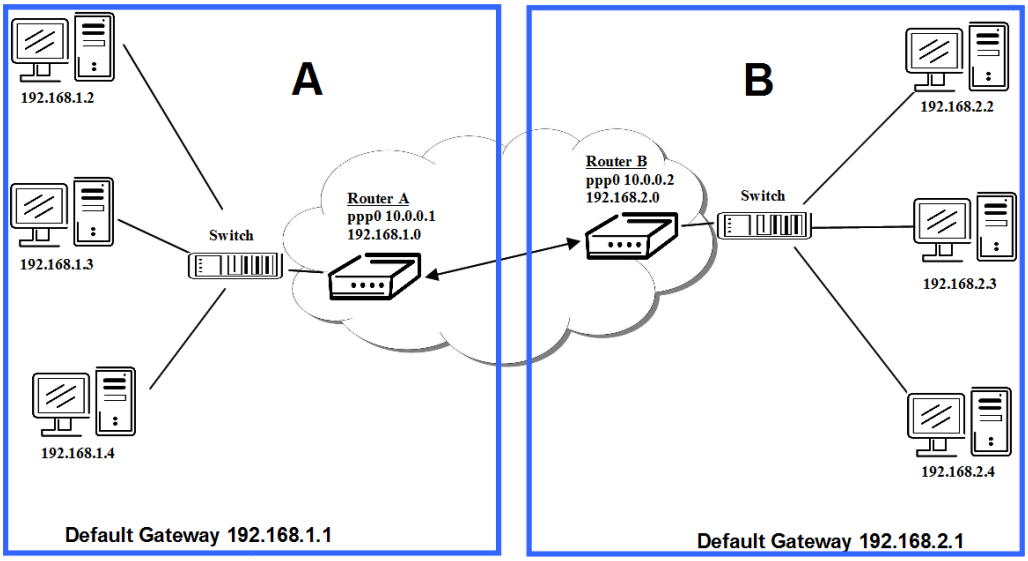
Při nastavování časů pro výměnu klíčů doporučujeme nechat výchozí nastavení, při kterém je garantována bezpečnost tunelu. Při nastavení vyššího času se sníží provozní režie a zároveň se sníží bezpečnost tunelu. Naopak při snížení času dojde ke zvýšení provozní režie a bezpečnosti tunelu.

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 34: Konfigurace IPsec tunelu

Příklad konfigurace IPSec tunelu:



Obrázek 35: Topologie příkladu konfigurace IPsec tunelu

Konfigurace IPsec tunelu:

Konfigurace	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mas:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Tabulka 34: Příklad konfigurace IPsec tunelu

Příklady nastavení všech různých možností konfigurací a autentizací IPsec je možné nalézt v konfiguračním manuálu IPsec tunelu.

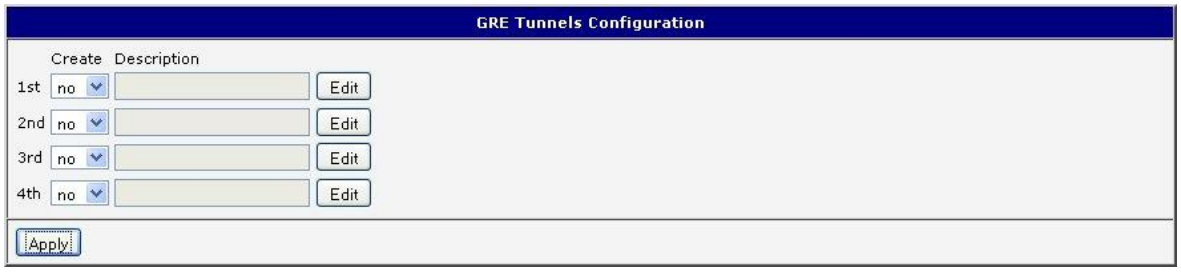
1.18 Konfigurace GRE tunelu

GRE je nešifrovaný protokol.

GRE tunel vytváří propojení dvou sítí LAN do jedné, která se tváří jako homogenní. Router umožňuje vytvořit až čtyři GRE tunely, jejichž konfiguraci je možné vyvolat volbou položky *GRE* v menu. V okně *GRE Tunnels Configuration* jsou čtyři řádky, přičemž každý řádek odpovídá konfiguraci jednoho tunelu.

Položka	Popis
Create	Tato položka zapíná jednotlivé tunely.
Description	Tato položka zobrazuje název tunelu, zadaný v konfiguraci tunelu.
Edit	Konfigurace GRE tunelu.

Tabulka 35: Přehled GRE tunelů



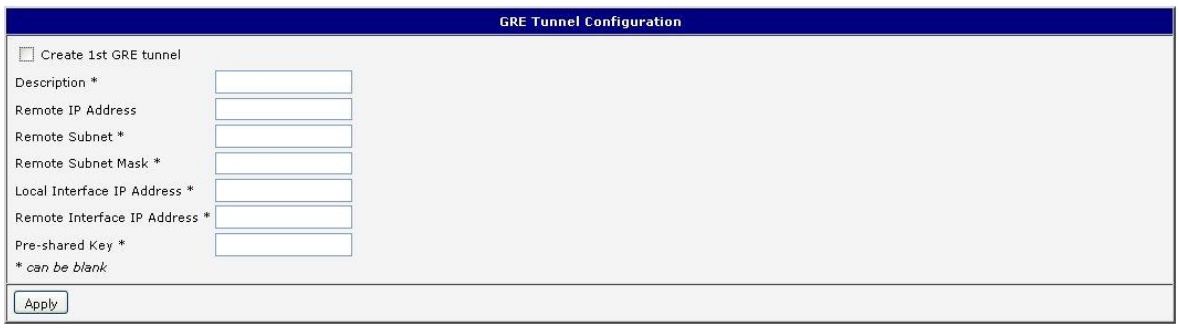
Obrázek 36: Přehled GRE tunelů

Položka	Popis
Description	Název tunelu.
Remote IP Address	IP adresa protější strany tunelu.
Local Interface IP Address	Interní IP adresa lokální strany tunelu.
Remote Interface IP Address	Interní IP adresa protější strany tunelu.
Remote Subnet	Adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Pre-shared Key	Volitelná položka, která definuje 32 bit sdílený klíč, pomocí kterého se filtrují data procházející tunelem. Tento klíč musí být na obou routerech definován stejně, jinak bude router zahazovat přijaté pakety. Pomocí tohoto klíče se nezabezpečují data procházející tunelem.

Tabulka 36: Konfigurace GRE tunelu

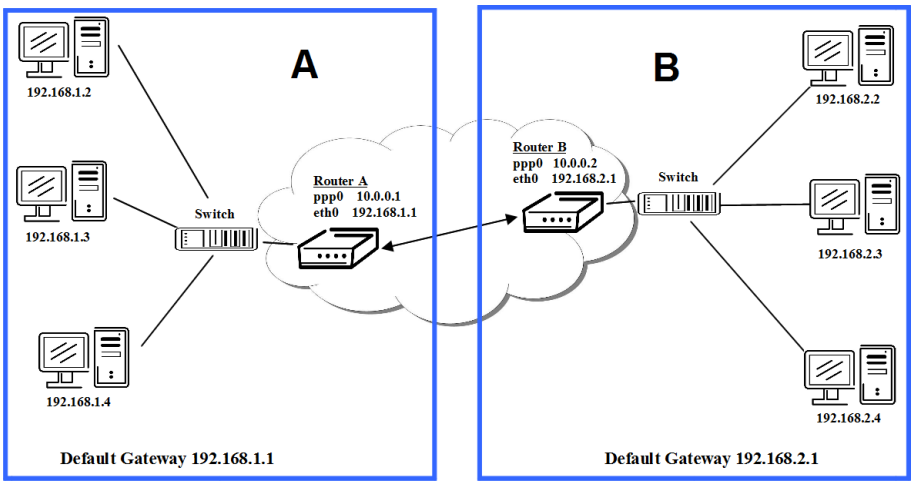
Pozor, GRE tunel neprojde přes překlad adres NAT.

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 37: Konfigurace GRE tunelu

Příklad konfigurace GRE tunelu:



Obrázek 38: Topologie příkladu konfigurace GRE tunelu

Konfigurace GRE tunelu:

Konfigurace	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Tabulka 37: Příklad konfigurace GRE tunelu

1.19 Konfigurace L2TP tunelu

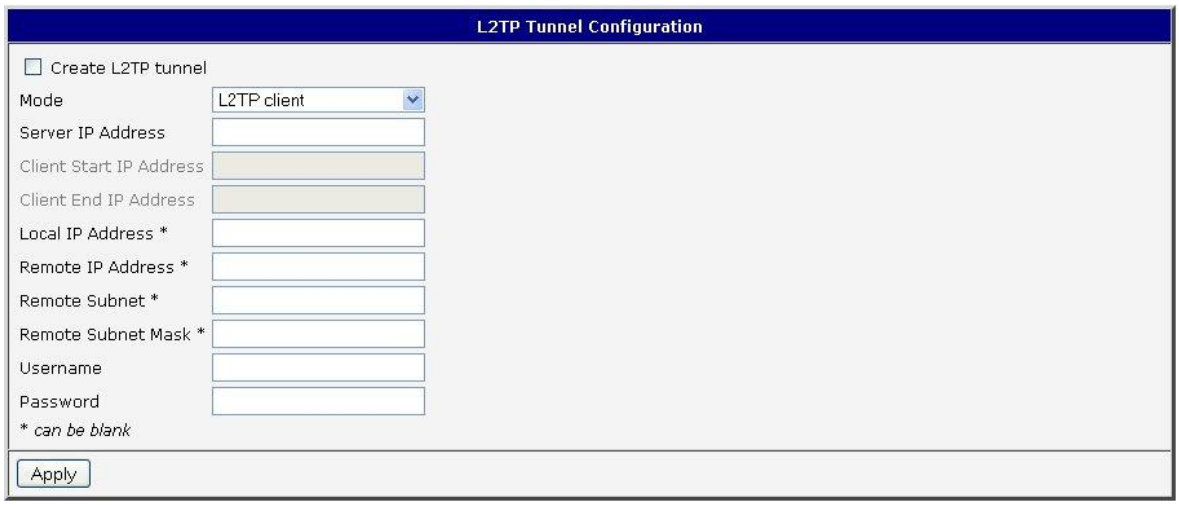
L2TP je nešifrovaný protokol.

Konfiguraci L2TP tunelu lze vyvolat volbou položky *L2TP* v menu. L2TP tunel se používá pro spojení dvou sítí LAN do jedné s autentizací, která se tváří jako homogenní. L2TP tunel se bude vytvářet po zaškrtnutí volby *Create L2TP tunnel*.

Položka	Popis
Mode	Mód L2TP tunelu na straně routeru: • L2TP server – Lze definovat počáteční a konečnou IP adresu rozsahu nabízenou serverem. • L2TP client – Lze definovat IP adresu server.
Server IP Address	Adresa serveru.
Client Start IP Address	První IP adresa v rozsahu nabízeném serverem klientům.
Client End IP Address	Poslední IP adresa v rozsahu nabízeném serverem klientům.
Local IP Address	IP adresa lokální strany tunelu.
Remote IP Address	IP adresa protější strany tunelu.
Remote Subnet	IP adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Username	Přihlašovací jméno pro přihlášení do L2TP tunelu.
Password	Heslo pro přihlášení do L2TP tunelu.

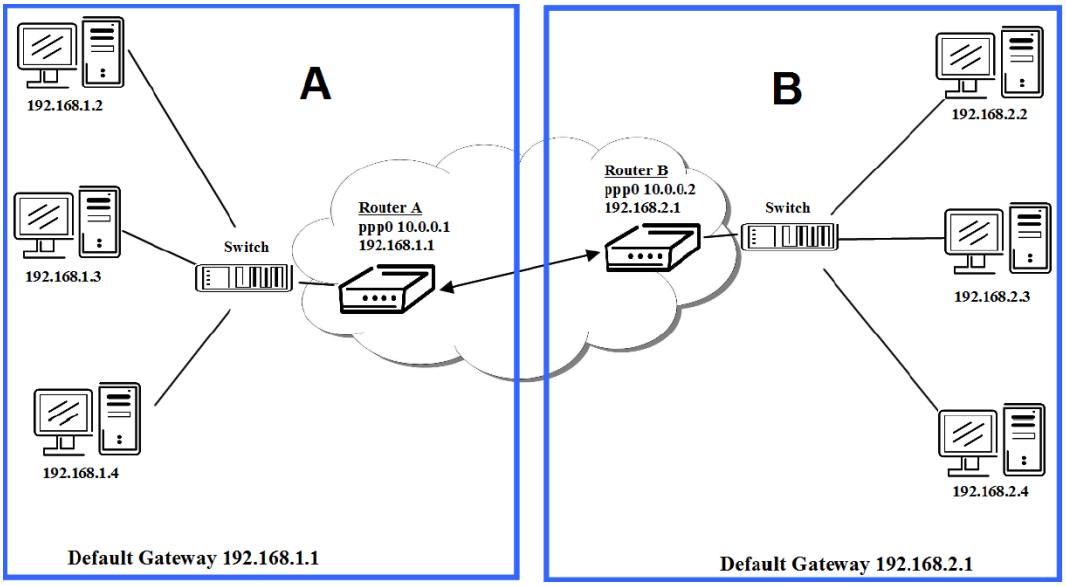
Tabulka 38: Konfigurace L2TP tunelu

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 39: Konfigurace L2TP tunelu

Příklad konfigurace L2TP tunelu:



Obrázek 40: Topologie příkladu konfigurace L2TP tunelu

Konfigurace L2TP tunelu:

Konfigurace	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.1.2	—
Client End IP Address	192.168.1.254	—
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	uživatel	uživatel
Password	heslo	heslo

Tabulka 39: Příklad konfigurace L2TP tunelu

1.20 Konfigurace PPTP tunelu

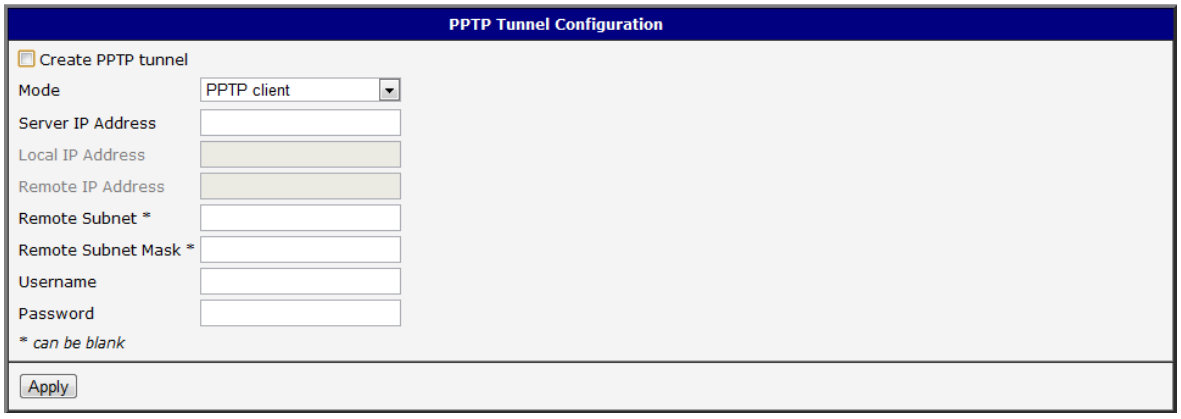
PPTP je nešifrovaný protokol.

Konfiguraci PPTP tunelu lze vyvolat volbou položky *PPTP* v menu. PPTP tunel se používá pro spojení dvou sítí LAN do jedné s autentizací, která se tváří jako homogenní. Jde o obdobný způsob realizace VPN jako L2TP. PPTP tunel se bude vytvářet po zaškrtnutí volby *Create PPTP tunnel*.

Položka	Popis
Mode	Mód PPTP tunelu na straně routeru: • PPTP server – Lze definovat počáteční a konečnou IP adresu rozsahu nabízenou serverem. • PPTP client – Lze definovat IP adresu serveru.
Server IP Address	Adresa serveru.
Local IP Address	IP adresa lokální strany tunelu.
Remote IP Address	IP adresa protější strany tunelu.
Remote Subnet	IP adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Username	Přihlašovací jméno pro přihlášení do PPTP tunelu.
Password	Heslo pro přihlášení do PPTP tunelu.

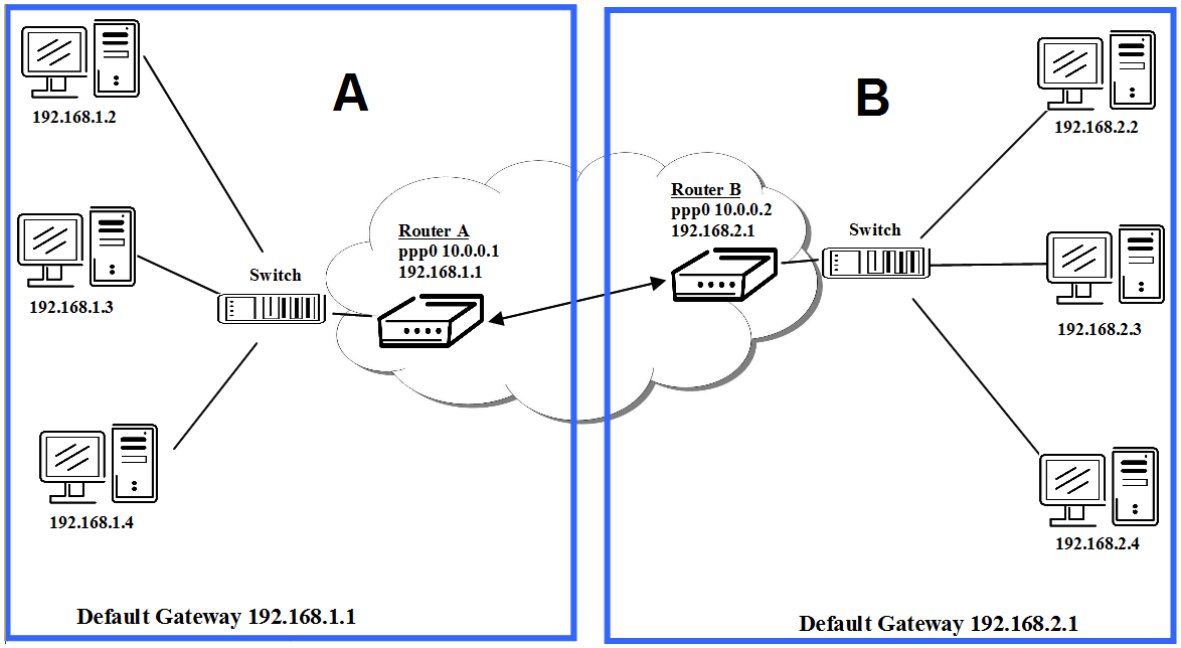
Tabulka 40: Konfigurace PPTP tunelu

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 41: Konfigurace PPTP tunelu

Příklad konfigurace PPTP tunelu:



Obrázek 42: Topologie příkladu konfigurace PPTP tunelu

Konfigurace PPTP tunelu:

Konfigurace	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	uživatel	uživatel
Password	heslo	heslo

Tabulka 41: Příklad konfigurace PPTP tunelu

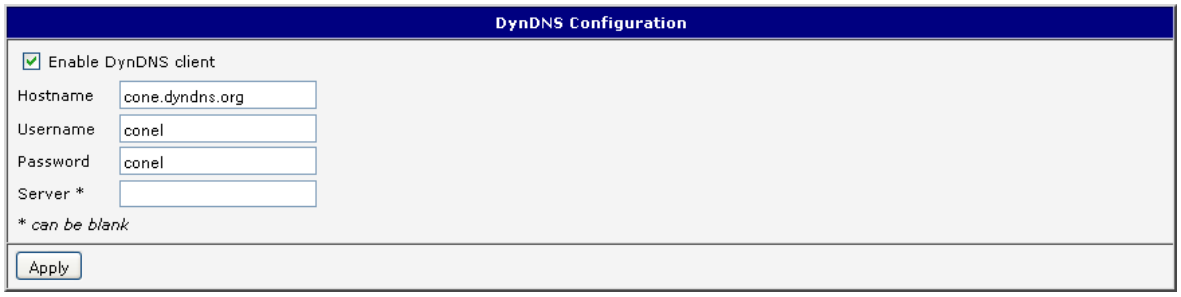
1.21 Konfigurace DynDNS klienta

Konfiguraci DynDNS klienta lze vyvolat volbou položky *DynDNS* v menu. V okně lze definovat doménu třetího řádu registrovanou na serveru www.dyndns.org.

Položka	Popis
Hostname	Doména třetího řádu registrovanou na serveru www.dyndns.org.
Username	Přihlašovací jméno pro přihlášení k DynDNS serveru.
Password	Heslo pro přihlášení k DynDNS serveru.
Server	Chcete-li použít jinou DynDNS službu než www.dyndns.org, zadejte adresu aktualizačního serveru služby do této položky. Pokud tato položka zůstane nevyplněna, používá se výchozí server members.dyndns.org.

Tabulka 42: Konfigurace DynDNS

Příklad konfigurace DynDNS klienta pro doménu conel.dyndns.org:



Obrázek 43: Příklad nastavení DynDNS

1.22 Konfigurace NTP klienta

Konfiguraci NTP klienta lze vyvolat volbou položky *NTP* v menu. NTP (Network Time Protocol) umožňuje pravidelně nastavovat přesný čas do routeru ze serverů, které přesný čas na síti poskytují.

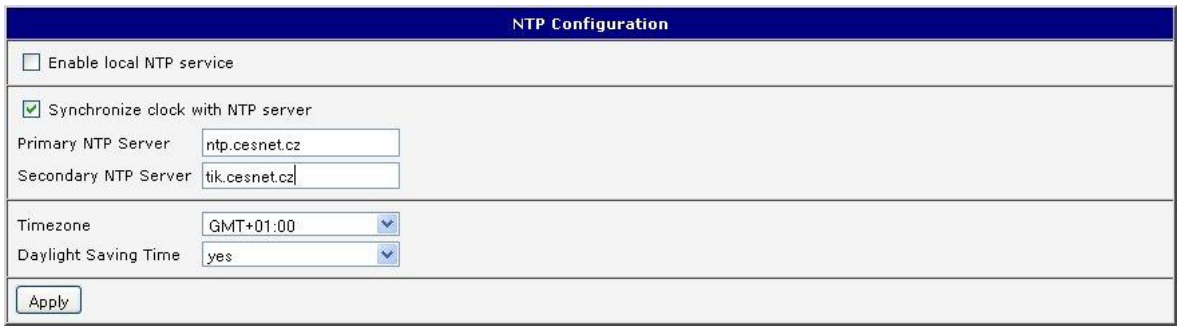
Parametr *Enable local NTP service* nastaví router do režimu, při němž funguje jako NTP server pro ostatní zařízení v lokální síti za routerem.

Parametr *Synchronize clock with NTP server*, nastaví router do režimu NTP klienta, kdy každých 24 hodin router automaticky seřídí vnitřní hodiny.

Položka	Popis
Primary NTP Server Address	IP nebo doménová adresa primárního NTP serveru.
Secondary NTP Server Address	IP nebo doménová adresa sekundárního NTP serveru.
Timezone	Tímto parametrem lze nastavit časové pásmo routeru.
Daylight Saving Time	Tímto parametrem je možné povolit časový posun pomocí letního času.: • No – Časový posun je zakázán. • Yes – Časový posun je povolen.

Tabulka 43: Konfigurace NTP

Na následujícím obrázku je uveden příklad konfigurace NTP s nastaveným primárním (ntp.cesnet.cz) a sekundárním (Htik.cesnet.cz) NTP serverem a s nastavením změny času při přechodu mezi zimním a letním časem:



Obrázek 44: Příklad nastavení NTP

1.23 Konfigurace SNMP agenta

Vyvoláním položky *SNMP* je možná konfigurace SNMP agenta v1/v2 nebo v3, který zasílá informace o routeru, případně o stavu volitelném portu CNT nebo MBUS.

SNMP (Simple Network Managment Protocol) poskytuje stavové informace o prvcích sítě, jakými jsou routery nebo koncové počítače. Pro povolení této služby zatrhněte položku *Enable SNMP agent*.

Položka	Popis
Name	Definuje pojmenování routeru.
Location	Popisuje fyzické umístění routeru.
Contact	Identifikuje osobu, která spravuje router, společně s informacemi jak tuto osobu kontaktovat.

Tabulka 44: Konfigurace SNMP agenta

Aktivace SNMPv1/v2 se provádí pomocí položky *Enable SNMPv1/v2 access*. Zároveň je potřeba nadefinovat heslo pro přístup k SNMP agentovi (*Community*), což standardně bývá *public*, který je předdefinován.

Položka *Enable SNMPv3 access* umožňuje aktivovat SNMPv3, přičemž je nutné nadefinovat následující parametry:

Položka	Popis
Username	Uživatelské jméno
Authentication	Šifrovací algoritmus na autentizačním protokolu, který se používá pro zajištění totožnosti uživatelů.
Authentication Password	Autentizační heslo, které slouží k vygenerování klíče používaného pro autentizaci.
Privacy	Šifrovací algoritmus na Privacy protokolu, které slouží k zajištění důvěrnosti dat.
Privacy Password	Heslo pro šifrování na Privacy protokolu

Tabulka 45: Konfigurace SNMPv3

Dále je možná tato konfigurace:

- Zaškrtnutím volby *Enable I/O extension* je možné sledovat stav I/O vstupů na routeru.
- Zaškrtnutím volby *Enable XC-CNT extension* je možné sledovat stav vstupů a výstupů volitelného portu CNT.
- Zaškrtnutím volby *Enable M-BUS extension* a nastavením následujících parametrů lze sledovat stav připojených měřidel na volitelném portu MBUS.

Položka	Popis
Baudrate	Komunikační rychlosti.
Parity	Control parity bit: • none – Nebude odesílána žádná parita. • even – Bude odesílána sudá parita. • odd – Bude odesílána lichá parita.
Stop Bits	Počtu stop bitů.

Tabulka 46: Konfigurace SNMP (MBUS extension)

Parametry *Enable XC-CNT extension* a *Enable M-BUS extension* nemohou být zaškrtnuty **zároveň**.

Zaškrtnutím volby *Enable reporting to supervisory system* a nastavením parametrů uvedených v tabulce níže je možné povolit odesílání statistických informací do monitorovacího systému R-SeeNet.

Položka	Popis
IP Address	IP adresa
Period	Interval odesílání statistických informací (v minutách)

Tabulka 47: Konfigurace SNMP (R-SeeNet)

Každá sledovaná hodnota je jednoznačně identifikována pomocí číselného identifikátoru *OID – Object Identifier*. Pro I/O vstupy a výstupy je použit následující rozsah OID (vnitřních proměnných):

OID	Význam
.1.3.6.1.4.1.30140.2.3.1.0	Binární vstup BIN0 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binární výstup OUT0 (hodnoty 0,1)

Tabulka 48: Vnitřní proměnné pro vstupy a výstupy routeru

Pro volitelný port CNT je použit následující rozsah OID (vnitřních proměnných):

OID	Význam
.1.3.6.1.4.1.30140.2.1.1.0	Analogový vstup AN1 (rozsah 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogový vstup AN2 (rozsah 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Čítačový vstup CNT1 (rozsah 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Čítačový vstup CNT2 (rozsah 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binární vstup BIN1 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binární vstup BIN2 (hodnoty 0,1)

Pokračování na následující straně

Pokračování z předchozí strany

OID	Význam
.1.3.6.1.4.1.30140.2.1.7.0	Binární vstup BIN3 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binární vstup BIN4 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binární výstup OUT1 (hodnoty 0,1)

Tabulka 49: Vnitřní proměnné pro CNT port

Pro volitelný port M-BUS je použit následující rozsah OID (vnitřních proměnných):

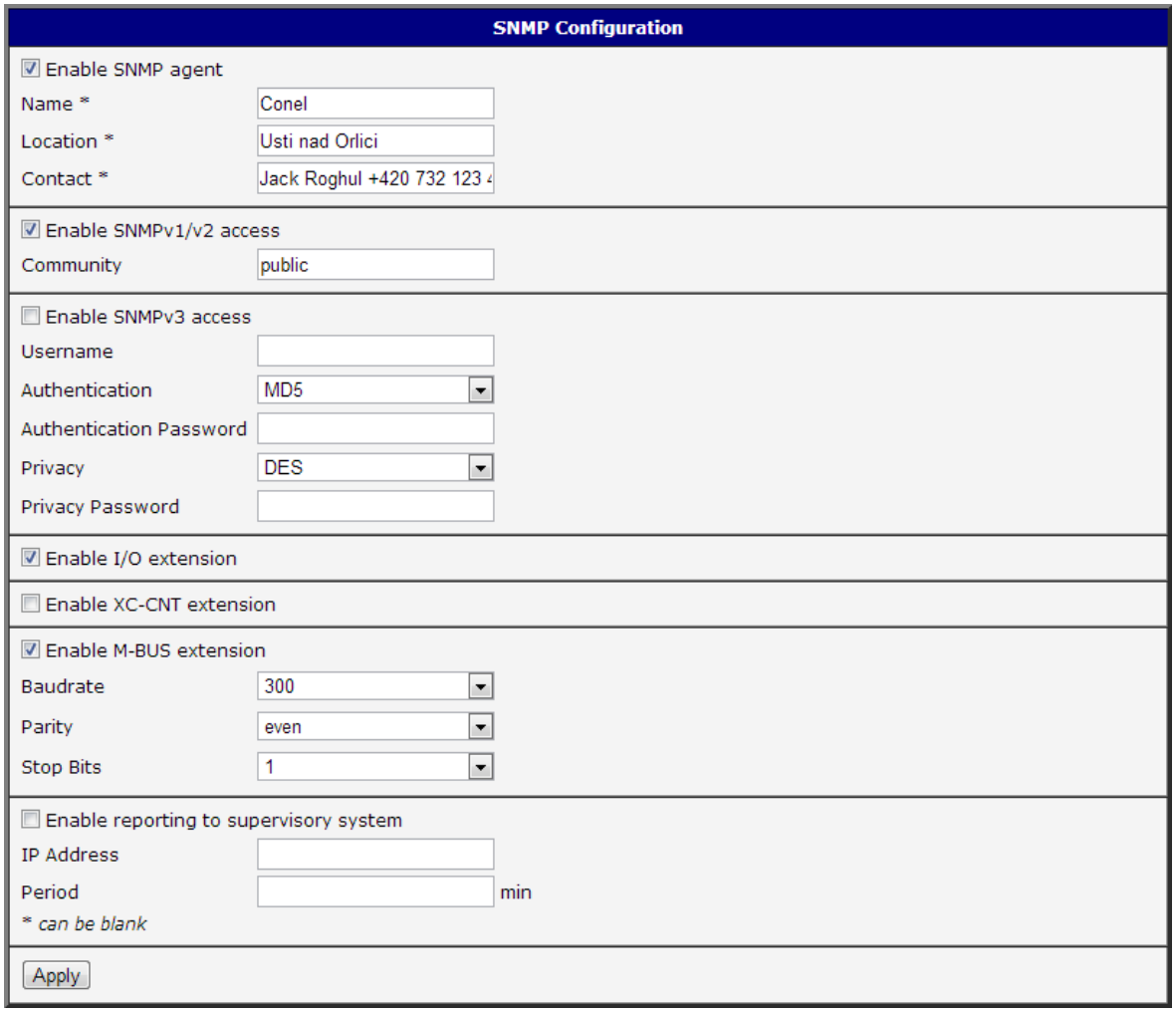
OID	Význam
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – číslo měřiče
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer – výrobce
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – specifikuje verzi měřiče
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – typ měřeného média
.1.3.6.1.4.1.30140.2.2.<address>.5.0	Status – hlášení chybových stavů
.1.3.6.1.4.1.30140.2.2.<address>.6.0	0. VIF – informační pole hodnoty
.1.3.6.1.4.1.30140.2.2.<address>.7.0	Out
.1.3.6.1.4.1.30140.2.2.<address>.8.0	1. VIF – informační pole hodnoty
.1.3.6.1.4.1.30140.2.2.<address>.9.0	1. měřená hodnota
.1.3.6.1.4.1.30140.2.2.<address>.10.0	2. VIF – informační pole hodnoty
.1.3.6.1.4.1.30140.2.2.<address>.11.0	2. měřená hodnota
.1.3.6.1.4.1.30140.2.2.<address>.12.0	3. VIF – informační pole hodnoty
.1.3.6.1.4.1.30140.2.2.<address>.13.0	3. měřená hodnota
⋮	⋮
.1.3.6.1.4.1.30140.2.2.<address>.100.0	47. VIF – informační pole hodnoty
.1.3.6.1.4.1.30140.2.2.<address>.101.0	47. měřená hodnota

Tabulka 50: Vnitřní proměnné pro M-BUS port

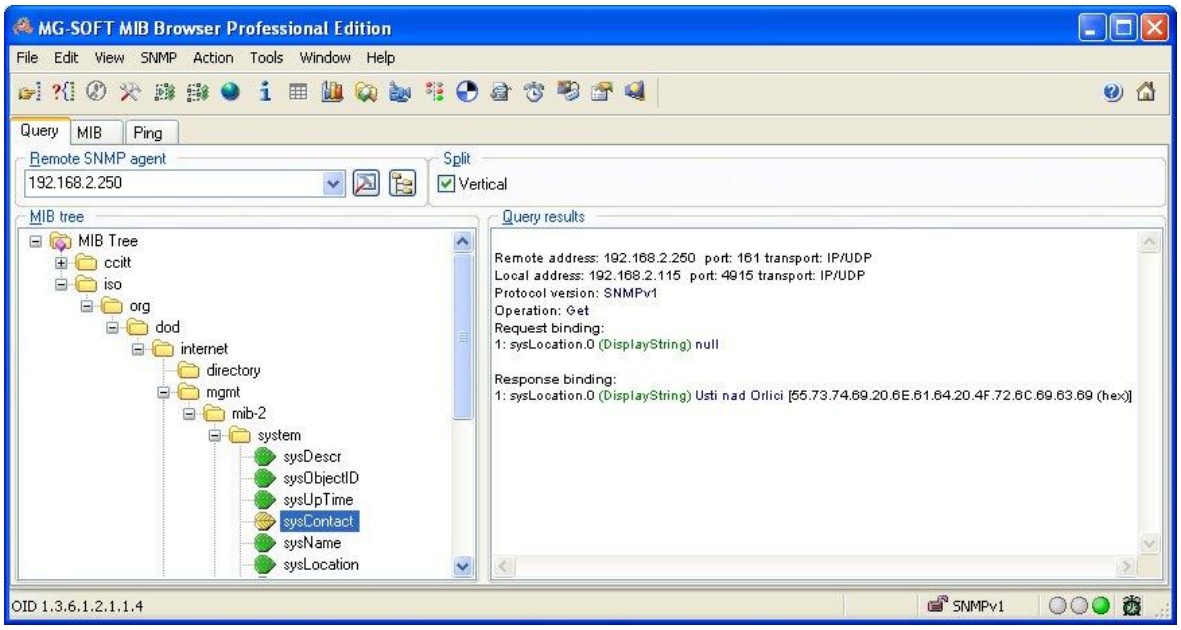
Adresa měřiče může být z rozsahu 0..254, kdy 254 je broadcast.

Počínaje firmwarem 3.0.4 je možné sledovat vnitřní teplotu (OID 1.3.6.1.4.1.30140.3.3) a získávat informace o napájecím napětí (OID 1.3.6.1.4.1.30140.3.4). Tyto funkce jsou však dostupné pouze pro routery se základní deskou RB-v2-6 a novější.

Příklad nastavení a vyčtení SNMP:



Obrázek 45: Příklad SNMP konfigurace



Obrázek 46: Příklad MIB prohlížeče

Důležité je nastavit IP adresu SNMP agenta (router) v poli *Remote SNMP agent*. Po zadání IP adresy je v části *MIB tree* možné zobrazit vnitřní proměnné. Dále lze stav vnitřních proměnných zjistit zadáním jejich OID.

Cesta k proměnným je:

iso → org → dod → internet → private → enterprises → conel → protocols

Cesta k základním informacím o routeru je:

iso → org → dod → internet → mgmt → mib-2 → system

1.24 Konfigurace SMTP

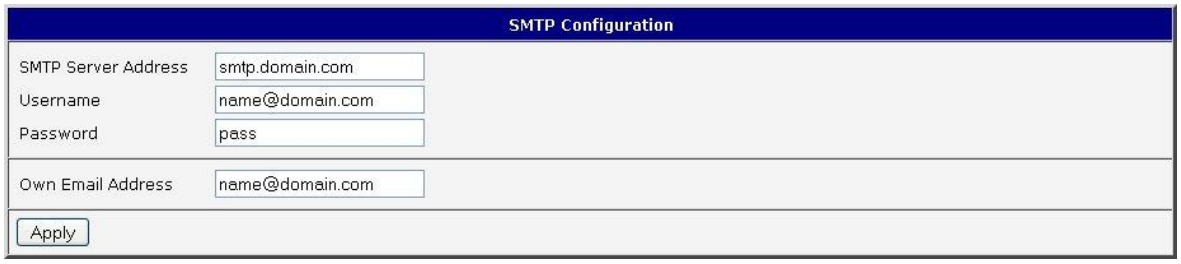
Vyvoláním položky *SMTP* je možná konfigurace SMTP (Simple Mail Transfer Protocol) klienta, pomocí kterého se nastavuje odesílání emailů.

Položka	Popis
SMTP Server Address	Doménová nebo IP adresa e-mail serveru.
Username	Uživatelské jméno k emailovému účtu.
Password	Heslo k emailovému účtu.
Own Email Address	Email odesílatele.

Tabulka 51: Konfigurace SMTP klienta

Mobilní operátor může blokovat jiné SMTP servery. V takovém případě lze použít pouze SMTP server operátora.

Příklad nastavení SMTP klienta:



Obrázek 47: Příklad SMTP konfigurace

Samotné emaily lze posílat ze Startup skriptu nebo v Telnet rozraní. Pomocí příkazu *email* s následujícími parametry.

- -t Email příjemce
- -s Předmět zprávy (předmět zprávy musí být ohraničen uvozovkami)
- -m Zpráva (zpráva musí být ohraničena uvozovkami)
- -a Příloha
- -r Počet pokusů odeslání emailu (standardně jsou nastaveny 2 pokusy)

Příkazy a parametry mohou být zapsány pouze malými písmeny.

Příklad odeslaného e-mailu:

email –t name@domain.com –s "predmet" –m "zprava" –a c:\directory\abc.doc –r 5

Tento příkaz odešle e-mail na adresu name@domain.com s předmětem zprávy *"predmet"*, tělem zprávy *"zprava"* a přílohou *"abc.doc"* z adresáře c:\directory\ a s 5 pokusy o odeslání.

1.25 Konfigurace posílání SMS

U průmyslového routeru XR5i v2 není položka SMS Configuration k dispozici.

SMS konfigurace se vyvolá volbou položky *SMS* v hlavním menu. Nastavení definuje možnosti posílání SMS zpráv z routeru při různých definovaných událostech a stavech routeru. V první části okna se konfiguruje posílání SMS.

Položka	Popis
Send SMS on power up	Automatické poslání SMS po zapnutí napájení.
Send SMS on connect to mobile network	Automatické poslání SMS po připojení do mobilní sítě.
Send SMS on disconnect to mobile network	Automatické poslání SMS po ztrátě připojení do mobilní sítě.
Send SMS when datalimit exceeded	Automatické poslání SMS při překročení datového limitu.
Send SMS when binary input on I/O port (BIN0) is active	Automatické poslání SMS při aktivním binárním výstupu routeru, jejíž text je určen parametrem BIN0.
Send SMS when binary input on expansion port (BIN1 – BIN4) is active	Automatické poslání SMS při aktivním binárním výstupu na volitelné CNT desce, jejíž text je určen parametrem BIN1-SMS až BIN4-SMS.
Add timestamp to SMS	Přidává časovou značku (razítko) do poslaných SMS. Tato značka má fixní formát YYYY-MM-DD hh:mm:ss.
Phone Number 1	Telefonní číslo pro odesílání automaticky generovaných SMS.
Phone Number 2	Telefonní číslo pro odesílání automaticky generovaných SMS.
Phone Number 3	Telefonní číslo pro odesílání automaticky generovaných SMS.
Unit ID	Pojmenování routeru, které bude zasláno v SMS.
BIN0 – SMS	Text SMS při aktivaci bin. vstupu na routeru.
BIN1 – SMS	Text SMS při aktivaci bin. vstupu 1 na CNT desce.
BIN2 – SMS	Text SMS při aktivaci bin. vstupu 2 na CNT desce.
BIN3 – SMS	Text SMS při aktivaci bin. vstupu 3 na CNT desce.
BIN4 – SMS	Text SMS při aktivaci bin. vstupu 4 na CNT desce.

Tabulka 52: Konfigurace posílání SMS

Ve druhé části je možné nakonfigurovat ovládání routeru pomocí SMS zpráv. Po zaškrtnutí volby *Enable remote control via SMS* je možné ovládat router pomocí SMS zpráv.

Položka	Popis
Phone Number 1	Ovládání routeru je možné nastavit až pro tři telefonní čísla. Pokud je nastaveno ovládání routeru pomocí SMS zpráv, všechny příchozí SMS se automaticky zpracují a smažou. V defaultním nastavení je tento parametr zapnut.
Phone Number 2	Ovládání routeru je možné nastavit až pro tři telefonní čísla. Pokud je nastaveno ovládání routeru pomocí SMS zpráv, všechny příchozí SMS se automaticky zpracují a smažou. V defaultním nastavení je tento parametr zapnut.
Phone Number 3	Ovládání routeru je možné nastavit až pro tři telefonní čísla. Pokud je nastaveno ovládání routeru pomocí SMS zpráv, všechny příchozí SMS se automaticky zpracují a smažou. V defaultním nastavení je tento parametr zapnut.

Tabulka 53: Konfigurace ovládání pomocí SMS

Pokud není vyplněno žádné telefonní číslo, je možné pouze znovuspustit router zasláním SMS ve tvaru *Reboot* z libovolného čísla. Při vyplnění jednoho, nebo více čísel lze ovládat router pomocí SMS zaslaných pouze z těchto čísel. Vložením znaku $*$ je možné ovládat router z kteréhokoliv čísla.

Ovládací SMS zprávy nemění konfiguraci routeru. Pokud je router například přepnut do režimu offline pomocí SMS zprávy, zůstane v tomto režimu jen do příštího restartu routeru. Toto chování je stejné pro všechny ovládací SMS zprávy.

Ovládací SMS jsou možné ve tvaru:

SMS	Význam
go online sim 1	Přepnutí na první SIM (APN1)
go online sim 2	Přepnutí na druhou SIM (APN2)
go online	Přepne router do online režimu
go offline	Ukončení spojení
set out0=0	Nastaví výstup I/O konektoru na 0
set out0=1	Nastaví výstup I/O konektoru na 1
set out1=0	Nastaví výstup volitelného portu CNT na 0
set out1=1	Nastaví výstup volitelného portu CNT na 1
set profile std	Nastavení standardního profilu
set profile alt1	Nastavení alternativního profilu 1
set profile alt2	Nastavení alternativního profilu 2

Pokračování na následující straně

Pokračování z předchozí strany

SMS	Význam
set profile alt3	Nastavení alternativního profilu 3
reboot	Reboot routeru
get ip	Odešle odpověď s IP adresou SIM karty

Tabulka 54: Význam ovládacích SMS

Volbou *Enable AT-SMS protocol on expansion port 1* a nastavením rychlosti (*Baudrate*) je možné povolit posílání/příjem SMS zpráv na sériovém portu na Portu 1.

SMS	Význam
Baudrate	Rychlost na volitelném portu 1.

Tabulka 55: Posílání/Příjem zpráv na sériovém portu 1

Volbou *Enable AT-SMS protocol on expansion port 2* a nastavením rychlosti (*Baudrate*) je možné povolit posílání/příjem SMS zpráv na sériovém portu.

SMS	Význam
Baudrate	Rychlost na volitelném portu 2.

Tabulka 56: Posílání/Příjem zpráv na sériovém portu 2

Volbou *Enable AT-SMS protocol on TCP port* je možné povolit posílání/příjem SMS zpráv na TCP portu. SMS zprávy se posílají pomocí standardních AT příkazů.

SMS	Význam
TCP Port	Port na které bude povolen posílání/příjem SMS zpráv.

Tabulka 57: Posílání/Příjem zpráv na zadaném TCP portu

1.25.1 Práce s SMS

Po sestavení spojení s routerem přes sériové rozhraní či Ethernet, je možné pomocí AT příkazů pracovat s SMS zprávami.

V následující tabulce jsou uvedeny pouze AT příkazy, které jsou podporovány routery firmy Conel. Na ostatní příkazy je vždy posílána odpověď *OK*. Není podporováno zpracování složených AT příkazu (oddělených středníkem), tudíž na ně router posílá odpověď *ERROR*.

AT příkaz	Popis
AT+CGMI	Identifikuje výrobce daného zařízení
AT+CGMM	Vypisuje identifikační označení zařízení
AT+CGMR	Vypisuje informaci o verzi systému
AT+CGPADDR	Vrací IP adresu rozhraní ppp0
AT+CGSN	Zobrazí sériové číslo zařízení
AT+CIMI	Vrací hodnotu čísla označovaného jako IMSI (unikátní číslo pro SIM kartu)
AT+CMGD	Mazání SMS zprávy podle jejího indexu
AT+CMGF	Nastavuje režim psaní SMS zpráv
AT+CMGL	Vypisuje seznam uložených SMS zpráv
AT+CMGR	Čtení určité SMS zprávy (všechny SMS mají svůj index)
AT+CMGS	Posílá SMS na uvedené telefonní číslo
AT+CMGW	Ukládá zprávu do paměti
AT+CMSS	Odesílá zprávu z paměti (na základě zadané pozice zprávy)
AT+COPS?	Identifikuje aktuálně dostupné mobilní sítě
AT+CPIN	Dotazování a zadávání PIN kódu
AT+CPMS	SDefinuje paměť pro práci s SMS
AT+CREG	Zobrazuje stav registrace v síti
AT+CSCA	Nastavuje číslo servisního střediska pro SMS zprávy
AT+CSCS	Nastavuje používanou znakovou sadu
AT+CSQ	Udává kvalitu přijímaného signálu
AT+GMI	Identifikuje výrobce daného zařízení
AT+GMM	Vypisuje identifikační označení zařízení
AT+GMR	Vypisuje informaci o verzi systému
AT+GSN	Zobrazí sériové číslo zařízení
ATE	Stylem ozvěny vrací zadané příkazy odesílateli
ATI	Zobrazuje základní informace poskytované výrobcem

Tabulka 58: AT příkazy pro práci s SMS

Podrobnější popis těchto příkazů a příklady jejich použití najdete v aplikační příručce pojmenované *AT příkazy*.

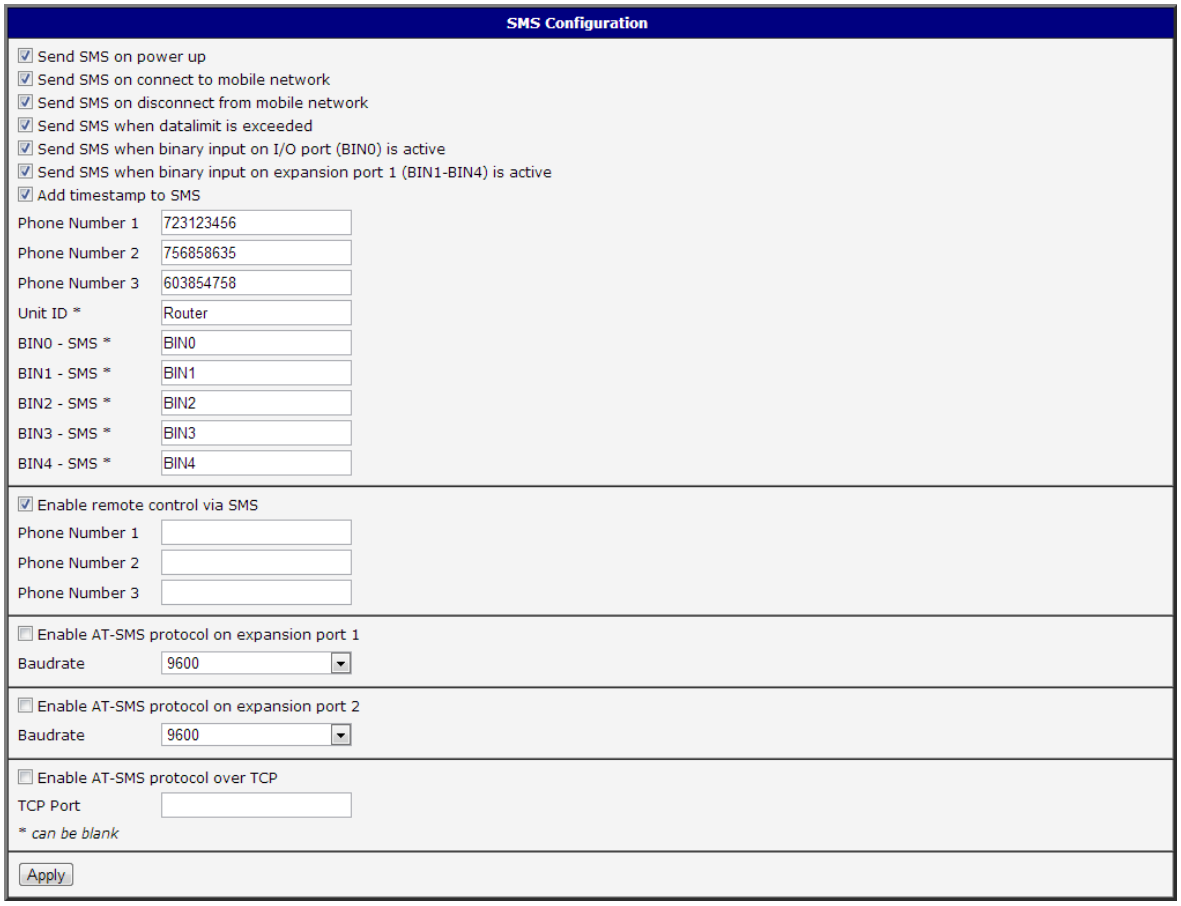
Příklad nastavení posílání SMS:

Po zapnutí napájení (*Power up*) přijde na uvedené telefonní číslo sms ve tvaru:
Router (*Unit ID*) has been powered up. Signal strenght: -xx dBm, kde signal strenght udává úroveň signálu.

Při sestavení spojení přijde na uvedené telefonní číslo SMS ve tvaru:
Router (*Unit ID*) has established connection to mobile network. IP address: xxx.xxx.xxx.xxx

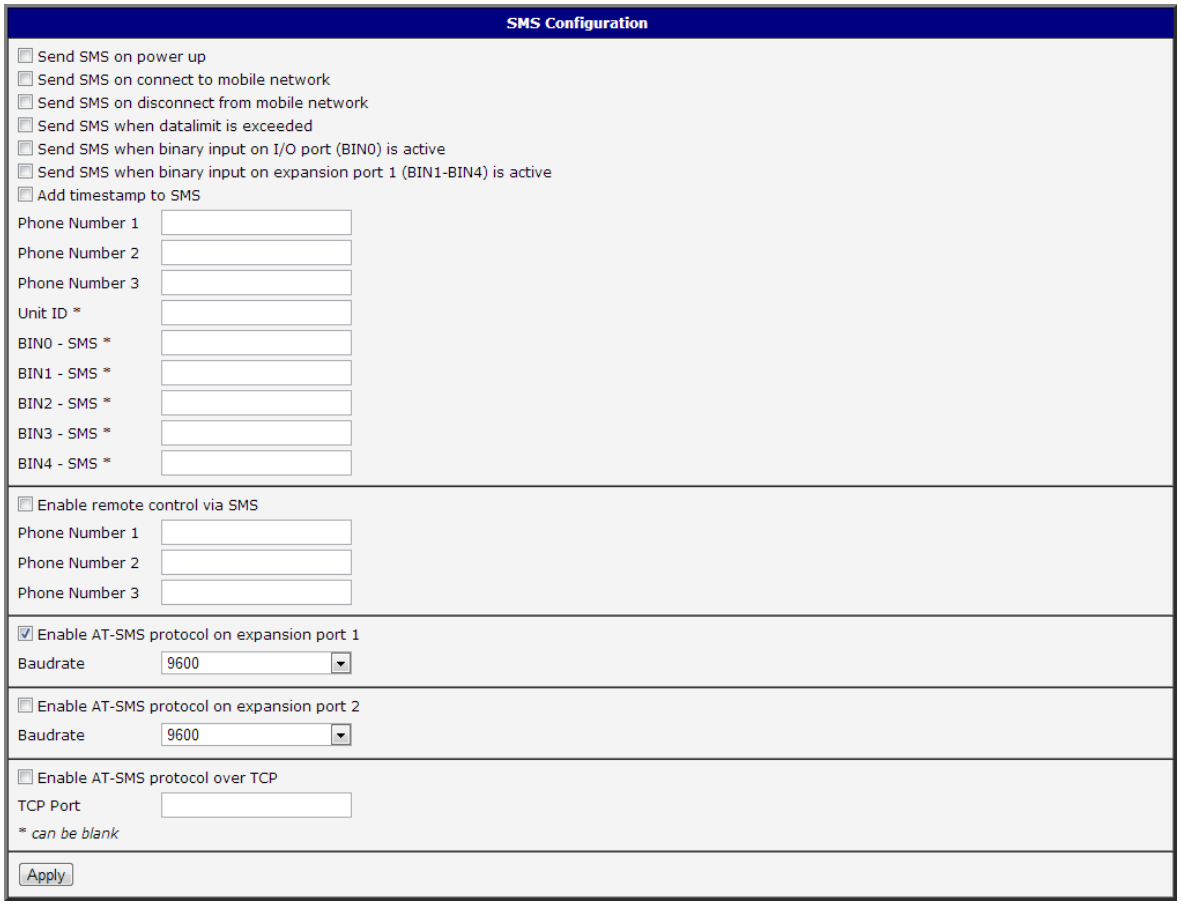
Po ztrátě spojení přijde na uvedené telefonní číslo SMS ve tvaru:
Router (*Unit ID*) has lost connection to mobile network. IP address: xxx.xxx.xxx.xxx

Nastavení posílání těchto SMS je:



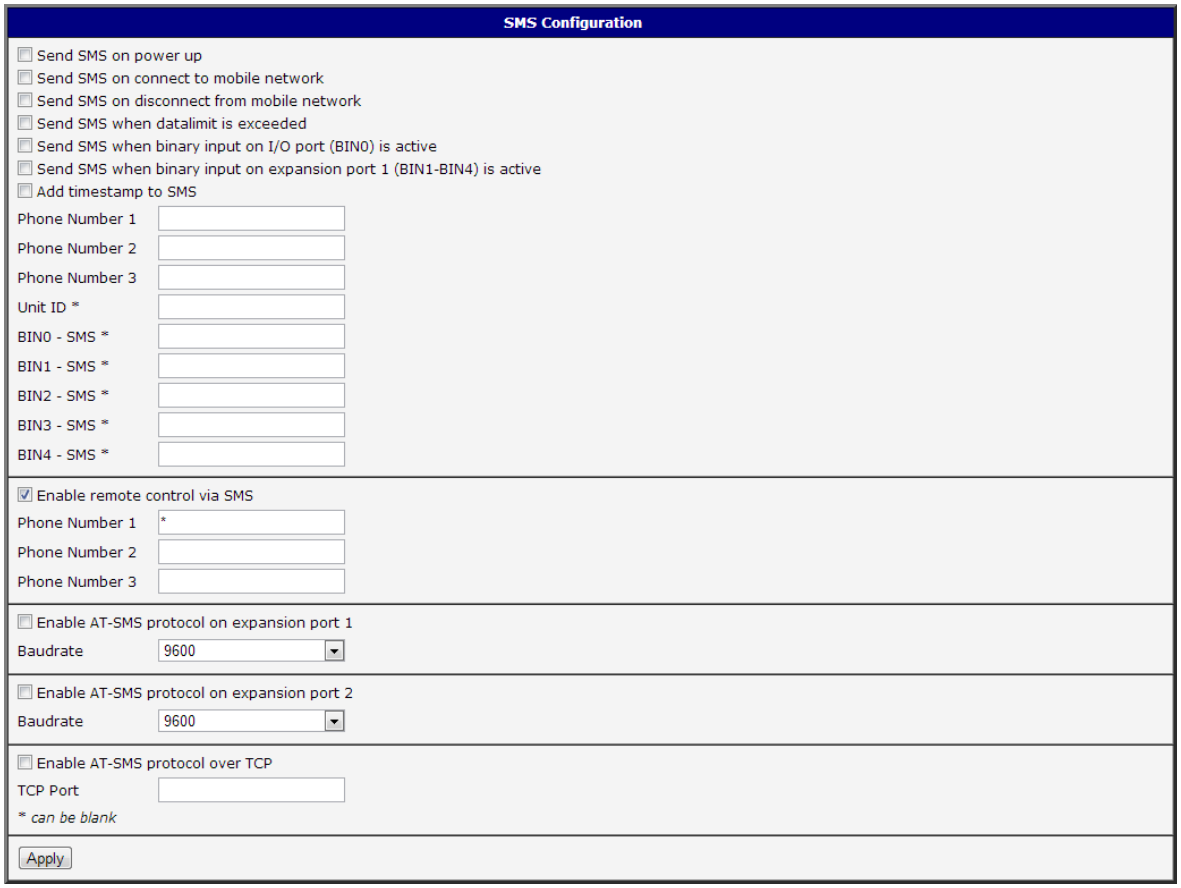
Obrázek 48: Příklad nastavení SMS konfigurace 1

Příklad nastavení routeru pro posílání SMS zpráv přes sériové rozhraní portu PORT1:



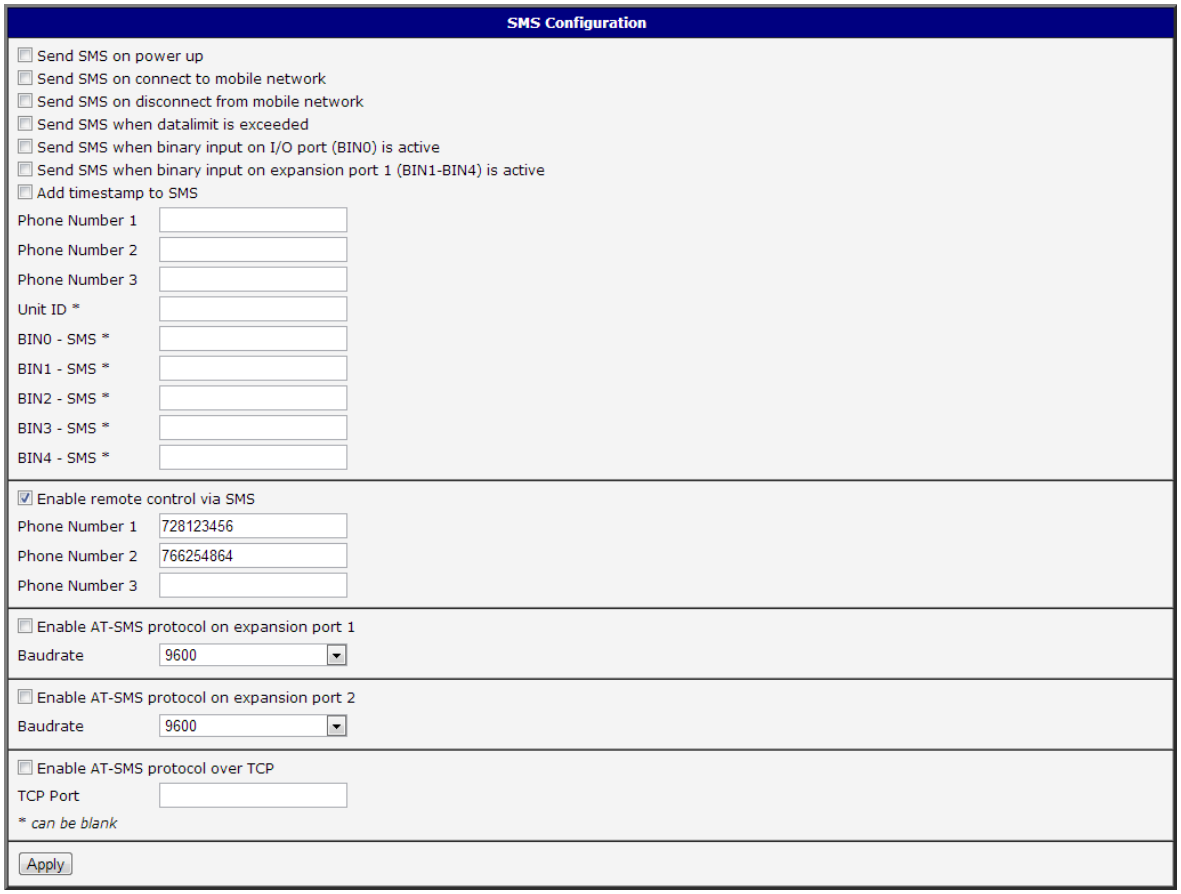
Obrázek 49: Příklad nastavení SMS konfigurace 2

Příklad nastavení routeru pro ovládání pomocí SMS zpráv z libovolného tel. čísla:



Obrázek 50: Příklad nastavení SMS konfigurace 3

Příklad nastavení routeru pro ovládání pomocí SMS zpráv ze dvou tel. čísel:



Obrázek 51: Příklad nastavení SMS konfigurace 4

1.26 Konfigurace volitelného portu

Konfiguraci volitelných portů PORT1 a PORT2 je možné vyvolat volbou položky *Expansion Port 1* nebo *Expansion Port 2*.

Položka	Popis
Baudrate	Komunikační rychlost.
Data Bits	Počet datových bitů.
Parity	Kontrolní paritní bit: • none – Nebude odesílána žádná parita. • even – Bude odesílána sudá parita. • odd – Bude odesílána lichá parita.
Stop Bits	Počet stop bitů.
Split Timeout	Nastavuje dobu pro roztržení zprávy. Pokud při přijímání dojde k rozpoznání mezery mezi dvěma znaky, která je delší než hodnota parametru v milisekundách, pak je ze všech přijatých dat sestavená zpráva a odeslána.
Protocol	Protokol: • TCP – Komunikace pomocí spojového protokolu TCP. • UDP – Komunikace pomocí nespojového protokolu UDP.
Mode	Režim komunikace: • TCP server – Router naslouchá příchozím žádostem na zadaném portu. • TCP client – Router se připojuje na zadanou adresu serveru na zadaném portu.
Server Address	V režimu TCP klienta je nutné zadat adresu serveru.
TCP Port	TCP/UDP port na kterém probíhá komunikace.

Tabulka 59: Konfigurace volitelného portu 1

Při zaškrtnutí volby *Check TCP connection* se aktivuje kontrola navázaného TCP spojení.

Položka	Popis
Keepalive Time	Doba, po které se provádí kontrola spojení
Keepalive Interval	Doba čekání na odpověď
Keepalive Probes	Počet pokusů

Tabulka 60: Konfigurace volitelného portu 2

Při zaškrtnutí položky *Use CD as indicator of TCP connection* se aktivuje funkce indikace stavu TCP spojení pomocí signálu CD (DTR na straně routeru).

CD	Popis
Active	TCP spojení je sestavené
Nonactive	TCP spojení není sestavené

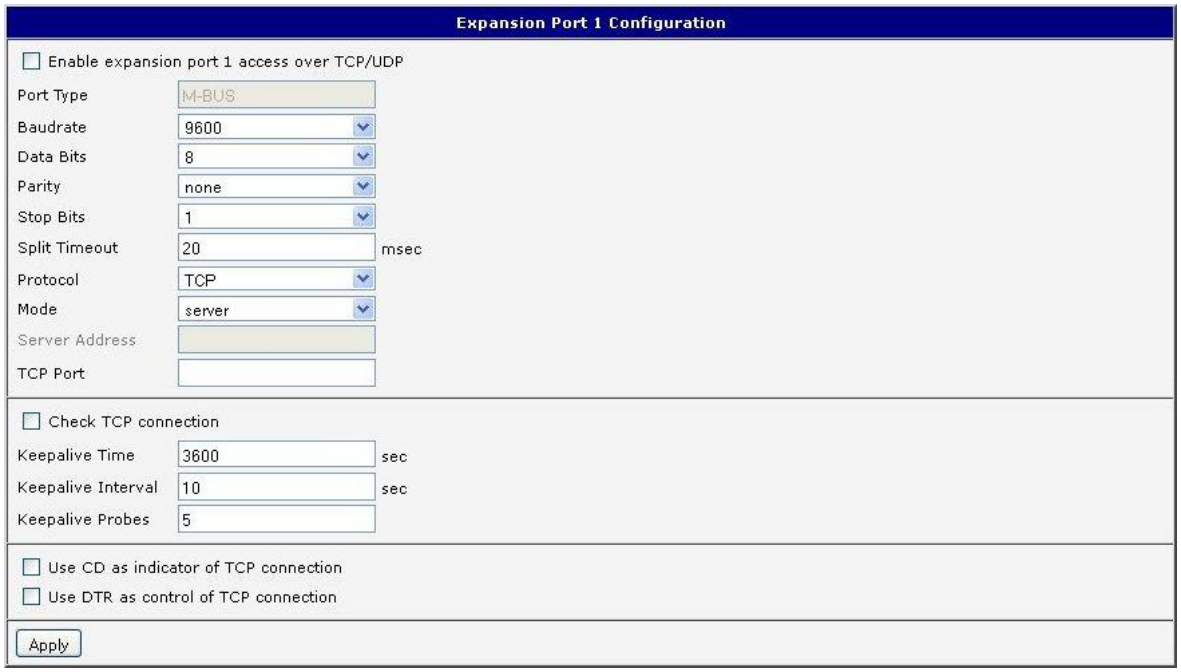
Tabulka 61: Popis signálu CD

Při zaškrtnutí položky *Use DTR as control of TCP connection* se aktivuje funkce řízení TCP spojení pomocí signálu DTR (CD na straně routeru).

DTR	Popis chování serveru	Popis chování klienta
Active	Router povolí sestavení TCP spojení	Router sestaví TCP spojení
Nonactive	Router nepovolí sestavení TCP spojení	Router rozpojí TCP spojení

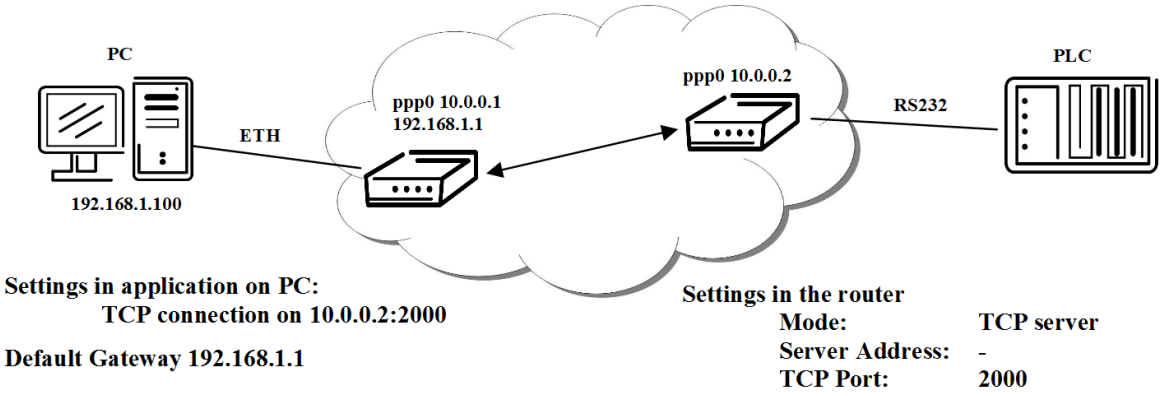
Tabulka 62: Popis signálu DTR

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.

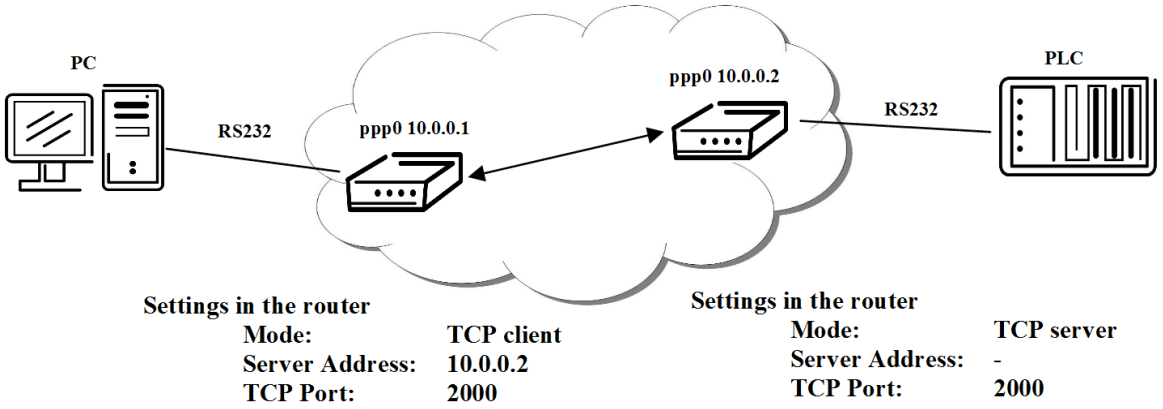


Obrázek 52: Konfigurace volitelného portu

Příklad konfigurace volitelného portu:



Obrázek 53: Příklad nastavení volitelného portu 1



Obrázek 54: Příklad nastavení volitelného portu 2

1.27 Konfigurace USB portu

Konfiguraci portu USB lze vyvolat volbou položky *USB Port* v menu. Konfiguraci je možné provést, pokud máme k dispozici převodník USB/RS232.

Položka	Poips
Baudrate	Komunikační rychlost RS232.
Data Bits	Počet datových bitů.
Parity	Kontrolní paritní bit: • none – Nebude odesílána žádná parita. • even – Bude odesílána sudá parita. • odd – Bude odesílána lichá parita.
Stop Bits	Počet stop bitů.
Split Timeout	Nastavuje dobu pro roztržení zprávy. Pokud při přijímání dojde k rozpoznání mezery mezi dvěma znaky, která je delší než hodnota parametru v milisekundách, pak je ze všech přijatých dat sestavená zpráva a odeslána.
Protocol	Komunikační protokol: • TCP – Komunikace pomocí spojového protokolu TCP. • UDP – Komunikace pomocí nespojového protokolu UDP.
Mode	Režim komunikace: • TCP server – Router naslouchá příchozím žádostem na zadaném portu. • TCP client – Router se připojuje na zadanou adresu serveru na zadaném portu.
Server Address	V režimu TCP klienta je nutné zadat adresu serveru.
TCP Port	TCP/UDP port na kterém probíhá komunikace.

Tabulka 63: Konfigurace USB portu 1

Při zaškrtnutí volby *Check TCP connection* se aktivuje kontrola navázaného TCP spojení.

Položka	Popis
Keepalive Time	Doba, po které se provádí kontrola spojení
Keepalive Interval	Doba čekání na odpověď
Keepalive Probes	Počet pokusů

Tabulka 64: Konfigurace USB portu 2

Při zaškrtnutí položky *Use CD as indicator of TCP connection* se aktivuje funkce indikace stavu TCP spojení pomocí signálu CD (DTR na straně routeru).

CD	Popis
Active	TCP spojení je sestavené
Nonactive	TCP spojení není sestavené

Tabulka 65: Popis signálu CD

Při zaškrtnutí položky *Use DTR as control of TCP connection* se aktivuje funkce řízení TCP spojení pomocí signálu DTR (CD na straně routeru).

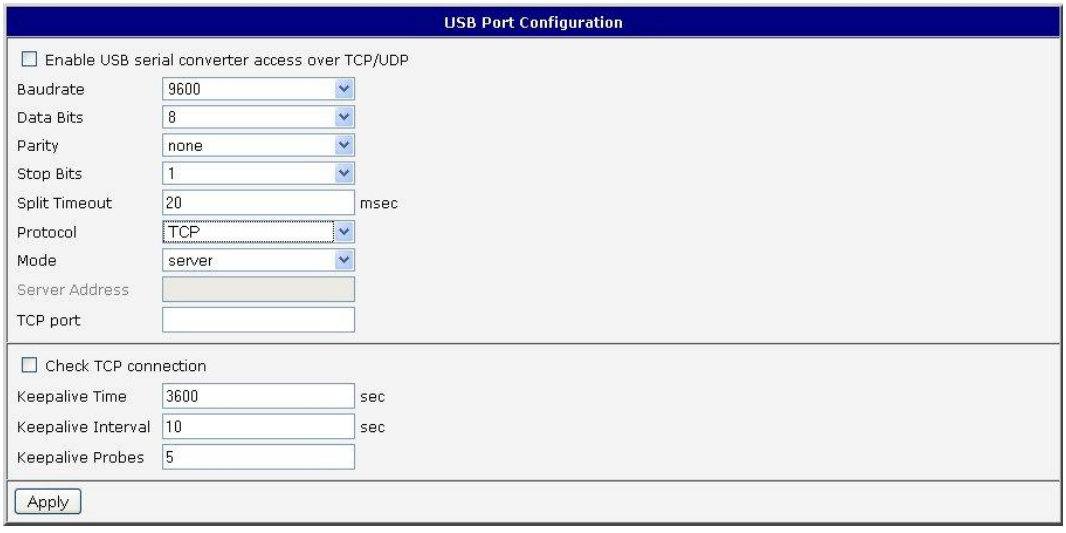
DTR	Popis chování serveru	Popis chování klienta
Active	Router povolí sestavení TCP spojení	Router sestaví TCP spojení
Nonactive	Router nepovolí sestavení TCP spojení	Router rozpojí TCP spojení

Tabulka 66: Popis signálu DTR

Podporované USB/RS232 převodníky:

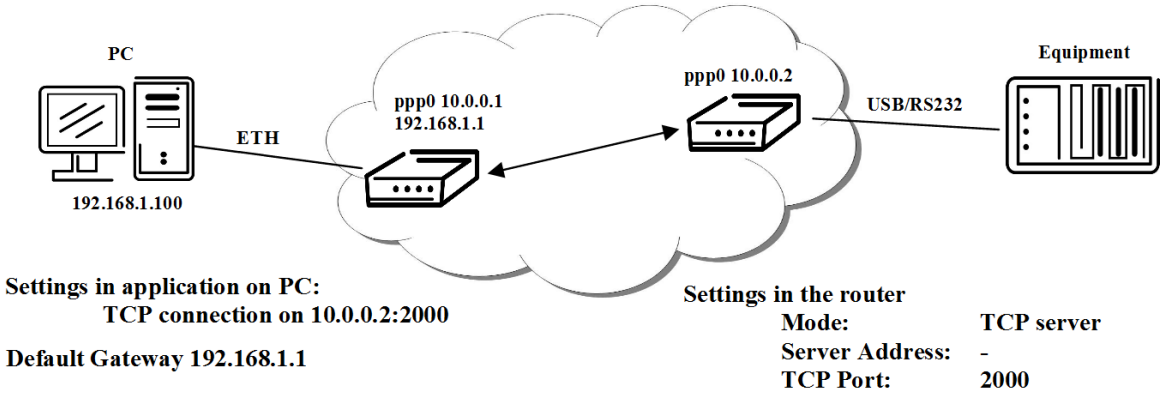
- FTDI
- Prolific PL2303
- Silicon Laboratories CP210× (Podporován od firmware verze 3.0.1)

Změny v nastavení se projeví po stisknutí tlačítka *Apply*.

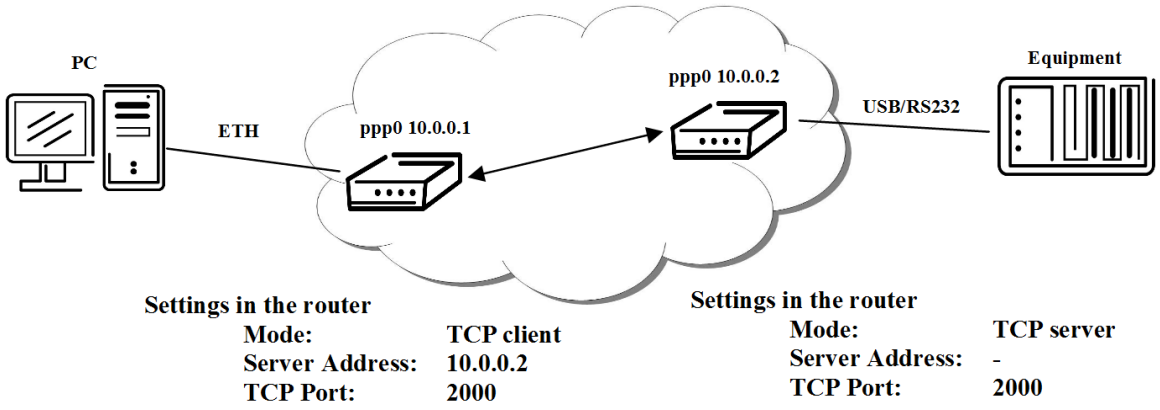


Obrázek 55: Konfigurace USB

Příklad konfigurace USB portu:



Obrázek 56: Příklad nastavení USB portu 1

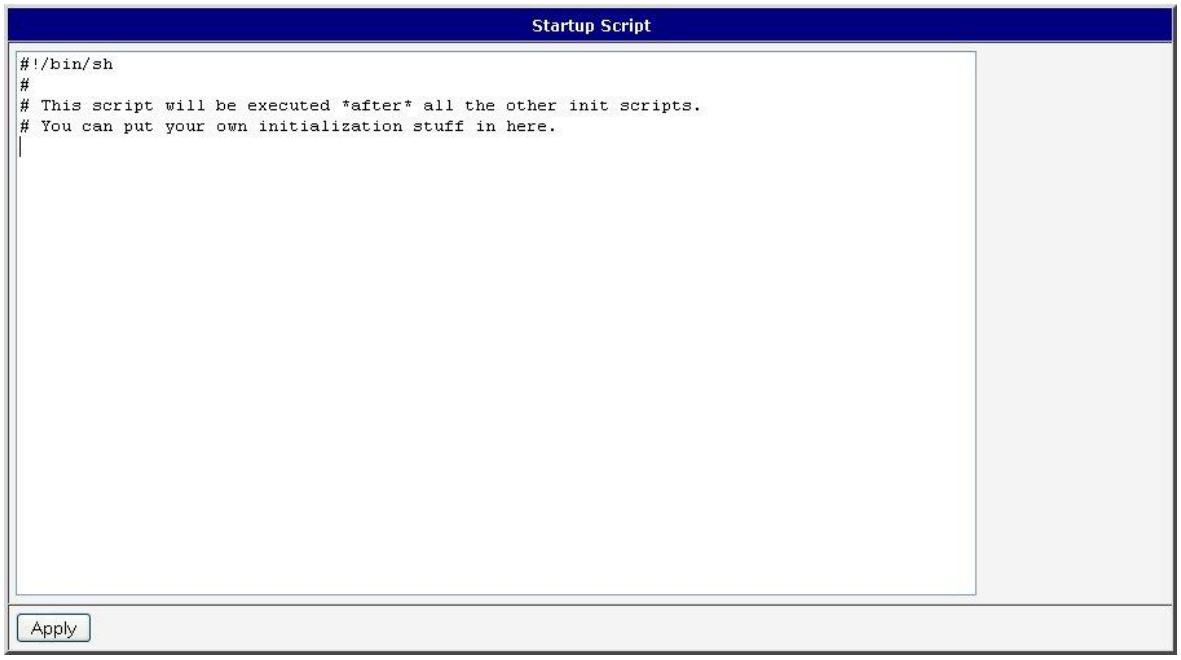


Obrázek 57: Příklad nastavení USB portu 2

1.28 Startup Script

V okně *Startup Script* lze vytvářet vlastní skripty, které budou spuštěny po init skriptech.

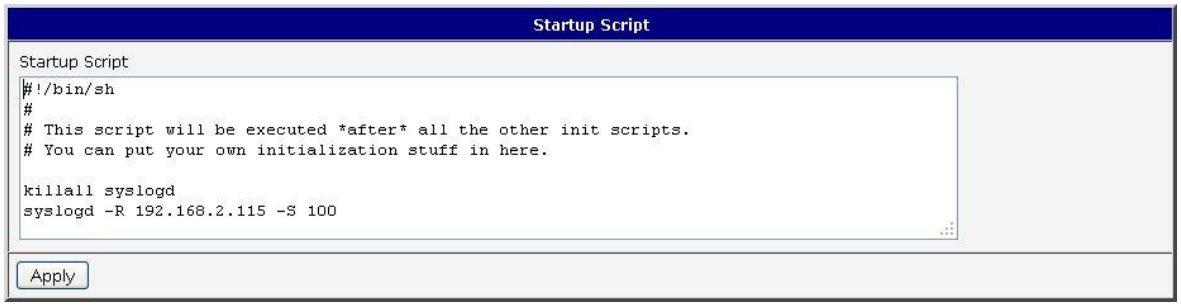
Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 58: Startup script

Aby se skripty projevily v chování routeru, je důležité router vypnout a znovu nastartovat pomocí tlačítka *Reboot* ve webové administraci nebo pomocí SMS zprávy.

Příklad Startup skriptu: Při startu routeru zastaví program syslogd a následně je spuštěn se vzdáleným logováním na adresu 192.168.2.115 a omezený výpisem na 100 záznamů.

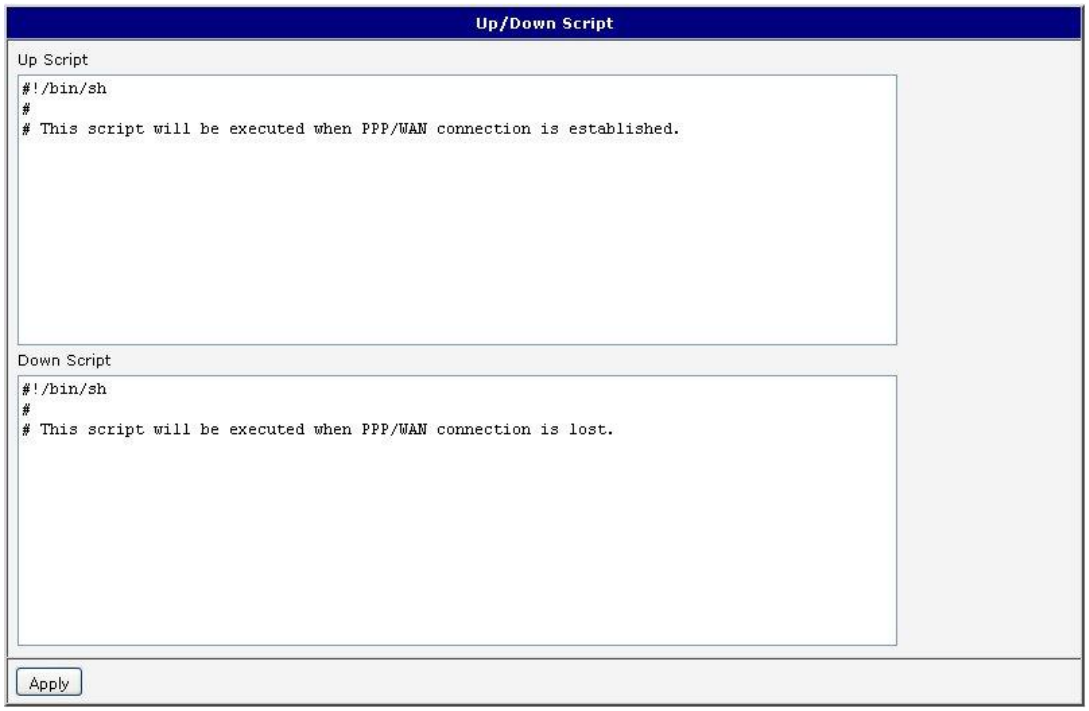


Obrázek 59: Příklad Startup scriptu

1.29 Up/Down Script

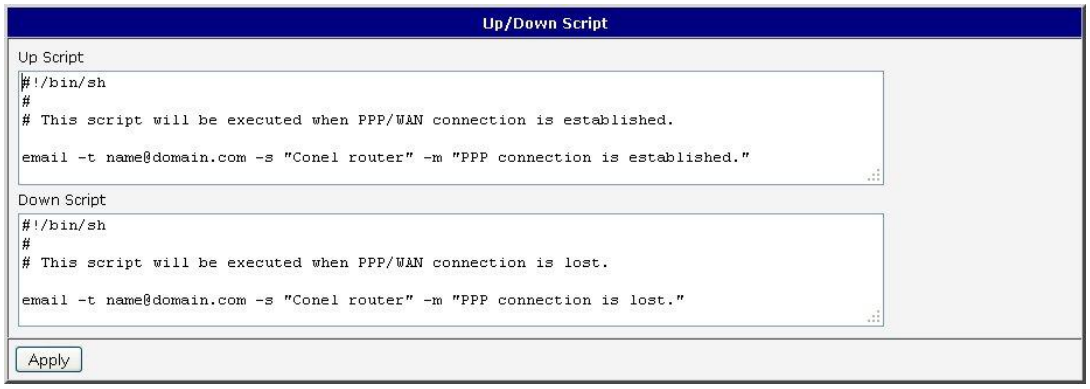
V okně *Up/Down Script* je také možné vytvářet vlastní skripty. Skripty zapsané v poli *Up Script* budou spuštěny po inicializaci PPP (u průmyslového routeru XR5i v2 PPPoE spojení). Do pole *Down Script* se zapisují skripty, které budou spuštěny při výpadku nebo po ztrátě spojení (u průmyslového routeru XR5i v2 PPPoE spojení).

Změny v nastavení se projeví až po stisknutí tlačítka *Apply*.



Obrázek 60: Up/Down Script

Příklad Up/Down skriptu: Po navázání nebo ztrátě spojení router odešle email s informací o navázání nebo ztrátě spojení.



Obrázek 61: Příklad Up/Down Scriptu

1.30 Konfigurace automatické aktualizace

Konfiguraci automatické aktualizace nastavení routeru je možné vyvolat v menu položkou *Automatic Update*. Na základě této funkce si router si sám automaticky stahuje konfiguraci anebo aktuální firmware ze serveru, kde je konfigurační soubor nebo firmware uložen. Aby se předešlo případné manipulaci s aktualizací, dochází ke kontrole stahovaného souboru (archivu typu tar.gz). Nejprve se prověří formát stahovaného archivu, následně typ architektury a na konec se provede kontrola jednotlivých souborů v archivu.

Zaškrtnutím *Enable automatic update of configuration* je možné povolit automatickou aktualizaci nastavení routeru.

Parametrem *Enable automatic update of firmware* je možné povolit automatickou aktualizaci firmware routeru.

Položka	Popis
Source	Nastavuje, odkud bude router aktuální firmware stahovat: • HTTP/FTP server – Aktualizace se stahují z adresy zadané v položce *Base URL*. • USB flash drive – Router hledá aktuální firmware v kořenovém adresáři zařízení připojeného do USB portu. • Both – Router hledá aktuální firmware z obou zdrojů.
Base URL	Umožňuje zadat základní část doménového jména nebo IP adresy serveru, ze které se bude firmware nebo konfigurace routeru stahovat.
Unit ID	Název stahované konfigurace. Jestliže není Unit ID vyplněno, pak se jako název souboru použije MAC adresa routeru. (Jako oddělovací znak je místo dvojtečky použita tečka.)
Update Hour	Pomocí této položky lze nastavit hodinu (rozsah 1-24), ve kterou bude každý den prováděna automatická aktualizace. Pokud hodina není zadána, probíhá automatická aktualizace 5 minut po zapnutí routeru a pak každých 24 hodin. Je-li na zadané URL rozdílná konfigurace než v routeru, router si tuto konfiguraci nahraje a poté se restartuje.

Tabulka 67: Konfigurace automatické aktualizace

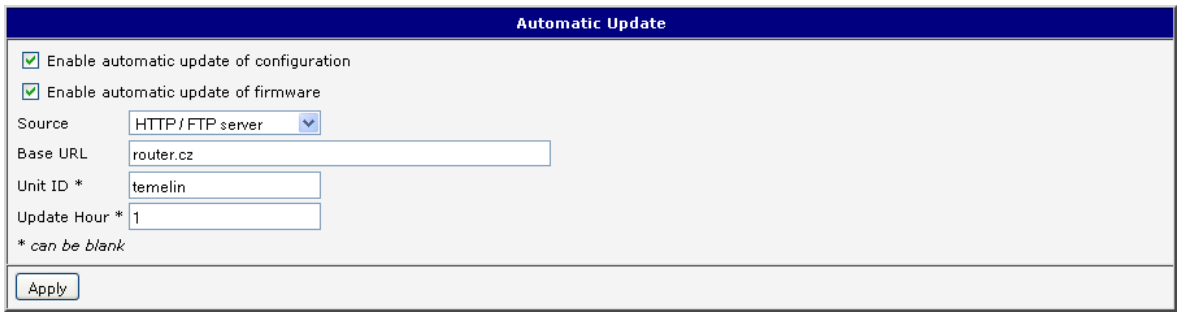
Název stahovaného *konfiguračního souboru* se skládá z parametru *Base URL*, hardwarové MAC adresy rozhraní eth0 routeru a přípony *cfg*. Hardwarová MAC adresa a přípona *cfg* se připojuje automaticky a není třeba je nikde vyplňovat. Parametrem *Unit ID* lze definovat konkrétní název stahovaného souboru, který bude stažen do routeru. V případě použití tohoto parametru bude místo MAC adresy použit parametr *Unit ID*.

Název stahovaného *firmware* se skládá z parametru *Base URL*, typu routeru a přípony *bin*.

Na HTTP/FTP server je nutné vždy nahrát dva soubory – .bin a .ver. Pokud by byl na server nahrán pouze soubor s příponou .bin a HTTP by při pokusu o stahování neexistujícího souboru .ver odeslalo chybnou odpověď *200 OK* (místo očekávané *404 Not Found*), pak je zde vysoké riziko, že router bude stahovat soubor .bin stále dokola.

Následující příklady zjišťují, jestli je k dispozici nový firmware nebo konfigurace a případně provádí aktualizaci každý den v 1:00 ráno. Příklad je uveden pro typ routeru ER75i v2.

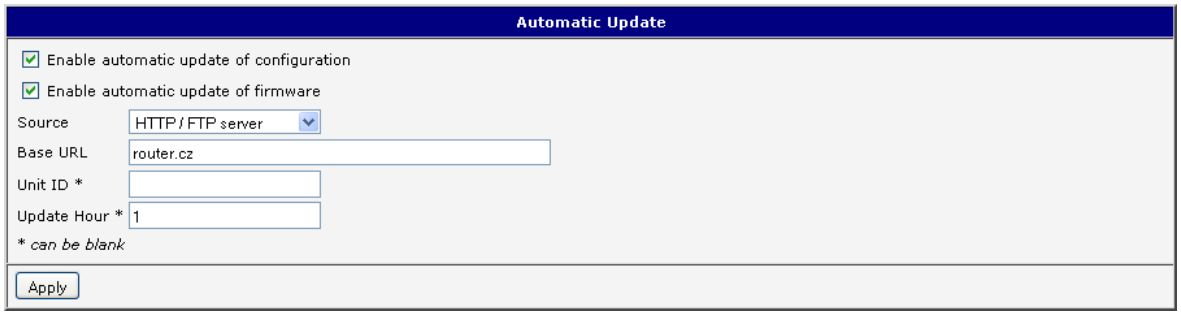
- Firmware: http://router.cz/er75i-v2.bin
- Konfigurační soubor: http://router.cz/temelin.cfg



Obrázek 62: Příklad automatické aktualizace 1

Následující příklady zjišťují, jestli je k dispozici nový firmware nebo konfigurace a případně provádí aktualizaci každý den v 1:00 ráno. Příklad je uveden pro typ routeru ER75i v2 s MAC adresou 00:11:22:33:44:55.

- Firmware: http://router.cz/er75i-v2.bin
- Konfigurační soubor http://router.cz/00.11.22.33.44.55.cfg



Obrázek 63: Příklad automatické aktualizace 2

1.31 Správa uživatelských modulů

Konfiguraci uživatelských modulů lze vyvolat volbou položky *User Modules*. V tomto okně lze přidávat nové programové moduly, odstraňovat je a přecházet do jejich konfigurace. Stisknutím tlačítka *Procházet...* zvolte požadovaný modul (přeložený modul má koncovku tgz) a přidejte jej kliknutím na tlačítko *Add*.

Obrázek 64: User modules

Přidaný modul se zobrazí v seznamu modulů na téže stránce. Pokud modul obsahuje stránku index.html nebo index.cgi, slouží název modulu jako odkaz na tuto stránku. Dále je možné modul smazat tlačítkem *Delete*.

Aktualizace uživatelského modulu se provádí stejným způsobem jako přidání nového modulu. Modul s vyšší verzí (novější) nahradí stávající modul. Původní konfigurace modulu je po aktualizaci zachována.

Programování a překlad uživatelských modulů je popsáno v programátorské příručce.

Obrázek 65: Přidán uživatelský modul

Dostupné jsou například tyto uživatelské moduly:

Název modulu	Poips
MODBUS TCP2RTU	Zajišťuje převod protokolu MODBUS TCP/IP na protokol MODBUS RTU, který je možný provozovat na sériové lince.
Easy VPN client	Zajišťuje zabezpečené propojení sítě LAN za naším routerem a sítě LAN za CISCO routerem.
NMAP	Umožňuje provádět TCP a UDP scan.
Daily Reboot	Umožňuje provádět denní restart routeru v daném čase.
HTTP Authentication	Tento modul doplňuje proces ověřování identity (autentizaci) k serveru, který tuto službu neposkytuje.
BGP, RIP, OSPF	Doplňují podporu dynamických protokolů BGP, RIP, OSPF.
PIM SM	Doplňuje podporu multicastového směrovacího protokolu PIM-SM.

Pokračování na následující straně

Pokračování z předchozí strany

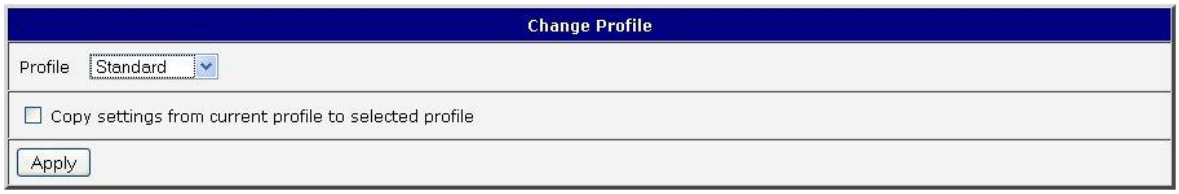
Název modulu	Poips
WMBUS Concentrator	Umožňuje přijímat zprávy od WMBUS měřičů a poté ukládat jejich obsah do souboru ve formátu XML.
pduSMS	Odesílá krátké textové zprávy (SMS) na zvolené číslo.
GPS	Umožňuje v2 routerům využívat polohový družicový systém, s jehož pomocí je možno určit polohu a přesný čas kdekoliv na světě, kde je přímá viditelnost na čtyři či více GPS satelitů.
Pinger	Umožňuje manuálně nebo automaticky ověřovat funkčnost spojení mezi dvěma síťovými rozhraními (tzv. pingat).
WiFi STA	Umožňuje routeru, aby se choval jako klasická WiFi klientská stanice.
IS-IS	Doplňuje podporu protokolu IS-IS.

Tabulka 68: Uživatelské moduly

1.32 Změna profilu

Dialog pro změnu profilu lze vyvolat volbou položky *Change Profile* v menu. Přepnutí profilu se provede stisknutím tlačítka *Apply*. Změny v konfiguraci routeru se projeví až po jeho restartu. V nabídce je možné zvolit standardní nebo až tři alternativní profily. Zaškrtnutím volby *Copy settings from current profile to selected profile* je také možné zkopírovat aktuálně platný profil do zde vybraného profilu.

Příklad využití profilů: Profily lze využít například pro přepínání mezi různými režimy provozu routeru (router má sestavené spojení, router nemá sestavené spojení, router vytváří tunel do servisního střediska). Změnu profilu lze poté provést pomocí binárního vstupu, SMS zprávy nebo z webového rozhranní routeru.

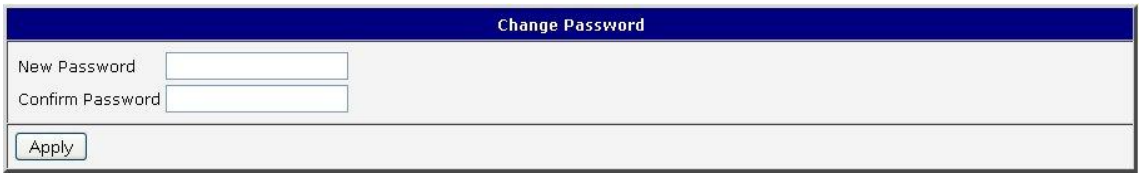


Obrázek 66: Změna profilu

1.33 Změna přístupového hesla

Dialog pro změnu hesla lze vyvolat volbou položky *Change Password* v menu. Nové heslo se uloží po stisknutí tlačítka *Apply*.

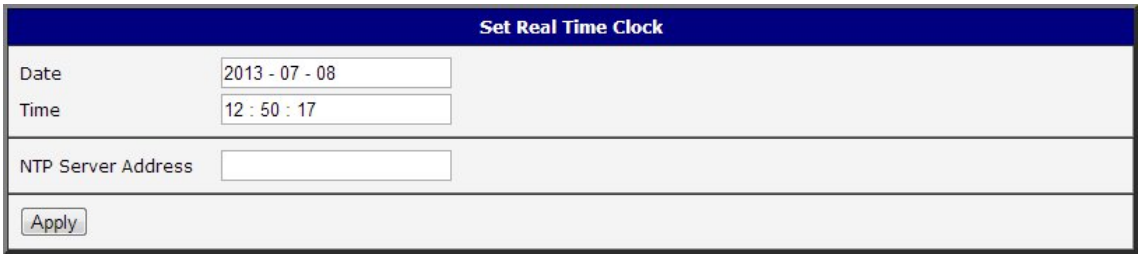
V základním nastavení routeru je heslo nastaveno defaultně na *root*. Pro zajištění bezpečnosti sítě spravované routerem důrazně doporučujeme toto heslo změnit.



Obrázek 67: Změna přístupového hesla

1.34 Nastavení vnitřních hodin

Jednorázové nastavení vnitřních hodin routeru lze vyvolat volbou položky *Set Real Time Clock* v menu. Hodiny a datum lze nastavit ručně prostřednictvím položek *Date* a *Time*. Údaje zadávejte vždy ve formátu, který je znázorněn na obrázku níže. Hodiny lze seřídit také podle zadaného NTP serveru po stisknutí tlačítka *Apply*.

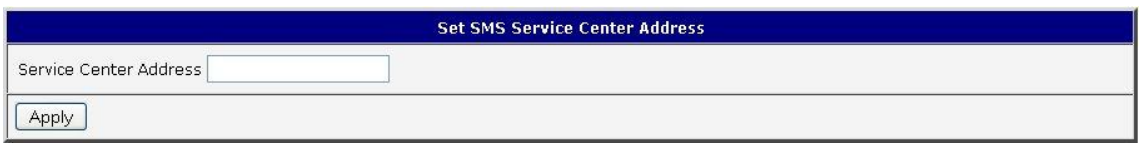


Obrázek 68: Nastavení vnitřních hodin

1.35 Nastavení SMS centra

U průmyslového routeru XR5i v2 není položka *Set SMS Service Center Address* dostupná.

V některých případech je nutné nastavit telefonní číslo SMS centra, aby se odesílaly uživatelské SMS zprávy. Parametr se nemusí nastavovat u SIM karet, které mají telefonní číslo SMS centra nastavené od operátora. Telefonní číslo může mít tvar bez mezinárodní předpony xxx xxx xxx nebo s mezinárodní předponou +420 xxx xxx xxx.



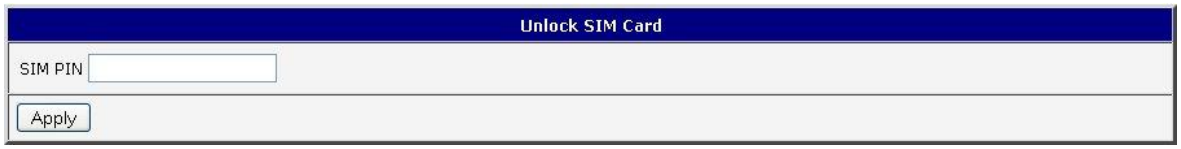
Obrázek 69: Nastavení SMS centra

1.36 Odemknutí SIM karty

U průmyslového routeru XR5i v2 není položka *Unlock SIM Card* dostupná.

Možnost odemknutí SIM karty je dostupná pod položkou *Unlock SIM Card*. Pokud je SIM karta vložená do routeru chráněná PINem, napíše se PIN (čtyřmístné číslo) do pole SIM PIN a odemkne se kliknutím na tlačítko *Apply*.

SIM karta je zablokována po třech neúspěšných pokusech o zadání PIN kódu.

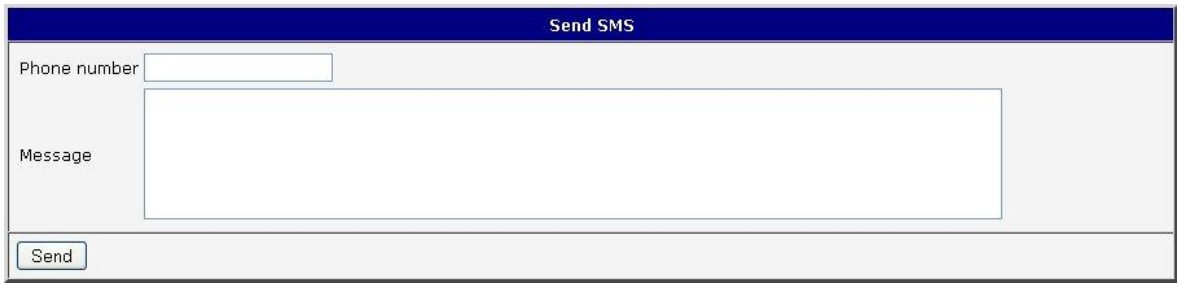


Obrázek 70: Odemknutí SIM karty

1.37 Poslání SMS zprávy

U průmyslového routeru XR5i v2 není položka *Send SMS* dostupná.

Poslání SMS zprávy je možné v okně *Send SMS*. Po vložení telefonního čísla příjemce (*Phone number*) a textu SMS zprávy (*Message*) se zpráva odešle pomocí tlačítka *Send*.



Obrázek 71: Poslání SMS zprávy

Odeslání SMS zprávy přes HTTP dotaz pak je ve tvaru:

GET/send_exec.cgi?phone=%2B420712345678&message=Test HTTP/1.1
Authorization: Basic cm9vdDpyb290

HTTP dotaz se pošle do TCP spojení na port 80 routeru Na základě výše uvedeného příkazu router pošle SMS s textem *Test*. SMS je poslána na telefonní číslo *420712345678*. Autorizace je ve formátu *user:password* zakódovaná BASE64. V příkladu je použit *root:root*.

1.38 Zálohování konfigurace

Konfiguraci modemu je možné uložit pomocí položky *Backup Configuration*. Po kliknutí je možné vybrat cílový adresář, kam se uloží konfigurační soubor routeru.

1.39 Obnovení konfigurace

Pokud je potřeba obnovit konfiguraci routeru, je možné v položce *Restore Configuration* vybrat konfigurační soubor pomocí tlačítka *Procházet*.

Obrázek 72: Obnovení konfigurace

1.40 Aktualizace firmware

Informace o verzi firmware a pokyny pro jeho aktualizaci lze vyvolat volbou položky *Update Firmware* v menu. Nový firmware je vybrán přes položku *Procházet* a zaktualizuje následným stisknutím tlačítka *Update*. Celková doba aktualizace trvá přibližně tři minuty.

Obrázek 73: Aktualizace firmware

Po úspěšné aktualizaci firmwaru se vypíše následující výpis:

Uploading firmware to RAM... ok
Programming FLASH..... ok

Reboot in progress

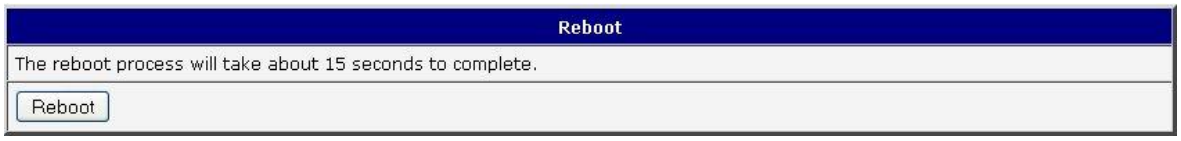
Continue here after reboot.

Tento výpis informuje o naprogramování paměti FLASH.

Nahrání firmware jiného přístroje by mohlo dojít k poškození routeru! Během aktualizace firmwaru musí být zajištěno trvalé napájení. Při výpadku napájení by mohlo dojít k poškození routeru.

1.41 Reboot

Znovu spuštění routeru lze vyvolat volbou položky *Reboot* v menu a následným stisknutím tlačítka *Reboot*.



Obrázek 74: Restart routeru

2. Nastavení konfigurace přes Telnet

Pro sledování stavu, konfiguraci a správu routeru je k dispozici Telnet rozhraní. Po zadání IP adresy routeru do Telnet rozhraní je možné provádět konfiguraci pomocí AT příkazů. Výchozí IP adresa routeru je 192.168.1.1. Konfiguraci může provádět pouze uživatel *root* s výchozím heslem *root*.

Pro Telnet existují následující příkazy:

Příkaz	Poips
cat	vypsání obsahu souboru
cp	kopírování souboru
date	zobrazení/změna systémového času
df	zobrazení informací o souborovém systému
dmesg	zobrazení diagnostických zpráv kernelu
echo	výpis řetězce
email	odeslání Emailu
free	zobrazení informací o paměti
gsmat	odeslání AT příkazů
gsminfo	zobrazení informací o kvalitě signálu
gsmsms	odeslání SMS
hwclock	zobrazení/změna času v RTC obvodu
ifconfig	zobrazení/změna konfigurace rozhraní
io	ovládání/čtení výstupů
ip	zobrazení/změna routovací tabulky
iptables	zobrazení/modifikace pravidel NetFilteru
kill	zabití procesu
killall	zabití procesu
ln	vytvoření odkazu
ls	výpis obsahu adresáře
mkdir	vytvoření adresáře
mv	přesun souboru
ntpdate	synchronizace systémového času s NTP serverem
passwd	změna hesla
ping	ICMP ping

Pokračování na následující straně

Pokračování z předchozí strany

Příkaz	Poips
ps	zobrazeni informací o procesech
pwd	výpis aktuálního adresáře
reboot	znovuspuštění routeru
rm	odstranění souboru
rmdir	odstranění adresáře
route	zobrazení/změna routovací tabulky
service	spuštění/zastavení služby
sleep	pauza na zadaný počet sekund
slog	zobrazení systémového logu
tail	zobrazení konce souboru
tcpdump	monitoring síťového provozu
touch	vytvoření souboru/aktualizace časového razítka souboru
vi	textový editor

Tabulka 69: Telnet příkazy