Průmyslový LTE Router

SmartStart

KONFIGURAČNÍ MANUÁL

B+B SMARTWORX

Powered by ADVANTECH

Použité symboly

Danger – Důležité upozornění, které může mít vliv na bezpečí osoby nebo funkčnost přístroje.

Attention – Upozornění na možné problémy, ke kterým může dojít ve specifických případech.

Information, notice – Informace, které obsahují užitečné rady, nebo zajímavé poznámky.

Example – Příklad funkce, příkazu nebo skriptu.

Verze firmware

Aktuální verze firmware popsaného v manuálu je 6.1.0 (15. prosince 2016).

Open Source softwarové licence

Software v tomto zařízení používá části open source software pod různými licencemi: GPL verze 2 a 3, LGPL verze 2, licence ve stylu BSD, licence ve stylu MIT. Seznam komponent spolu s plnými texty licencí je přístupný v samotném zařízení: Viz odkaz *Licenses* dole na hlavní stránce webového rozhraní routeru (*General Status*) nebo navštívením adresy IP_adresa_zařízení/licenses.cgi. V případě zájmu o zdrojové kódy nás kontaktujte na adrese:

cellularsales@advantech-bb.com

Modifikace a debugování spustitelných programů využívajících knihovny LGPL:

Výrobce zařízení tímto deklaruje právo použít pro vlastní potřebu debugovací techniky (např. dekompilaci) a provést uživatelské úpravy pouze těch spustitelných programů, které využívají knihovny pod licencí LGPL. Toto může být provedeno pouze pro osobní použití zákazníka. Není povolena žádná distribuce takto upravených programů, ani žádné předávání informací získaných během modifikace programů.

Advantech B+B SmartWorx s.r.o., Sokolská 71, 562 04 Ústi nad Orlicí, Česká Republika
Manuál Rev. 1 vydán v ČR, 11. ledna 2017

Obsah

Seznam obrázků

Seznam tabulek

1. Základní informace

Router SmartStart je LTE router určený pro bezdrátovou komunikaci v rámci mobilních sítí, jež využívají technologii LTE, HSPA+, UMTS, EDGE či GPRS. Díky mimořádným rychlostem přenosu dat až 100 Mbit/s (download) a 50 Mbit/s (upload) je možné tento router využít pro bezdrátové připojení kamer dopravních a bezpečnostních systémů, jednotlivých počítačů, sítí typu LAN, bankomatů a dalších samoobslužných terminálů.

1.1 Standardní vybavení

Router je standardně vybaven LTE bezdrátovým modulem (se dvěma anténními konektory – pro hlavní a diverzitní anténu), jedním portem Ethernet 10/100, jedním binárním vstupem a jedním binárním výstupem (I/O konektor dohromady s napájecím konektorem). Zařízení disponuje také dvěma čtečkami pro 3 V a 1,8 V SIM karty, které jsou umístěné na zadním panelu. Router je dodáván v plastové krabičce.

1.2 Volitelné vybavení

Zákazníkovi je umožněno zvolit si verzi s WiFi modulem, jehož anténní konektor je vyveden na přední panel routeru. Tato další komunikační rozhraní není možno do routeru doosadit později. Informace o verzích routerů – které kombinace volitelných rozhraní jsou možné – lze najít v technickém manuálu daného routeru.

1.3 Přednosti vůči v2 konceptu routerů

Nejvýraznějším krokem kupředu je pro novou generaci routerů čtyřikrát výkonnější procesor zajišťující značně vyšší propustnost a rychlejší šifrování. Router se rovněž může pochlubit výrazně větší pamětí (512 MB RAM a 256 MB flash).

1.4 Konfigurace

Pro konfiguraci routeru je k dispozici webové rozhraní zabezpečené jménem a heslem. Po přihlášení jsou dostupné podrobné statistiky o činnosti routeru, síle signálu, podrobný systémový log a další. Podporovány jsou oba protokoly IPv4 a IPv6, tvorba VPN tunelů technologiemi IPsec, OpenVPN či L2TP pro zabezpečenou komunikaci. Dále pak funkce jako DHCP, NAT, NAT-T, DynDNS client, NTP, VRRP, ovládání pomocí SMS, zálohování primárního připojení, možnost více WAN připojení (multiple WANs), RADIUS na WiFi a mnoho dalších.

Mezi další diagnostické funkce zabezpečující nepřerušovanou komunikaci patří automatická kontrola mobilního (PPP) spojení s možností automatického restartu v případě ztráty spojení, nebo HW watchdog, který monitoruje stav samotného routeru. Pomocí speciálního okna (start up script window) je možné vkládat linuxové scripty různých akcí. Pro některé

aplikace je klíčová možnost vytváření několika odlišných konfigurací pro jeden router, které je pak možné podle potřeby přepínat (například pomocí SMS, stavu binárního vstupu apod.). Samozřejmostí je pro routery Advantech B+B SmartWorx podpora automatické aktualizace konfigurace a firmware ze serveru, což umožňuje hromadně konfigurovat celou síť routerů.

1.5 Způsoby konfigurace

Router může být konfigurován pomocí webového rozhraní nebo pomocí Secure Shell (SSH). Konfigurace pomocí webového rozhraní je popsána v tomto konfiguračním manuálu. Příkazy a skripty použitelné pro SSH konfiguraci jsou popsány v Commands and Scripts for v2 and v3 Routers, Application Note (v angličtině) [1]. Je možno také využít další software pro routery – VPN server SmartCluster pro realizaci bezpečného komunikačního systému [2] nebo R-SeeNet pro monitoring stavu a funkce routerů [3,4].

1.6 Podpora IPv6

Ve firmware routeru je implementován nezávislý souběh protokolů IPv4 a IPv6 – tzv. dual stack. To znamená, že lze konfigurovat provoz v rámci obou IP protokolů nezávisle a oba jsou podporovány. IPv6 adresy ve formátu EUI-64 jsou pro každé rozhraní generovány automaticky – rozhraní tak může mít více IPv6 adres. V routeru také automaticky funguje síťové rozhraní NAT64 – brána pro překlad mezi protokoly IPv6 a IPv4 (více podrobností v kap. 3.5). NAT64 pracuje v routeru dohromady s DNS64 pro překlad doménových jmen.

Pro nastavení IPv6 mobilního připojení viz kapitolu 4.3.1. Pro nastavení IPv6 LAN sítě viz kapitolu 4.1, DHCPv6 server/klient je podporován. Ve všech nastaveních je IPv4 výchozí volbou, ale všechny funkce routeru a protokoly lze nastavit nebo použít v IPv6 režimu – kromě nešifrovaných tunelů GRE, L2TP a PPTP, a také VRRP – tam není IPv6 podporován. Při použití šifrovaných tunelů OpenVPN a IPsec je možné provozovat IPv6 provoz uvnitř IPv4 tunelu a naopak. Konfigurační formuláře *NAT*, *Firewall* a *Up/Down Script* jsou pro IPv4 a IPv6 úplně odděleny. Podporován je ICMPv6 protokol. Specifika IPv6 konfigurace jsou zmíněna v každé příslušné kapitole níže, tam kde je IPv6 nastavení možné.

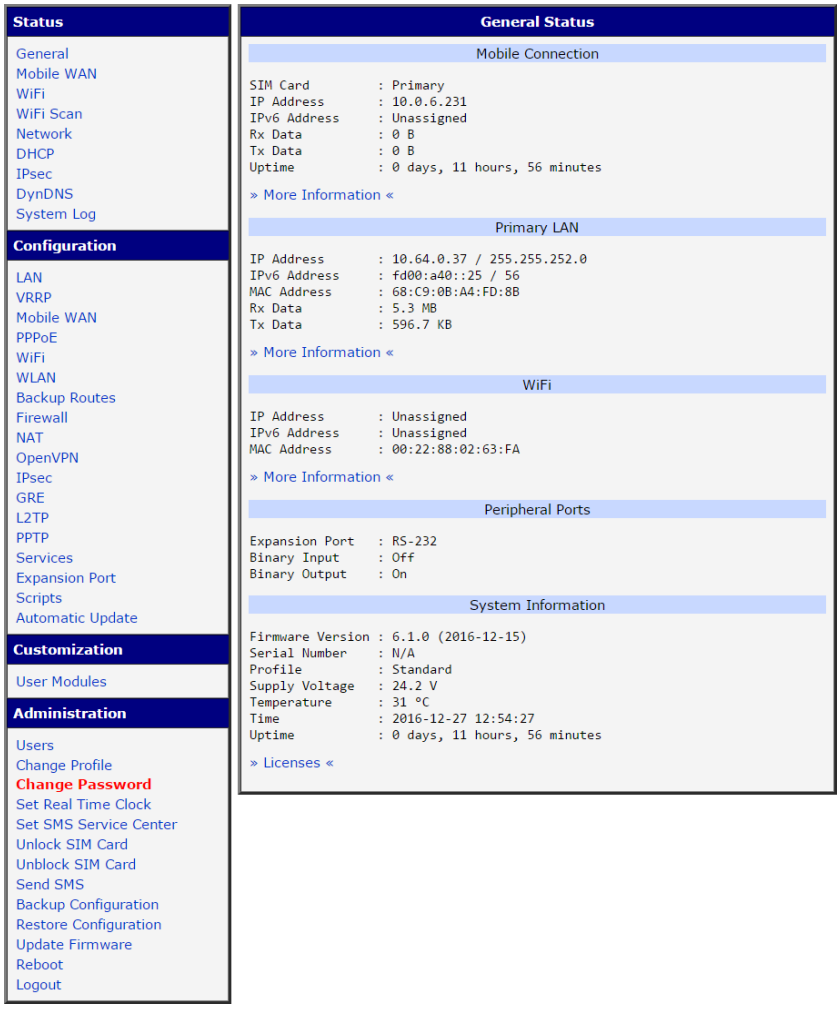
1.7 Tento konfigurační manuál popisuje

- Konfiguraci routeru – v kapitolách 3 až 6 možnosti konfigurace routeru položku po položce tak, jak jsou přístupny pomocí webového rozhraní.
- Konfiguraci v typických situacích – příklady konfigurace routeru (kapitola 7):
  - Přístup na internet z LAN (Local Area Network) přes mobilní síť, kap. 7.1.
  - zálohovaný přístup na Internet (z LAN), kap. 7.2.
  - zabezpečené propojení sítí nebo využití VPN (Virtal Private Network), kap. 7.3.
  - Serial Gateway (brána do internetu pro zařízení se sériovým rozhraním), kap. 7.4.

2. Přístup k webové konfiguraci

Pozor! Bez vložené SIM karty nebudou fungovat bezdrátové přenosy. Vložená SIM karta musí mít aktivované přenosy přes technologie používané vaším 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. a přístup k webovému rozhraní je možný pouze přes zabezpečený protokol HTTPS – přístupovou adresu k routeru je tedy nutno zadat ve tvaru https://192.168.1.1. Při prvním přístupu je potřeba nainstalovat bezpečnostní certifikát. Jestliže prohlížeč hlásí neshodu v doméně, je k odstranění tohoto hlášení možné použít postup popsaný v následující podkapitole.



Obrázek 1: Webové rozhraní

Konfiguraci může provádět pouze uživatel „***root***“ s výchozím heslem „***root***“. Výchozí heslo je třeba co nejdříve změnit.

> 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.

Po úspěšném zadání přihlašovacích údajů na úvodní obrazovce (tzv. login page) se zobrazí webové rozhraní. 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*).

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

2.1 Certifikáty a odstranění hlášení neshody v doméně

V routeru je nahraný self-signed certifikát (certifikát podepsaný sám sebou). Pokud chcete použít vlastní certifikát (např. v kombinaci se službou dynamického DNS záznamu), je nutné nahradit v routeru soubory certifikátu: /etc/certs/https_cert a /etc/certs/https_key.

> Generování HTTPS certifikátu bylo ve firmware 5.3.5 a vyšším aktualizováno pro větší bezpečnost. Tyto nově vygenerované certifikáty jsou ovšem pouze v routerech vyrobených s firmware 5.3.5 a novějším – certifikáty se automaticky negenerují s přechodem na nový firmware! Chcete-li používat aktualizovaný HTTPS certifikát po upgradu z firmware staršího než 5.3.5, smažte soubory začínající "https" v adresáři /etc/certs/ v routeru (/etc/certs/https*), napřípklad přes SSH. Certifákty pak budou automaticky vygenerovány znovu již novým aktualizovaným způsobem.

Pokud se rozhodnete využít self-signed certifikátu v routeru k odstranění bezpečnostního hlášení o neshodě v doméně, které se objeví pokaždé při přístupu k routeru, můžete použít následující postup. Poznámka: pro přístup k routeru bude nutné použít adresu založenou na MAC adrese routeru. Tento způsob také nemusí fungovat na některých kombinacích operačního systému a webového prohlížeče.

- Je třeba přidat DNS záznam do vašeho operačního systému. To lze provést upravením souboru /etc/hosts (Linux/Unix), nebo C:\WINDOWS\system32\drivers\etc\hosts (Windows), nebo nastavením vlastního DNS serveru. Nový záznam bude obsahovat IP adresu routeru a doménové jméno založené na MAC adrese routeru (MAC adresa prvního síťového rozhraní z těch, která jsou viditelná ve webovém rozhraní routeru v sekci *Network Status*.) Jako oddělovač použijte v doménovém jméně pomlčky místo dvojteček

v MAC adrese. Příklad: Routeru s MAC adresou 00:11:22:33:44:55 odpovídá doménové jméno 00-11-22-33-44-55.

- Připojte se k routeru přes webové rozhraní pomocí nového doménového jména (např. https://00-11-22-33-44-55). Pokud se objeví bezpečnostní hlášení o neshodě v doméně, přidejte výjimku, aby se při dalším připojení hlášení již neobjevilo (např. v prohlížeči Firefox). Pokud není v prohlížeči možnost přidat výjimku, nainstalujte do svého systému certifikát routeru. V prohlížeči exportujte certifikát do souboru a následně jej importujte do vašeho prohlížeče nebo operačního systému.

3. Status

3.1 Hlavní status (General)

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*. Pokud je router ve verzi s WiFi, je k dispozici i blok *WiFi*.

Pod položkou *IPv6 Address* může být zobrazeno více rozdílných addres pro jedno síťové rozhraní. To je standardní chování, protože v protokolu IPv6 může jedno rozhraní využívat více adres. Druhá IPv6 adresa se zobrazí po kliknutí na *More Information*. Je to IPv6 adresa ve formátu EUI-64 (link local), automaticky generovaná z MAC adresy síťové rozhraní. Adresa je generována a přiřazena až při prvním použití rozhraní (např. při připojení kabelu do portu, při připojování do mobilní sítě apod.).

3.1.1 Mobilní připojení (Mobile Connection)

Položka	Popis
SIM Card	Identifikace SIM karty (*Primary* nebo *Secondary*).
Interface	Definuje síťové rozhraní.
Flags	Příznaky daného síťového rozhraní.
IP Address	IPv4 adresa daného síťového rozhraní.
IPv6 Address	IPv6 adresa nebo adresy daného síťového rozhraní. Více IPv6 adres může být přiřazeno jednomu síťovému rozhraní.
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.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Tx Overruns	Ztracené odchozí pakety z důvodu přetížení.
Uptime	Doba, po kterou je sestavené spojení na mobilní síti.

Tabulka 1: Mobile Connection

3.1.2 Rozhraní LAN a WiFi

Položky zobrazené v této části mají stejný význam jako položky v části předchozí. Navíc je zde informace o MAC adrese (položka *MAC Address*) příslušného rozhraní routeru (*Primary LAN – eth0*, *WiFi – wlan0*). Zobrazené informace závisí na konfiguraci (viz 4.1 nebo 4.5).

3.1.3 Volitelné porty (Peripheral Ports)

Položka	Popis
Expansion Port	Sériové rozhraní routeru (konektor DB9 na předním panelu routeru)
Binary Input	Stav binárního vstupu
Binary Output	Stav binárního výstupu

Tabulka 2: Peripheral Ports

3.1.4 Informace o systému (System Information)

Položka	Popis
Firmware Version	Informace o verzi firmware
Serial Number	Sériové číslo daného routeru (v případě *N/A* není dostupné)
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
Licenses	Odkaz na seznam open source softwarových komponent, které firmware routeru obsahuje, společně s plnými texty jejich licencí (GPL verze 2 a 3, LGPL verze 2, licence ve stylu BSD a MIT).

Tabulka 3: System Information

3.2 Stav připojení k mobilní síti

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	Popis
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 (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 není tato hodnota dostupná
CSQ	Cell Signal Quality – Relativní kvalita signálu v buňce. Bezrozměrná hodnota dána převodním vztahem z hodnoty RSSI (v dBm). Rozsah 2–9: malá kvalita signálu, v rozsahu 10–14 je kvalita OK, 15–16 je dobrá kvalitu signálu, 20–30 excelentní kvalita signálu.
Neighbours	Síla signálu sousedních slyšitelných buněk
Manufacturer	Výrobce modulu
Model	Typ modulu
Revision	Verze osazeného modulu
IMEI	IMEI (International Mobile Equipment Identity) modulu
MEID	MEID modulu
ICCID	Mezinárodní unikátní sériové číslo SIM karty.

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 zvýšený o jedna (počet použitých buněk)
Availability	Dostupnost routeru přes mobilní síť

Tabulka 6: Mobile Network Statistics

Tipy pro tabulku *Mobile Network Statistics*:

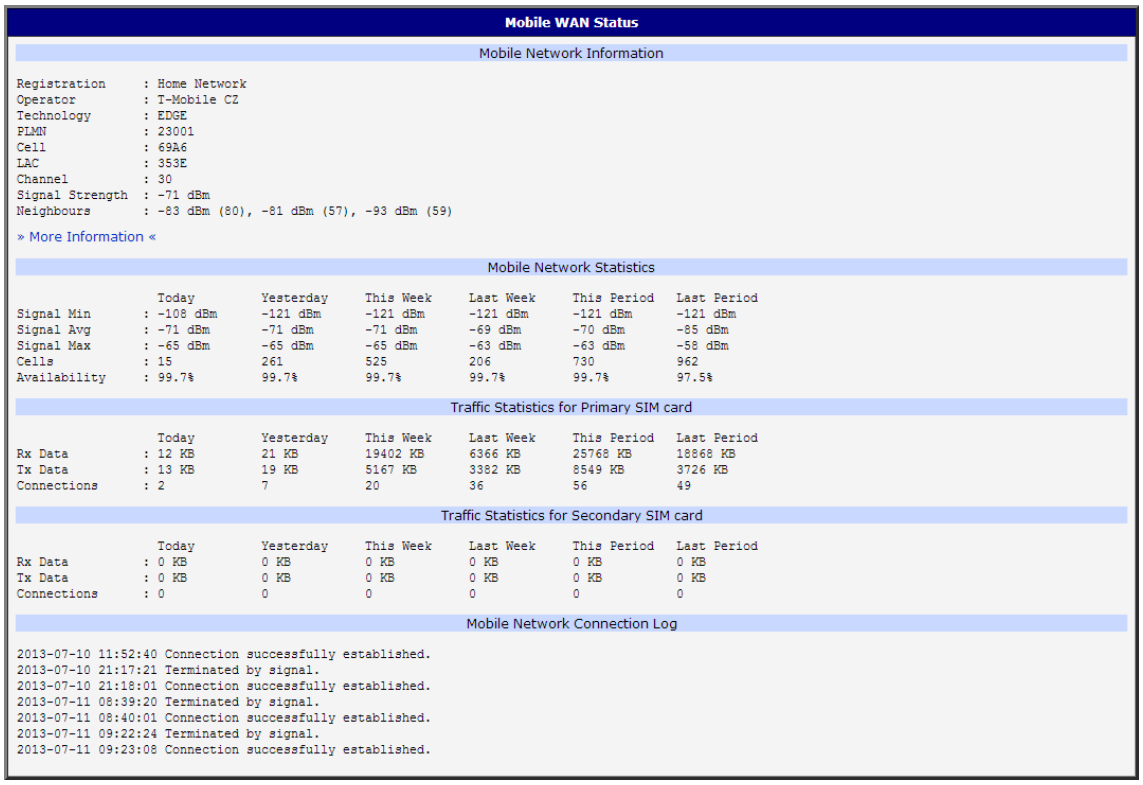
- Dostupnost spojení do mobilní sítě je údaj v procentech, který je počítán poměrem času navázaného spojení do mobilní sítě vůči času, kdy je router zapnutý.
- Po najetí kurzorem na hodnoty maximální nebo minimální síly signálu se zobrazí poslední čas, kdy této síly signálu router dosáhl.

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*).



Mobile WAN Status

Mobile Network Information

```
Registration     : Home Network
Operator         : T-Mobile CZ
Technology       : EDGE
PLMN             : 23001
Cell             : 69A6
LAC              : 353E
Channel          : 30
Signal Strength  : -71 dBm
Neighbours       : -83 dBm (80), -81 dBm (57), -93 dBm (59)
```

» More Information «

Mobile Network Statistics

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Signal Min	-108 dBm	-121 dBm	-121 dBm	-121 dBm	-121 dBm	-121 dBm
Signal Avg	-71 dBm	-71 dBm	-71 dBm	-69 dBm	-70 dBm	-85 dBm
Signal Max	-65 dBm	-65 dBm	-65 dBm	-63 dBm	-63 dBm	-58 dBm
Cells	15	261	525	206	730	962
Availability	99.7%	99.7%	99.7%	99.7%	99.7%	97.5%

Traffic Statistics for Primary SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	12 KB	21 KB	19402 KB	6366 KB	25768 KB	18868 KB
Tx Data	13 KB	19 KB	5167 KB	3382 KB	8549 KB	3726 KB
Connections	2	7	20	36	56	49

Traffic Statistics for Secondary SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	0	0	0	0	0	0

Mobile Network Connection Log

```
2013-07-10 11:52:40 Connection successfully established.
2013-07-10 21:17:21 Terminated by signal.
2013-07-10 21:18:01 Connection successfully established.
2013-07-11 08:39:20 Terminated by signal.
2013-07-11 08:40:01 Connection successfully established.
2013-07-11 09:22:24 Terminated by signal.
2013-07-11 09:23:08 Connection successfully established.
```

Obrázek 2: Mobile WAN status

3.3 WiFi

Tato položka je dostupná pouze tehdy, je-li v routeru osazen WiFi modul.

Volbou položky *WiFi* v menu webového rozhraní routeru se zobrazí okno s informacemi o přístupovém bodu (AP) routeru a o připojených klientech.

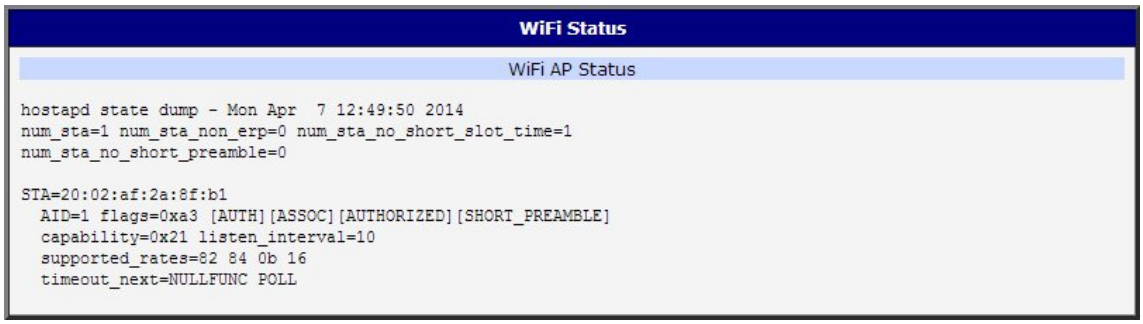
Položka	Popis
hostapd state dump	Čas, ke kterému se statistická data vztahují
num_sta	Počet připojených stanic
num_sta_non_erp	Počet stanic využívající připojení 802.11b v 802.11g BSS
num_sta_no_short_slot_time	Počet stanic nepodporující Short Slot Time
num_sta_no_short_preamble	Počet stanic nepodporující Short Preamble

Tabulka 8: Stavové informace o přístupovém bodu

Pro každého připojeného klienta jsou pak zobrazeny další podrobné informace. Většina z nich je však vnitřního charakteru, a tak jako užitečné zmiňme pouze následující:

Položka	Popis
STA	MAC adresa připojeného zařízení
AID	Identifikátor připojené stanice (1 – 2007). Je-li zobrazena 0, daná stanice není právě připojena.

Tabulka 9: Stavové informace o připojených klientech



Obrázek 3: WiFi Status

3.4 WiFi Scan

Tato položka je dostupná pouze tehdy, je-li v routeru osazen WiFi modul.

Volbou položky *WiFi Scan* v menu webového rozhraní routeru se vyvolá skenování okolních WiFi sítí a následné vypsání výsledků. **Skenování lze provést pouze tehdy, je-li vypnut přístupový bod (WiFi AP).**

Položka	Popis
BSS	MAC adresa přístupového bodu (AP)
TSF	Synchronizovaný čas udržovaný v celé síti spravované přístupovým bodem (AP)
freq	Frekvenční pásmo WiFi sítě [kHz]
beacon interval	Perioda časové synchronizace
capability	Seznam vlastností přístupového bodu (AP)
signal	Úroveň signálu přístupového bodu (AP)
last seen	Poslední odezva přístupového bodu (AP)
SSID	Identifikátor přístupového bodu (AP)
Supported rates	Podporované rychlosti přístupového bodu (AP)
DS Parameter set	Kanál, na kterém je vysílán broadcast přístupového bodu (AP)
ERP	Extended Rate PHY – informační element poskytující zpětnou kompatibilitu
Extended supported rates	Podporované rychlosti přístupového bodu (AP), které jsou nad rámec osmi rychlostí uváděných jako *Supported rates*
RSN	Robust Secure Network – Protokol pro sestavení bezpečné komunikace přes bezdrátovou síť 802.11

Tabulka 10: Informace o okolních sítích

Stránka *WiFi Scan* může vypadat například takto:

WiFi Scan

List of BSSs

```
BSS 00:22:88:02:0b:bd (on wlan0)
        TSF: 446998707938 usec (5d, 04:09:58)
        freq: 2447
        beacon interval: 100
        capability: ESS Privacy ShortSlotTime (0x0411)
        signal: -87.00 dBm
        last seen: 930 ms ago
        Information elements from Probe Response frame:
        SSID: conelguest
        Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
        DS Parameter set: channel 8
        ERP: Barker_Preamble_Mode
        Extended supported rates: 24.0 36.0 48.0 54.0
        RSN:     * Version: 1
                 * Group cipher: CCMP
                 * Pairwise ciphers: CCMP
                 * Authentication suites: PSK
                 * Capabilities: 16-PTKSA-RC (0x000c)
        HT capabilities:
                Capabilities: 0x0c
                        HT20
                        SM Power Save disabled
                        No RX STBC
                        Max AMSDU length: 3839 bytes
                        No DSSS/CCK HT40
                Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
                Minimum RX AMPDU time spacing: 2 usec (0x04)
                HT RX MCS rate indexes supported: 0-7, 32
                TX unequal modulation not supported
                HT TX Max spatial streams: 1
                HT TX MCS rate indexes supported may differ
        HT operation:
                 * primary channel: 8
                 * secondary channel offset: no secondary
                 * STA channel width: 20 MHz
                 * RIFS: 0
                 * HT protection: non-HT mixed
                 * non-GF present: 1
                 * OBSS non-GF present: 0
                 * dual beacon: 0
                 * dual CTS protection: 0
                 * STBC beacon: 0
                 * L-SIG TXOP Prot: 0
                 * PCO active: 0
                 * PCO phase: 0
        WMM:     * Parameter version 1
                 * BE: CW 15-1023, AIFSN 3
                 * BK: CW 15-1023, AIFSN 7
                 * VI: CW 7-15, AIFSN 2, TXOP 3008 usec
                 * VO: CW 3-7, AIFSN 2, TXOP 1504 usec
```

Obrázek 4: WiFi Scan

3.5 Síťové informace (Network Status)

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 síťových rozhraních:

Rozhraní	Popis
eth0, eth1, eth2	Síťová rozhraní (připojení do ethernetu)
usb0	Aktivní PPP připojení do mobilní sítě – bezdrátový modul je připojen přes USB rozhraní.
wlan0	WiFi rozhraní
ppp0	PPP rozhraní (např. tunel PPPoE)
tun0	Rozhraní OpenVPN tunelu
ipsec0	Rozhraní IPsec tunelu
gre1	Rozhraní GRE tunelu
lo	Lokální smyčka (loopback)
nat64	Síťové rozhraní – gateway – pro překlad mezi IPv6 a IPv4 adresami.

Tabulka 11: Popis rozhranní network status

U každého rozhraní jsou pak zobrazeny následující informace:

Položka	Popis
HWaddr	Hardwarová (MAC) adresa síťového rozhraní.
inet addr	IPv4 adresa síťového rozhranní.
inet6 addr	IPv6 adresa síťového rozhranní. Může jich být více u jednoho síťového rozhraní.
P-t-P	IP adresa druhého konce spojení v případě dvoubodových 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.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
TX	• **packets** – odchozí pakety • **errors** – chybné odchozí pakety • **dropped** – zahozené odchozí pakety • **overruns** – ztracené odchozí pakety z důvodu přetížení. • **carrier** – chybné odch. 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 12: 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 usb0.

Ve spodní části stránky *Network Status* je také zobrazena routovací tabulka. Tabulka *Route Table* je IPv4 routovací tabulka, pod ní je zobrazena IPv6 routovací tabulka *IPv6 Route Table*.

Pokud je router připojen do internetu (výchozí cesta je nastavena), vytvoří se automaticky síťové rozhraní *nat64*. Jedná se o vnitřní síťovou bránu NAT64 pro překlad mezi IPv6 a IPv4 komunikací. Použije se automaticky v případě, že router je připojen přes IPv6 a potřebuje komunikovat s IPv4 sítí nebo zařízením. Toto síťové rozhraní spolupracuje s DNS64 (překlad doménových jmen na IP adresy), které je v routeru také automaticky aktivováno. Pro překlad NAT64 je použit standardní prefix 64:ff9b::/96, jak je vidět z obrázku 5 níže v IPv6 routovací tabulce úplně dole (*IPv6 Route Table*).

Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 00:0A:14:83:C6:68
          inet addr:192.168.1.6  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:680 errors:0 dropped:0 overruns:0 frame:0
          TX packets:452 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:91766 (89.6 KB)  TX bytes:264262 (258.0 KB)
          Interrupt:56

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

nat64     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

usb0      Link encap:Ethernet  HWaddr 00:A0:C6:00:00:00
          inet addr:10.143.10.85  Bcast:0.0.0.0  Mask:255.255.255.255
          inet6 addr: fe80::2a0:c6ff:fe00:0/64 Scope:Link
          inet6 addr: 2a01:598:89c1:8b2b::1/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10404 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:750432 (732.8 KB)  TX bytes:0 (0.0 B)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.254.254 0.0.0.0         UG    0      0        0 usb0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.254.254 0.0.0.0         255.255.255.255 UH    0      0        0 usb0
```

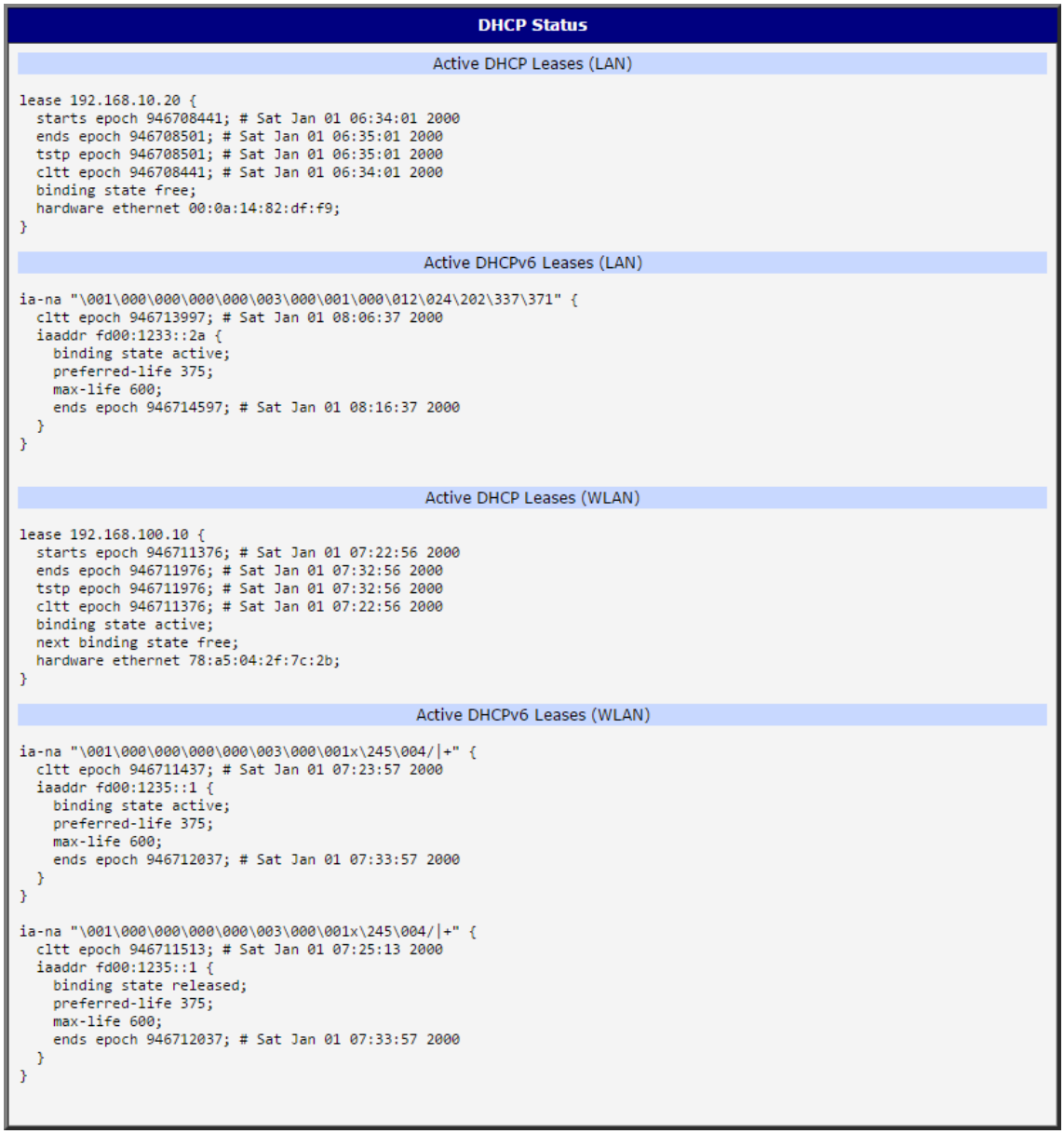
IPv6 Route Table

```
Destination                     Next Hop                    Flags Metric Ref    Use Iface
::1/128                         ::                          U     0      1        1 lo
64:ff9b::/96                    ::                          U     1024   0        0 nat64
2a01:598:89c1:8b2b::/128        ::                          U     0      0        1 lo
2a01:598:89c1:8b2b::1/128       ::                          U     0      0        1 lo
2a01:598:89c1:8b2b::/64         ::                          U     256    0        0 usb0
fe80::/128                      ::                          U     0      0        1 lo
fe80::2a0:c6ff:fe00:0/128       ::                          U     0      3408       1 lo
fe80::8819:7050:7ec5:2689/128   ::                          U     1024   0        0 usb0
fe80::/64                       ::                          U     256    0        0 usb0
ff00::/8                        ::                          U     256    0        0 usb0
::/0                            fe80::8819:7050:7ec5:2689   UG    1024   0        0 usb0
```

Obrázek 5: Network Status

3.6 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 jejich IP adresu, masku sítě, IP adresu výchozí brány a IP adresu DNS serveru.



DHCP Status

Active DHCP Leases (LAN)

```
lease 192.168.10.20 {
  starts epoch 946708441; # Sat Jan 01 06:34:01 2000
  ends epoch 946708501; # Sat Jan 01 06:35:01 2000
  tstp epoch 946708501; # Sat Jan 01 06:35:01 2000
  cltt epoch 946708441; # Sat Jan 01 06:34:01 2000
  binding state free;
  hardware ethernet 00:0a:14:82:df:f9;
}
```

Active DHCPv6 Leases (LAN)

```
ia-na "\001\000\000\000\000\003\000\001\000\012\024\202\337\371" {
  cltt epoch 946713997; # Sat Jan 01 08:06:37 2000
  iaaddr fd00:1233::2a {
    binding state active;
    preferred-life 375;
    max-life 600;
    ends epoch 946714597; # Sat Jan 01 08:16:37 2000
  }
}
```

Active DHCP Leases (WLAN)

```
lease 192.168.100.10 {
  starts epoch 946711376; # Sat Jan 01 07:22:56 2000
  ends epoch 946711976; # Sat Jan 01 07:32:56 2000
  tstp epoch 946711976; # Sat Jan 01 07:32:56 2000
  cltt epoch 946711376; # Sat Jan 01 07:22:56 2000
  binding state active;
  next binding state free;
  hardware ethernet 78:a5:04:2f:7c:2b;
}
```

Active DHCPv6 Leases (WLAN)

```
ia-na "\001\000\000\000\000\003\000\001x\245\004/|+" {
  cltt epoch 946711437; # Sat Jan 01 07:23:57 2000
  iaaddr fd00:1235::1 {
    binding state active;
    preferred-life 375;
    max-life 600;
    ends epoch 946712037; # Sat Jan 01 07:33:57 2000
  }
}

ia-na "\001\000\000\000\000\003\000\001x\245\004/|+" {
  cltt epoch 946711513; # Sat Jan 01 07:25:13 2000
  iaaddr fd00:1235::1 {
    binding state released;
    preferred-life 375;
    max-life 600;
    ends epoch 946712037; # Sat Jan 01 07:33:57 2000
  }
}
```

Obrázek 6: DHCP Status

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

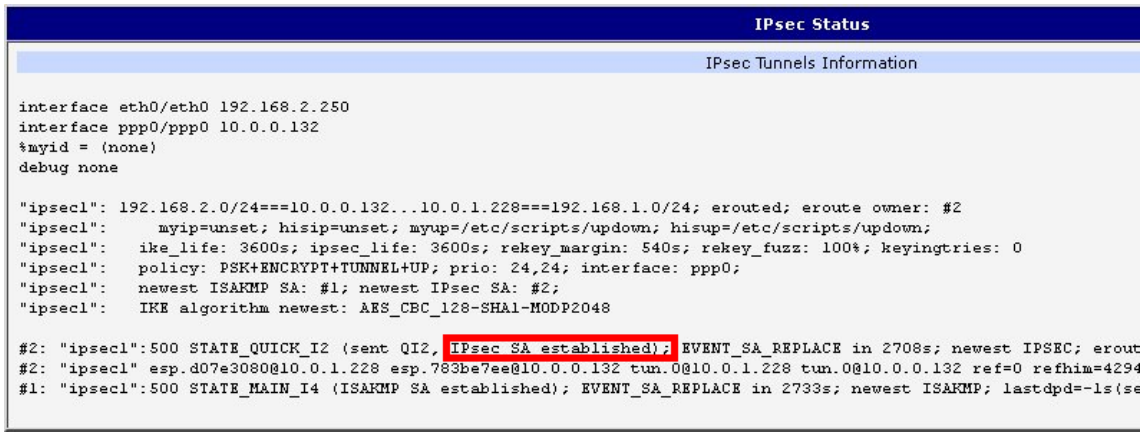
Záznamy v okně *DHCP status* jsou rozděleny do samostatných částí dle rozhraní LAN nebo WLAN a dle IPv4 (DHCP) a IPv6 (DHCPv6) protokolu – jsou zde části *Active DHCP Leases (LAN)*, *Active DHCPv6 Leases (LAN)*, *Active DHCP Leases (WLAN)* a *Active DHCPv6 Leases (WLAN)*, je-li router ve verzi s WiFi a má aktivováno rozhraní WLAN. Na obrázku 6 je vidět aktivní DHCP (IPv4) i DHCPv6 (IPv6) server na na rozhraní LAN i WLAN. Tabulka níže vysvětluje informace zobrazené v seznamu klientů:

Položka	Popis
lease	Přidělená IPv4 adresa.
iaaddr	(IPv6) Přidělená IPv6 adresa.
starts epoch	Čas přidělení IP adresy.
ends epoch	Čas ukončení platnosti přidělené IP adresy.
tstp epoch	Čas ukončení platnosti přidělené IP adresy, který byl zaslán klientovi.
cltt epoch	Čas poslední transakce klienta.
binding state	Stav platnosti přidělené adresy klientovi.
next binding state	Do kterého stavu přidělená adresa přejde po vypršení platnosti stávajícího stavu.
hardware ethernet	Hardwarová (MAC) adresa.
uid	Unikátní ID.
client-hostname	Název počítače.
preferred-life	(IPv6) Čas, po který může být přidělená adresa klientem jakkoli používána. Po vypršení této doby již nemůže být adresa používána pro nová spojení, pouze pro některá již probíhající.
max-life	(IPv6) Maximální čas, po který je přidělená adresa DHCPv6 serverem garantována.

Tabulka 13: Popis informací DHCP status pro IPv4 i IPv6 klienty

3.7 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). Pokud zda tato informace není, tunel nebyl sestaven! Ostatní informace mají pouze interní charakter.



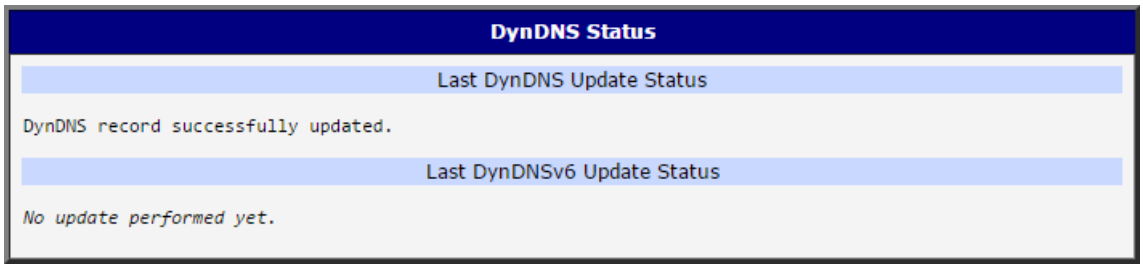
Obrázek 7: IPsec Status

3.8 DynDNS Status

Výsledek aktualizace DynDNS záznamu na serveru www.dyndns.org lze vyvolat volbou položky *DynDNS* v menu. Pro více informací, jak nakonfiguraovat Dynamic DNS klienta, navštivte web www.dyndns.org.

Pro službu Dynamického DNS záznamu je možné využít následující servery. Pro službu DynDNSv6 je nutné nastavit *IP Mode* na IPv6 na stránce *DynDNS Configuraction*.

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com



Obrázek 8: DynDNS Status

Při zjišťování stavu aktualizace jsou možná 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.

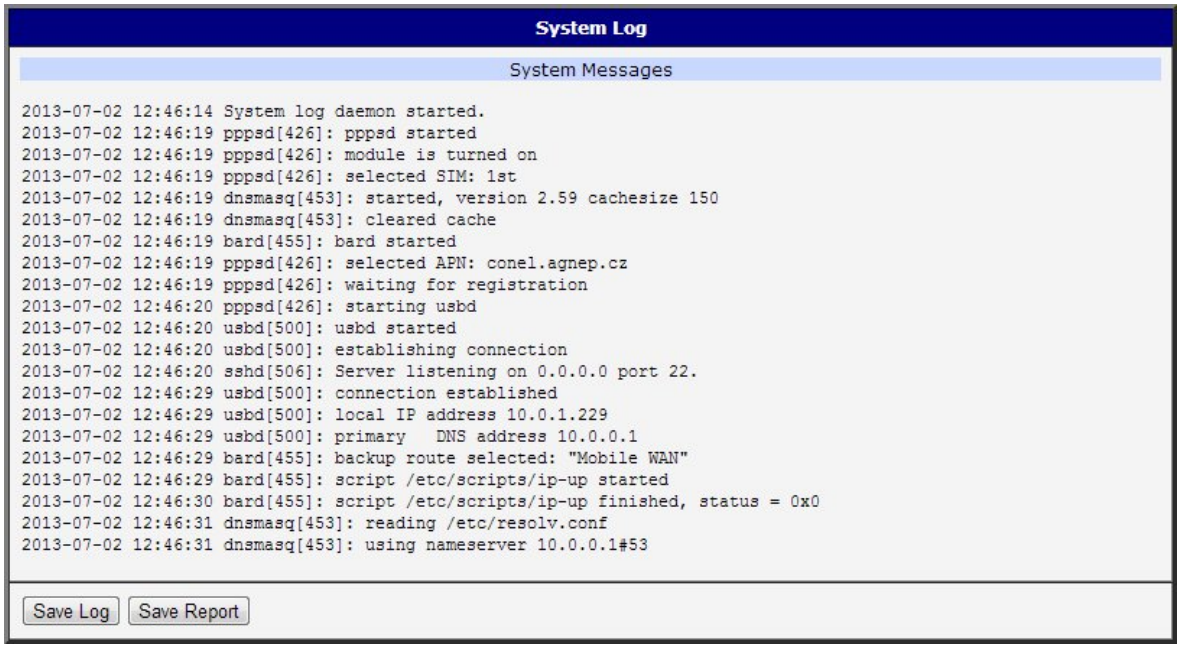
Pro správnou funkci DynDNS musí mít SIM karta routeru přiřazenou veřejnou IP adresu.

3.9 Systémový log

V případě problémů s 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 (uloží se soubor s textovými informacemi s příponou .log). Druhé tlačítko – *Save Report* – slouží k vytvoření reportu (jeden textový soubor obsahující všechny informace potřebné pro technickou podporu, s příponou .txt – statistické údaje, tabulky směrování a běžících procesů, system log, konfigurace).

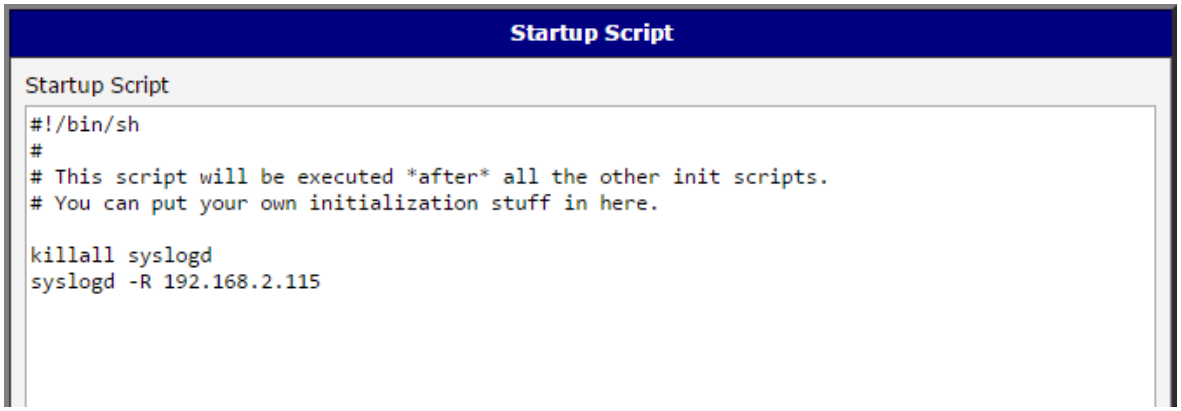
Defaultní velikost systémového logu je 1000 řádků. Po dovršení 1000 řádků se vytvoří nový soubor pro ukládání systémového logu. Po dovršení 1000 řádků v druhém souboru se maže první soubor a vytvoří se místo něho nový.

Výpis logu zajišťuje program *Syslogd*. Ten může být spuštěn se 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. (Pokud vzdálený syslog démon běží na systému Linux, musí v něm být povoleno vzdálené logování. Typicky spuštěním programu syslogd s volbou -R. Je-li vzdáleným démonem PC se systémem Windows, musí zde být nainstalován syslog server, např. Syslog Watcher.) Aby se program Syslogd spouštěl s těmito volbami, je nutné upravit skript */etc/init.d/syslog* přes SSH, nebo startup skript (viz *Startup Script* v sekci *Configuration*) podle obr. 10.



Obrázek 9: Systémový log

Níže je uveden příklad, jak poslat logování na vzdálený server s adresou 192.168.2.115.



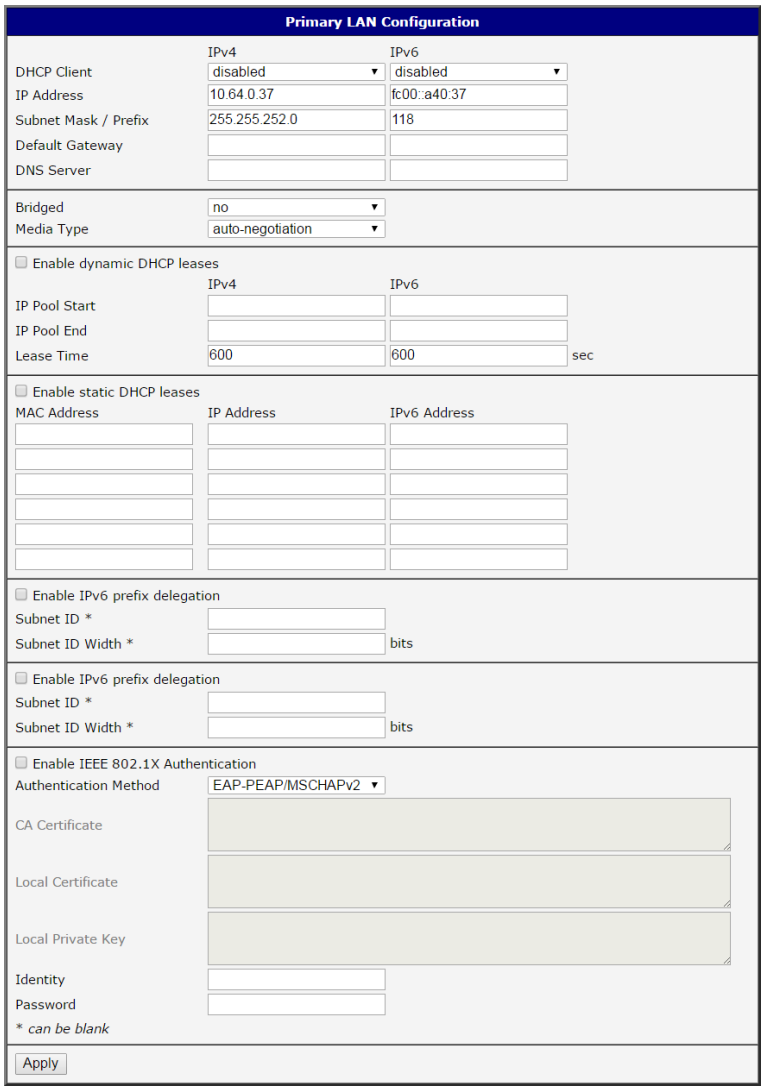
Obrázek 10: Příklad spuštění programu syslogd s volbou -R

4. Konfigurace

4.1 LAN konfigurace

Konfiguraci síťového rozhraní lze vyvolat volbou položky *LAN* v sekci *Configuration*.

Konfigurační stránka Ethernet rozhraní je rozdělena do sloupců IPv4 a IPv6, viz obr. 11. Router podporuje souběh protokolů IPv4 a IPv6, tkzv. *dual stack*. Je tedy možné nastavit jeden z protokolů nebo oba – potom router umožňuje okolním zařízením komunikaci pomocí obou protokolů a záleží tedy na ostatních zařízeních v síti, který protokol se použije. Položky konfigurace a rozdíly v nastavení IPv6 a IPv4 jsou popsány v tabulkách níže.



Obrázek 11: Stránka LAN Configuration

Item	Description
DHCP Client	Povoluje/zakazuje funkci DHCP klienta. Pokud je povolen v IPv6 sloupci, jedná se o DHCPv6 klienta. DHCPv6 klient podporuje všechny tři způsoby získání IPv6 adresy – SLAAC, stateless (bezestavový) DHCPv6 a stateful (stavový) DHCPv6. • **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. Ve sloupci IPv4 je nutné použít zápis adresy ve formátu IPv4, ve sloupci IPv6 ve formátu IPv6. Zkrácené zápisy IPv6 adres jsou povoleny.
Subnet Mask / Prefix	Specifikuje masku sítě v případě IPv4. Ve sloupci IPv6 je nutno vyplnit prefix – jedno číslo v rozsahu 0 až 128.
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. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
DNS server	Specifikuje IP adresu DNS serveru routeru. Adresa, na kterou jsou přeposlány všechny DNS dotazy na router. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.

Tabulka 14: Konfigurace síťového rozhraní – IPv4 a IPv6

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 kapitole 4.7). Od FW 5.3.0 jsou *Default Gateway* a *DNS Server* podporovány také na přemostěných rozhraních.

Následující položky (v tabulce níže) jsou obecná nastavení pro dané Ethernet rozhraní. 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 / Prefix*). Jestliže jsou do bridge přidávána další rozhraní (wan0), 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.

Item	Description
Bridged	Povoluje/zakazuje funkci bridge. • **no** – Router nemá aktivován režim bridge (výchozí hodnota) • **yes** – Router má aktivován režim bridge
Media type	Specifikuje typ duplexu a rychlost komunikace. • **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.

Tabulka 15: Konfigurace síťového rozhraní – obecné položky

4.1.1 DHCP server pro přidělování adres

DHCP server přiděluje připojeným klientům IP adresy, IP adresu brány (IP adresa routeru) a IP adresu DNS serveru (IP adresa routeru). Jsou-li tyto hodnoty v konfiguračním formuláři vyplněné uživatelem, preferují se.

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.

Pokud je vyplněn IPv6 sloupec, je použit DHCPv6 server. DHCPv6 server nabízí připojeným klientům stateful (stavovou) konfiguraci adresy. Pouze je-li *Subnet Prefix* nahoře nastaven na hodnotu 64, nabízí dva způsoby – stateful (stavovou) konfiguraci a SLAAC (bezestavovou automatickou konfiguraci) adresy.

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.

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. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
IP Pool End	Konec prostoru IP, které budou přidělovány DHCP klientům. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
Lease time	Čas v sekundách, po který smí klient IP adresu používat.

Tabulka 16: Konfigurace dynamického DHCP serveru

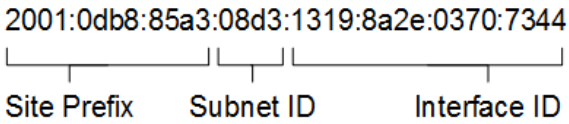
Položka	Popis
Enable static DHCP leases	Zaškrtnutím této položky lze povolit statický DHCP server.
MAC Address	MAC adresa DHCP klienta.
IPv4 Address	Přidělená IPv4 adresa v odpovídajícím formátu.
IPv6 Address	Přidělená IPv6 adresa v odpovídajícím formátu.

Tabulka 17: Konfigurace statického DHCP serveru

4.1.2 Delegace prefixu v IPv6

Toto je pokročilá možnost nastavení. Delegace prefixu v IPv6 funguje v routeru automaticky pomocí DHCPv6 – toto nastavení provádějte pouze pokud chcete použít jinou konfiguraci delegace prefixu než automatickou a pokud znáte důsledky takového nastavení.

Tímto nastavením je možno nahradit automatickou delegaci prefixu. Ke správnému nastavení je nutné znát vaši šířku Subnet ID (*Subnet ID Width*), což je část IPv6 adresy – viz obrázek níže pro pomoc při výpočtu: Zde příklad adresy se 48 bity Site Prefixu, 16 bity Subnet ID (*Subnet ID Width*) a 64 bity Interface ID.



Obrázek 12: IPv6 adresa s příkladem prefixu

Item	Description
Enable IPv6 prefix delegation	Aktivuje delegaci prefixu dle nastavení níže.
Subnet ID	Desítkový zápis hodnoty Subnet ID (části IPv6 adresy) daného Ethernetového rozhraní. Maximální možná hodnota závisí na délce této části adresy (*Subnet ID Width*).
Subnet ID Width	Délka části Subnet ID IPv6 adresy. Maximální hodnota závisí na délce přiděleného Site Prefix – jde o zbytek do 64 bitů.

Tabulka 18: Konfigurace delegace IPv6 prefixu

Následující část konfigurace umožňuje použít autentifikaci (802.1x) k Radius serveru. Tato funkcionalita vyžaduje nastavení identity a certifikátů, viz následující tabulka.

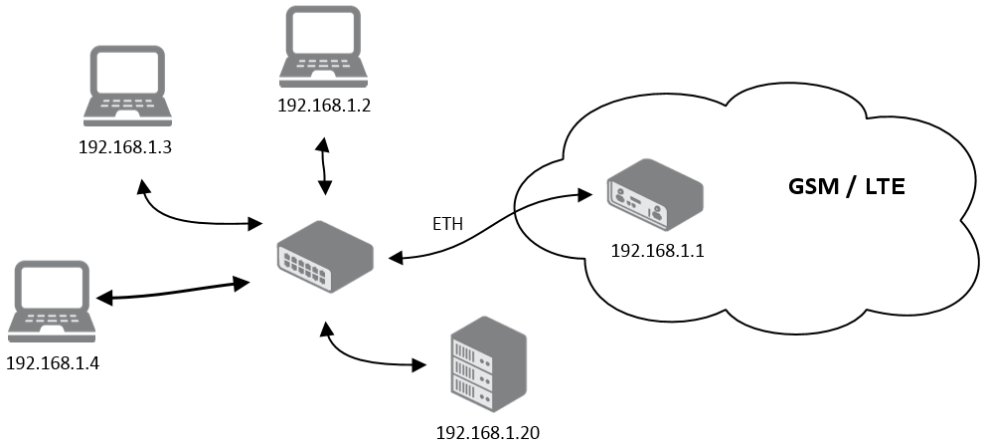
Položka	Popis
Enable IEEE 802.1X Authentication	Zaškrtnutím této položky lze povolit 802.1X autentizaci.
Authentication Method	Volba autentizační metody (EAP-PEAPMSCHAPv2 or EAP-TLS).
CA Certificate	Definice CA certifikátu pro autentizační protokol EAP-TLS.
Local Certificate	Definice lokálního certifikátu pro autentizační protokol EAP-TLS.
Local Private Key	Definice lokálního privátního klíče pro autentizační protokol EAP-TLS.
Identity	Uživatelské jméno.
Password	Přístupové heslo. Tato položka je k dispozici pouze pro protokol EAP-PEAPMSCHAPv2.
Local Private Key Password	Definice hesla pro privátní klíč EAP-TLS protokolu. Tato položka je k dispozici pouze pro protokol EAP-TLS.

Tabulka 19: Konfigurace 802.1X autentikace

4.1.3 Příklady konfigurace LAN

Příklad 1: IPv4 dynamický DHCP server, výchozí brána a DNS

- Rozsah přidělovaných adres je 192.168.1.2 až 192.168.1.4.
- Platnost přidělené adresy je 600 sekund (10 minut).
- Výchozí brána má IP adresu 192.168.1.20
- DNS server má IP adresu 192.168.1.20



Obrázek 13: Topologie sítě pro příklad 1

Primary LAN Configuration

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway	192.168.1.20	
DNS Server	192.168.1.20	

Bridged	no
Media Type	auto-negotiation

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec

☐ Enable static DHCP leases

MAC Address	IPv4 Address	IPv6 Address

☐ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

☐ Enable IEEE 802.1X Authentication

Authentication Method	EAP-PEAP/MSCHAPv2
CA Certificate	
Local Certificate	
Local Private Key	
Identity	
Password	

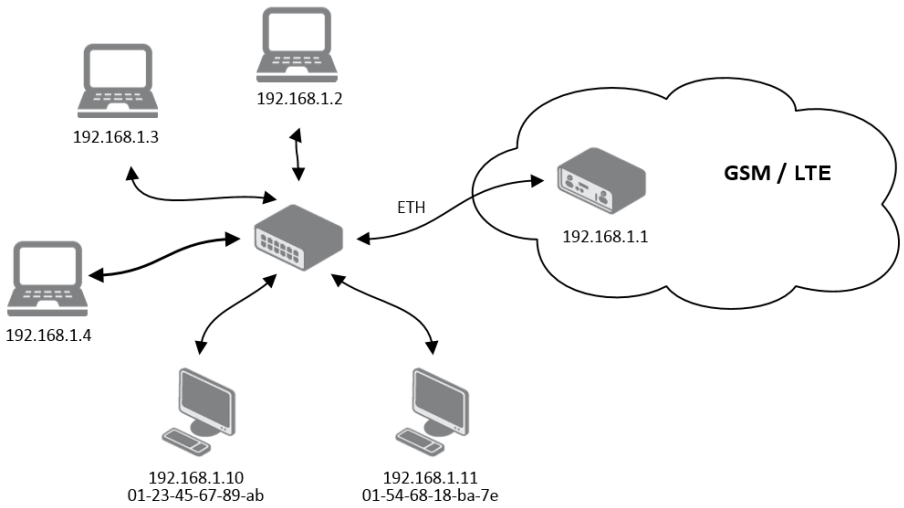
* *can be blank*

Apply

Obrázek 14: Konfigurace LAN pro příklad 1

Příklad 2: IPv4 dynamický a statický DHCP server

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



Obrázek 15: Topologie sítě pro příklad 2

Primary LAN Configuration

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	
Subnet Mask / Prefix	255.255.255.0	
Default Gateway		
DNS Server		

Bridged	no
Media Type	auto-negotiation

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start	192.168.1.2		
IP Pool End	192.168.1.4		
Lease Time	600	600	sec

☑ Enable static DHCP leases

MAC Address	IPv4 Address	IPv6 Address
01:23:45:67:89:ab	192.168.1.10	
01:54:68:18:ba:7e	192.168.1.11	

☐ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

☐ Enable IEEE 802.1X Authentication

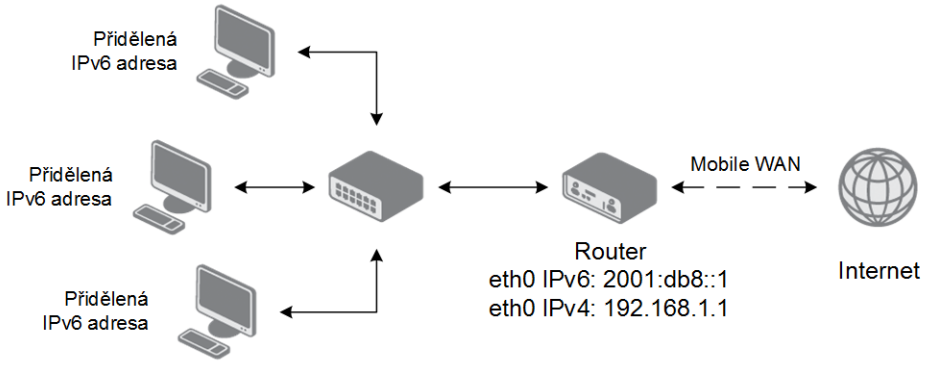
Authentication Method	EAP-TLS
CA Certificate	
Local Certificate	
Local Private Key	
Identity	
Local Private Key Password	

Apply

Obrázek 16: Konfigurace LAN pro příklad 2

Příklad 3: IPv6 dynamický DHCP server

- Rozsah přidělovaných IPv6 adres je 2001:db8::1 až 2001:db8::ffff.
- Platnost dynamicky přidělené adresy je 600 sekund (10 minut).
- Router je stále přístupný i přes IPv4 (192.168.1.1).



Obrázek 17: Topologie sítě pro příklad 3

Primary LAN Configuration

	IPv4	IPv6
DHCP Client	disabled	disabled
IP Address	192.168.1.1	2001:db8::1
Subnet Mask / Prefix	255.255.255.0	64
Default Gateway		
DNS Server		

Bridged	no
Media Type	auto-negotiation

☑ Enable dynamic DHCP leases

	IPv4	IPv6	
IP Pool Start		2001:db8::2	
IP Pool End		2001:db8::ffff	
Lease Time	600	600	sec

☐ Enable static DHCP leases

MAC Address	IPv4 Address	IPv6 Address

☐ Enable IPv6 prefix delegation

Subnet ID *		
Subnet ID Width *		bits

☐ Enable IEEE 802.1X Authentication

Authentication Method	EAP-TLS
CA Certificate	
Local Certificate	
Local Private Key	
Identity	
Local Private Key Password	

Apply

Obrázek 18: Konfigurace LAN pro příklad 3

4.2 VRRP konfigurace

VRRP přes IPv6 (VRRPv3) není podporováno.

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 20: 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 (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.

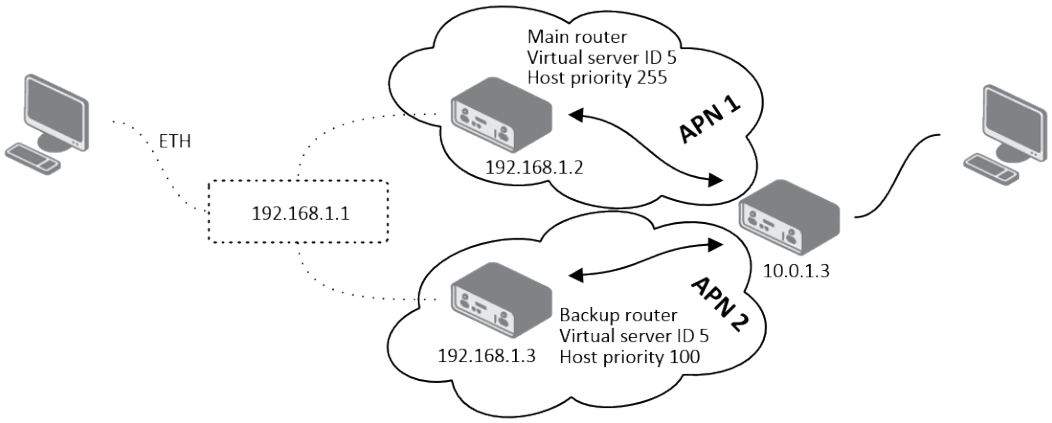
Tabulka 21: Check connection

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).

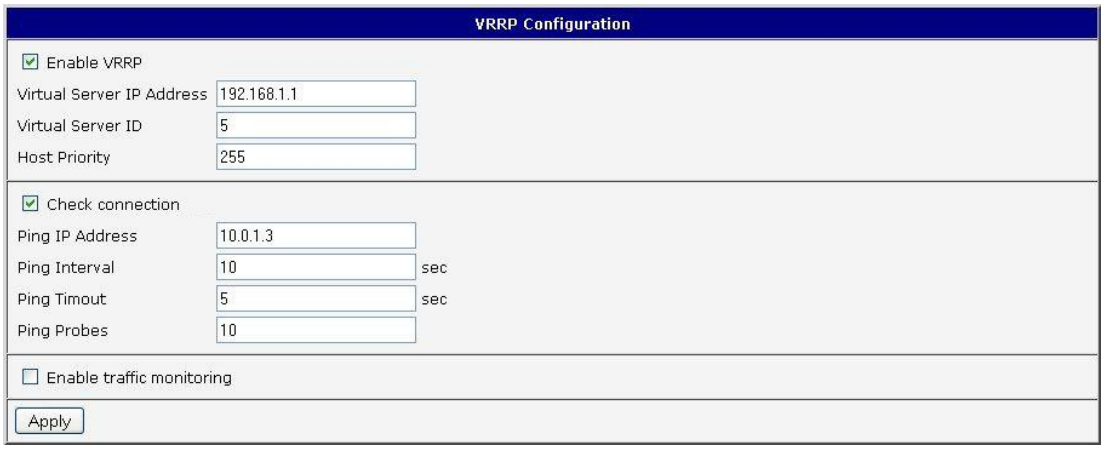
Pro sledování průchodnosti trasy je také možné využít parametr *Enable traffic monitoring*. Je-li tento parametr nastaven, pak se v případě, že je vysílán na sledovanou trasu paket jiný než ping, sleduje, zda do doby *Ping Timeout* přijde nějaká odpověď. Pokud ne, považuje se

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*.

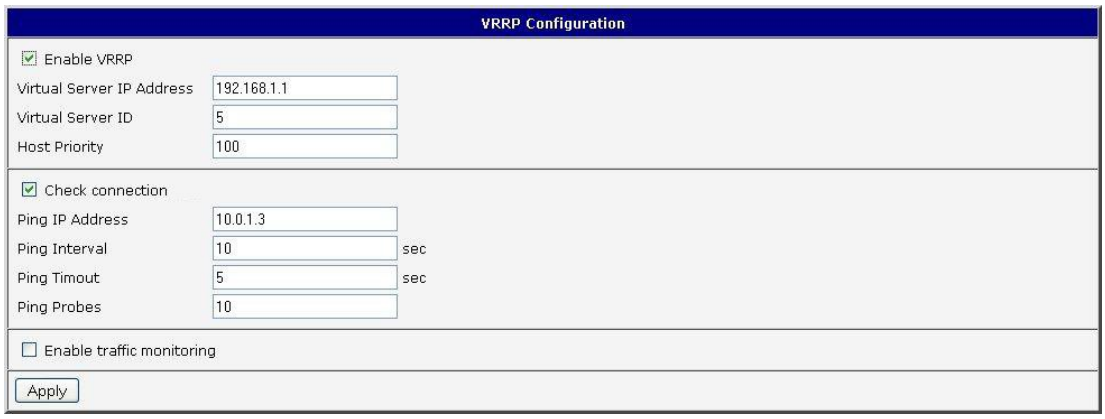
Nastavení protokolu VRRP:



Obrázek 19: Topologie k příkladu konfigurace VRRP



Obrázek 20: Příklad konfigurace VRRP – Hlavní router



Obrázek 21: Příklad konfigurace VRRP – Záložní router

4.3 Mobile WAN konfigurace

Zvolte položku *Mobile WAN* v sekci *Configuration* hlavního menu pro konfiguraci připojení do mobilní sítě. Konfigurační formulář je na obrázku 23.

4.3.1 Konfigurace připojení do mobilní sítě

Pokud je zaškrtnuta volba *Create connection to mobile network*, pak se router sám po zapnutí pokusí vytvořit spojení. Následující položky lze nastavit pro každou SIM kartu zvlášť.

Položka	Popis
Carrier	Výběr poskytovatele připojení (pouze pro routery **SmartStart SL302**).
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** – Autentizační metodu zvolí router. • **PAP** – Router používá autentizační metodu PAP. • **CHAP** – Router používá autentizační metodu CHAP.
IP Mode	Výběr použité verze IP protokolu: • **IPv4** – Bude použit pouze IPv4 protokol (výchozí). • **IPv6** – Bude použit pouze IPv6 protokol. • **IPv4/IPv6** – Souběh IPv4 a IPv6 protokolů – nezávislý dual stack.
IP Address	Pouze v režimu IPv4 nebo IPv4/IPv6. IPv4 adresa SIM karty. Nastavit pouze v případě, že byla 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. • Je možné vybrat konkrétní způsob přenosu dat: **LTE**, **UMTS/HSPA**, **GPRS/EDGE**.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
PIN	Nutno nastavit pouze pokud to vyžaduje SIM karta routeru. Po několika špatných pokusech o zadání PIN dojde k zablokování SIM karty.
MRU	Maximum Receiving Unit – maximální velikost paketu, kterou může router na daném rozhraní přijmout. Výchozí je 1500 B. Jiná velikost může způsobit nesprávnou funkci. Minimální hodnota v režimu IPv4 a IPv4/IPv6 je 128 B. Minimální hodnota v režimu IPv6 je 1280 B.
MTU	Maximum Transmission Unit – maximální velikost paketu, kterou může router na daném rozhraní odeslat. Výchozí je 1500 B. Jiná velikost může způsobit nesprávnou funkci. Minimální hodnota v režimu IPv4 a IPv4/IPv6 je 128 B. Minimální hodnota v režimu IPv6 je 1280 B.

Tabulka 22: Konfigurace přihlášení do mobilní sítě

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**“. V případě detekce operátora AT&T se použije defaultní APN „phone“. APN definuje mobilní operátor.
- Je-li v poli *APN* zadáno slovo *blank*, je APN routerem interpretováno jako prázdné.

Zkontrolujte správně zadaný PIN, 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 autentizační metodu nebo jiný typ sítě.

4.3.2 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*). Je možné vyplnit IPv4, nebo IPv6 adresu DNS serveru (nebo obě) – v závislosti na vybraném režimu *IP Mode*.

4.3.3 Konfigurace kontroly spojení s mobilní sítí

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

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*, *Ping IPv6 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 obě SIM karty. Jako ping adresu lze použít IP adresu, u které je jisté, že je stále funkční a je na ní možné posílat ICMP (ICMPv6) 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.

Pro routery **SmartStart SL302** připojené do sítě operátora **Verizon** (router automaticky rozpozná): Interval mezi pokusy o opětovné připojení do mobilní sítě se s vyšším počtem pokusů prodlužuje. První dva pokusy jsou provedeny po 1 minutě, pak se interval prodlužuje na 2, 8 a 15 minut. Devátý a každý další pokus je proveden po 90 minutách.

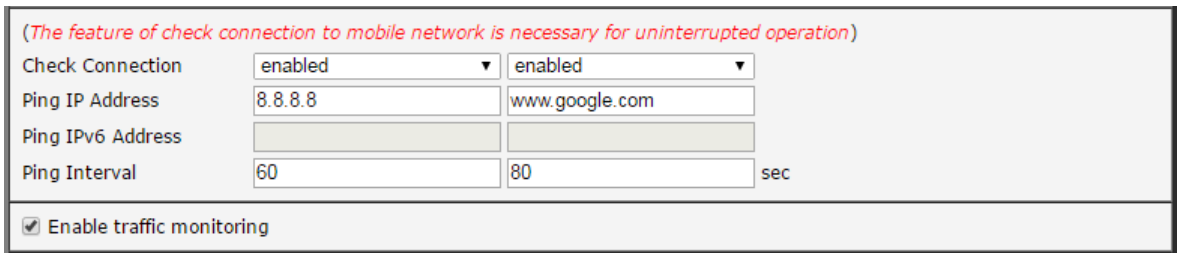
Položka	Popis
Ping IP Address	IPv4 adresa nebo doménové jméno pro odesílání kontrolního pingu. Dostupné v IPv4 a IPv4/IPv6 (*IP Mode*).
Ping IPv6 Address	IPv6 adresa nebo doménové jméno pro odesílání kontrolního pingu. Dostupné v IPv6 a IPv4/IPv6 (*IP Mode*).
Ping Interval	Časový interval odesílání pingu.

Tabulka 23: Konfigurace kontroly spojení s mobilní sítí

Při zaškrtnutí funkce *Enable Traffic Monitoring* router přestane posílat ping dotazy na *Ping IP Address* (*Ping IPv6 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* (*Ping IPv6 Address*).

4.3.4 Příklad nastavení kontroly spojení

Na obrázku níže je 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 22: Příklad 1 – Mobile WAN konfigurace

4.3.5 Konfigurace datového limitu

Položka	Popis
Data Limit	Nastavuje maximální očekávané množství přenesených dat (vyslaných i přijatých) přes GPRS v jedné účtovací periodě (měsíc). Maximální hodnota je 2 TB (2097152 MB).
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 24: Konfigurace datového limitu

Pokud je parametr *Data Limit State* níže nastaven na hodnotu *not applicable* nebo pokud není na stránce *SMS Configuration* zaškrtnuta položka *Send SMS when datalimit exceeded*, bude zde nastavený datový limit ignorován.

4.3.6 Konfigurace přepínání mezi SIM kartami

Ve spodní části konfiguračního formuláře je možné specifikovat pravidla pro přepínání mezi dvěma SIM kartami.

Router bude mezi SIM kartami přepínat automaticky na základě pravidel zde nastavených – ruční povolení, roaming, datový limit a stav binárního vstupu. Použitá SIM je výsledkem logického součinu (AND) těchto nastavení.

Položka	Popis
SIM Card	Povolí nebo zakáže použití SIM karty. Pokud jsou všechny SIM karty zakázány (nastaveny na *disabled*), daný bezdrátový modul není vůbec použit. • **enabled** – Je možné použít tuto SIM kartu. • **disabled** – Použití SIM karty je zakázáno, nelze ji použít a nebude nikdy automaticky vybrána.
Roaming State	Nastavení přepínání SIM karet na základě roamingu. Pro správnou funkci je nutné mít na SIM kartě povolený roaming! • **not applicable** – SIM kartu je možné použít kdekoli, i v roamingu. • **home network only** – SIM kartu je možné použít pouze pokud nebyl detekován roaming.
Data Limit State	Nastavení přepínání SIM karet na základě datového limitu nastaveného výše. • **not applicable** – SIM kartu je možné použít vždy, nehledě na překročení datového limitu. • **not exceeded** – SIM kartu je možné použít pouze pokud nebyl překročen datový limit nastavený výše.
BIN0 State	Nastavení přepínání SIM karet dle stavu binárního vstupu 0. • **not applicable** – SIM kartu je možné použít vždy, nehledě na stav vstupu BIN0. • **on** – SIM kartu je možné použít pouze pokud je stav vstupu BIN0 logická 0, tj. pod napětím. • **off** – SIM kartu je možné použít pouze pokud je stav vstupu BIN0 logická 1, tj. bez napětí.

Tabulka 25: Konfigurace přepínání mezi SIM kartami

Následující parametry definují politiku přepínání SIM karet v rámci bezdrátového modulu.

Položka	Popis
Default SIM Card	Definuje výchozí SIM kartu, s kterou se router bude pokoušet sestavit spojení do mobilní sítě. • **1st** – První SIM karta je výchozí. • **2nd** – Druhá SIM karta je výchozí.
Initial State	Definuje počáteční stav (akci) bezdrátového modulu po vybrání SIM karty. • **online** - po vybrání SIM karty dojde k sestavení spojení do mobilní sítě (výchozí). • **offline** - po vybrání SIM karty přejde modul do neaktivního stavu off-line. Poznámka: Počáteční stav je možné vzdáleně změnit pouze prostřednictvím SMS – viz *SMS Configuration*. Bezdrátový modul je přepnut do off-line režimu také pokud není možné vybrat žádnou SIM kartu.
Switch to other SIM card when connection fails	Dojde-li k výpadku spojení do mobilní sítě, tento parametr zajistí přepnutí na záložní SIM kartu. K přepnutí na záložní SIM kartu dojde tehdy, je-li funkcí *Check connection to mobile network* výše detekována ztráta spojení do mobilní sítě.
Switch to default SIM card after timeout	Tímto parametrem je možné aktivovat přepnutí zpět na výchozí SIM kartu po uplynutí časové prodlevy definované níže. Funguje pouze je-li definována výchozí SIM karta a pouze došlo-li k přepnutí z důvodu selhání (fail) nebo roamingu. Parametr lze použít pouze byla-li aktivována položka *Switch to other SIM card when connection fails*.
Initial Timeout	První pokus o přepnutí zpět na výchozí SIM kartu se provede za čas definovaný tímto parametrem, povolený rozsah je 1 až 10000 minut.
Subsequent Timeout	Při neúspěšném pokusu o přepnutí zpět se router podruhé pokusí za čas definovaný tímto parametrem – 1 až 10000 minut.
Additive Constant	Každý další pokus o přepnutí zpět na výchozí SIM kartu se provede za čas spočítaný jako součet času předchozího pokusu a času definovaného tímto parametrem, rozmezí je 1 až 10000 minut.

Tabulka 26: Parametry pro přepínání SIM karet

1st Mobile WAN Configuration

☑ Create connection to mobile network

	1st SIM card	2nd SIM card	
Carrier	AT&T	automatic detection	
APN *	conel.agnep.cz		
Username *			
Password *			
Authentication	PAP or CHAP	PAP or CHAP	
IP Mode	IPv4	IPv4	
IP Address *			
Phone Number *			
Operator *			
Network Type	automatic selection	automatic selection	
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes
DNS Settings	get from operator	get from operator	
DNS IP Address			
DNS IPv6 Address			

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

Check Connection	disabled	disabled	
Ping IP Address			
Ping IPv6 Address			
Ping Interval			sec

☐ Enable traffic monitoring

Data Limit			MB
Warning Threshold			%
Accounting Start		1	
SIM Card	enabled	enabled	
Roaming State	not applicable	not applicable	
Data Limit State	not applicable	not applicable	
BIN0 State	not applicable	not applicable	
Default SIM Card	1st		
Initial State	online		

☐ Switch to other SIM card when connection fails
☐ Switch to default SIM card after timeout

Initial Timeout		min
Subsequent Timeout *		min
Additive Constant *		min

☐ Enable PPPoE bridge mode

* *can be blank*

Apply

Obrázek 23: Mobile WAN konfigurace

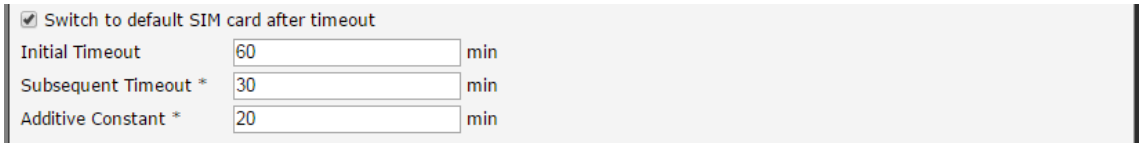
4.3.7 Příklady konfigurace přepínání SIM karet

Příklad 1: Přepnutí po časovém limitu

Mějme zaškrtnutu volbu *Switch to primary SIM card after timeout* a nastaveny následující parametry:

- *Initial Timeout* – 60 min,
- *Subsequent Timeout* – 30 min,
- *Additional Timeout* – 20 min.

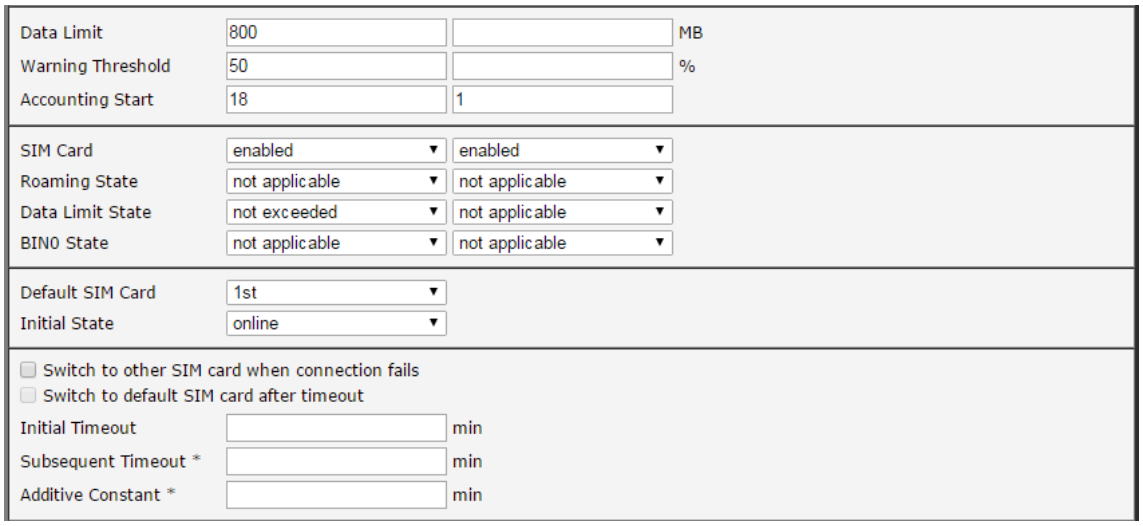
První pokus o přepnutí na primární SIM kartu se provede po 60 minutách. Při neúspěšném přepnutí se druhý pokus provádí po 30 minutách. Třetí po 50 minutách (30+20), čtvrtý po 70 minutách (30+20+20).



Obrázek 24: Konfigurace přepínání SIM karet pro příklad 1

Příklad 2: Přepnutí po dosažení datového limitu

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:



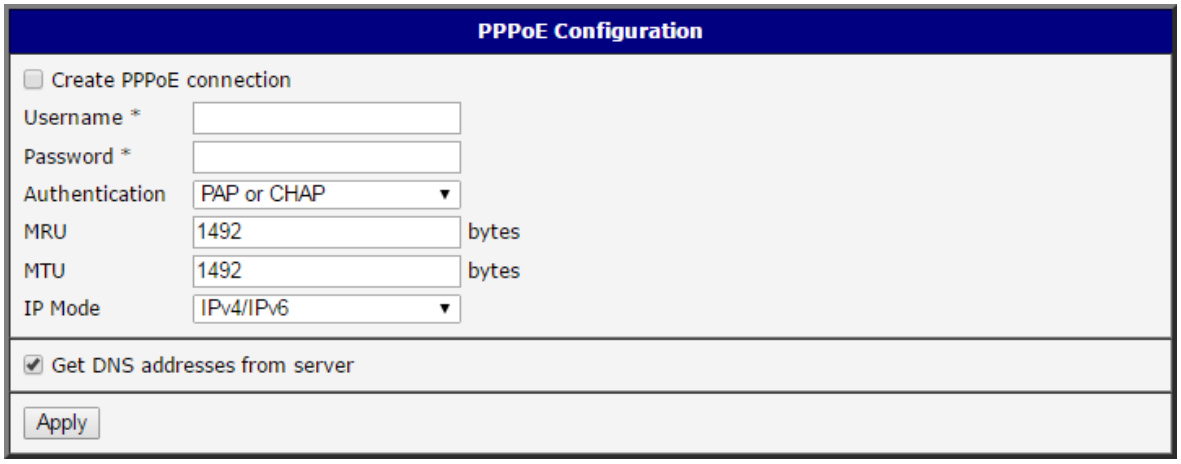
Obrázek 25: Konfigurace přepínání SIM karet pro příklad 2

4.3.8 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*.

4.4 PPPoE konfigurace

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 26: Konfigurace PPPoE

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** – Autentizační metodu zvolí router. • **PAP** – Router používá autentizační metodu PAP. • **CHAP** – Router používá autentizační metodu CHAP.
IP Mode	Výběr použité verze IP protokolu: • **IPv4** – Bude použit pouze IPv4 protokol (výchozí). • **IPv6** – Bude použit pouze IPv6 protokol. • **IPv4/IPv6** – Souběh IPv4 a IPv6 protokolů – dual stack.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
MRU	Maximum Receiving Unit – Identifikuje maximální velikost paketu, kterou může router na daném rozhraní přijmout. Z výroby je nastavena velikost na 1492 B (bytů). Jiná velikost může způsobit nesprávnou funkci. Minimální hodnota v režimu IPv4 a IPv4/IPv6 je 128 B. Minimální hodnota v režimu IPv6 je 1280 B.
MTU	Maximum Transmission Unit – Identifikuje maximální velikost paketu, kterou je router na daném rozhraní schopen odeslat. Z výroby je nastavena na 1492 B (bytů). Jiná velikost může způsobit nesprávnou funkci. Minimální hodnota v režimu IPv4 a IPv4/IPv6 je 128 B. Minimální hodnota v režimu IPv6 je 1280 B.
Get DNS addresses from server	Ve výchozím stavu je povoleno získání DNS adres ze serveru.

Tabulka 27: Konfigurace PPPoE

Při nastavení chybné velikosti paketu (MRU, MTU) se nemusí provést přenos dat.

4.5 WiFi konfigurace

Tato položka je dostupná pouze tehdy, je-li v routeru osazen WiFi modul.

Volbou položky *WiFi* v sekci *Configuration* webového rozhraní routeru lze vyvolat stránku s konfigurací WiFi. Zaškrtávací box *Enable WiFi* v úvodu stránky slouží k aktivaci WiFi. Dále je možné nastavit následující vlastnosti popsané v tabulce níže.

Protokol RADIUS (Remote Authentication Dial-In User Service) pro centralizovanou správu autentizace, autorizace a účtování (accountingu, AAA) je podporován na WiFi rozhraní. Router může být pouze RADIUS klient (ne server) – typicky jako WiFi AP (Access Point), který zprostředkovává komunikaci koncového uživatele s RADIUS serverem. V režimu WiFi STA (Station) je podporována pouze autentizační metoda EAP-PEAP/MSCHAPv2 (obojí PEAPv0 a PEAPv1 jsou podporovány).

Položka	Popis
Operating mode	Režim WiFi modulu: • **access point (AP)** – Router se stane přístupovým bodem, ke kterému je možné se připojit jinými zařízeními v režimu host *station (STA)*. • **station (STA)** – Router se stane klientskou stanicí, tzn. že přijímá datové pakety z dostupného access pointu (AP) a naopak ty, které přijdou po kabelu, odesílá prostřednictvím wifi sítě.
SSID	Jedinečný identifikátor WiFi sítě.
Broadcast SSID	Způsob vysílání jedinečného identifikátoru sítě SSID v tzv. majákovém rámci (beacon frame) a způsob reakce na žádost o vyslání majákového rámce. • **Enabled** – SSID je vysíláno v majákovém rámci. • **Zero length** – SSID je z majákového rámce vynecháno (vysláno s nulovou délkou) a žádosti o vyslání majákového rámce jsou ignorovány. • **Clear** – Všechy znaky SSID jsou v majákovém rámci nahrazeny číslicí 0. Původní délka SSID je však zachována. Žádosti o vyslání majákového rámce jsou ignorovány.
Probe Hidden SSID	Zjišťuje skryté SSID (dostupné pouze pro režim *station (STA)*).

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Client Isolation	Pouze v režimu *access point (AP)*. Pokud je zaškrtnuto, router bude izolovat každého přes WiFi připojeného klienta od ostatních klientů připojených přes WiFi v tom smyslu, že bude každý ve svojí síti LAN a neuvidí v síti ostatní klienty. Pokud nebude zaškrtnuto, WiFi AP se chová jako standardní switch, ale bezdrátový – klienti jsou ve stejné LAN a vidí na sebe navzájem.
Country Code	Kód země, kde je router s WiFi modulem používán. Tento kód je zadáván ve formátu ISO 3166-1 alpha-2. Jestliže kód není zadán a router nemá vlastní systém pro zjištění *country code*, použije se výchozí nastavení US. Jestliže není country code zadán nebo je zadán špatný *country code*, potom může dojít k porušení regulačních předpisů určujících využití kmitočtového pásma v dané zemi. **Tato položka není dostupná u routeru SmartStart SL302** – jako country code je napevno nastavena hodnota "US" v těchto verzích routeru.
HW Mode	HW mód WiFi standardu, který bude přístupový bod (AP) podporovat: • IEE 802.11b (2.4 GHz) • IEE 802.11b+g (2.4 GHz) • IEE 802.11b+g+n (2.4 GHz)
Channel	Kanál, na kterém access point (AP) vysílá. Pro jednotlivé *country code* jsou povoleny různé rozsahy kanálů! Kanály podporované na 2.4 GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13. Router **SmartStart SL302** podporuje pouze kanály 1 až 11!
BW 40 MHz	Volba pro HW mód 802.11n, která současně povoluje využití dvou standardních 20MHz kanálů. Volba je dostupná i v režimu STA a pro využití vyšší propustnosti díky dvěma kanálům musí být povolena v režimu AP i STA.
WMM	Zapíná jednoduchý QoS pro WiFi sítě. Tato verze negarantuje propustnost sítě, ale je určena pro jednoduché aplikace vyžadující QoS, například VoIP.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Authentication	Zajišťuje řízení přístupu oprávněných uživatelů ve WiFi síti: • **Open** – žádná autentizace není vyžadována, tzn. volný přístupový bod (AP). • **Shared** – Základní autentizace pomocí WEP klíče. • **WPA-PSK** – Autentizace pomocí dokonalejší autentizační metody PSK-PSK. • **WPA2-PSK** – Oproti WPA-PSK přináší nové šifrování AES. • **WPA-Enterprise** – RADIUS autentizace pomocí externího serveru, uživatelského jména a hesla. • **WPA2-Enterprise** – RADIUS autentizace s lepším šifrováním. • **802.1X** – RADIUS autentizace založená na kontrole přístupu k portům (PNAC) s využitím protokolu EAP (Extensible Authentication Protocol).
Encryption	Typ šifrování dat ve WiFi síti: • **None** – Žádné šifrování dat. • **WEP** – Šifrování pomocí statického WEP klíče, které lze použít u *Shared* autentizace. • **TKIP** – Dynamická správa šifrovacích klíčů, které je možné použít u *WPA-PSK* a *WPA2-PSK* autentizace. • **AES** – Dokonalejší šifra použitá při autentizaci *WPA2-PSK*.
WEP Key Type	Typ WEP klíče při WEP šifrování: • **ASCII** – WEP klíč je zadán v ASCII formátu. • **HEX** – WEP klíč je zadán v HEX formátu.
WEP Default Key	Určuje výchozí WEP klíč.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
WEP Key 1–4	Možnost zadání až 4 WEP klíčů: • WEP klíč v ASCII formátu musí být zadán v uvozovkách v následujících možných délkách: – 5 ASCII znaků (40b WEP klíč) – 13 ASCII znaků (104b WEP klíč) – 16 ASCII znaků (128b WEP klíč) • WEP klíč v hexadecimálním formátu musí být zadáván pouze pomocí číslic a písmen "A" až "F" v následujících možných délkách: – 10 hexadecimálních číslic (40b WEP klíč) – 26 hexadecimálních číslic (104b WEP klíč) – 32 hexadecimálních číslic (128b WEP klíč)
WPA PSK Type	Typ šifrování při WPA PSK autentizaci: • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Klíč použitý při WPA-PSK autentizaci. Klíč je nutné zadávat podle výše zvoleného typu následovně: • **256-bit secret** – 64 hexadecimálních číslic. • **ASCII passphrase** – 8 až 63 znaků, které jsou následně konvertovány do PSK. • **PSK File** – Absolutní cesta k souboru obsahující seznam párů (PSK klíč, MAC adresa).
RADIUS Auth Server IP	IPv4 nebo IPv6 adresa RADIUS serveru. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.
RADIUS Auth Password	Přístupové heslo k RADIUS serveru. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.
RADIUS Auth Port	Port RADIUS serveru. Výchozí hodnota je 1812. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
RADIUS Acct Server IP	IPv4 nebo IPv6 adresa serveru RADIUS pro účtování (accounting). Je nutné vyplnit pouze pokud je server pro účtování odlišný od serveru pro autentizaci a autorizaci. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.
RADIUS Acct Password	Přístupové heslo k serveru RADIUS pro účtování (accounting). Je nutné vyplnit pouze pokud je server pro účtování odlišný od serveru pro autentizaci a autorizaci. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.
RADIUS Acct Port	Port serveru RADIUS pro účtování (accounting). Výchozí hodnota je 1813. Je nutné vyplnit pouze pokud je server pro účtování odlišný od serveru pro autentizaci a autorizaci. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.
RADIUS EAP Authentication	Volba typu autentizačního protokolu (EAP-PEAP/MSCHAPv2 nebo EAP-TLS).
RADIUS CA Certificate	Definice CA certifikátu pro autentizační protokol EAP-TLS.
RADIUS Local Certificate	Definice lokálního certifikátu pro autentizační protokol EAP-TLS.
RADIUS Local Private Key	Definice lokálního privátního klíče pro autentizační protokol EAP-TLS.
RADIUS Local Private Key Password	Definice hesla pro privátní klíč autentizačního protokolu EAP-TLS. Položka je dostupná pouze pro autentizační protokol EAP-TLS.
RADIUS Identity	Uživatelské jméno pro RADIUS autentizaci – identita. Dostupné pouze v režimu STA a při zvolení některé z autentizačních metod RADIUS.
RADIUS Password	Přístupové heslo pro RADIUS autentizaci. Dostupné pouze v režimu STA a při zvolení některé z autentizačních metod RADIUS.
Access List	Určuje způsob aplikace Access/Deny listu: • **Disabled** – Access/Deny list není používán. • **Accept** – Pouze položky v Access/Deny listu mají přístup k síti. • **Deny** – Položky v Access/Deny listu mají zakázaný přístup k síti.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Accept/Deny List	Přístupový list klientských MAC adres nastavující přístup do sítě. Jednotlivé MAC adresy jsou odděleny novým řádkem.
Syslog Level	Úroveň sdílnosti při výpisu do systémového logu: • **Verbose debugging** – Nejvyšší úroveň sdílnosti. • **Debugging** • **Informational** – Výchozí úroveň pro zápis běžných událostí. • **Notification** • **Warning** – Nejnižší úroveň sdílnosti.
Extra options	Umožňuje definovat doplňující parametry

Tabulka 28: Konfigurace WiFi

WiFi Configuration

Enable WiFi	
Operating Mode	access point (AP)
SSID	
Broadcast SSID	enabled
Probe Hidden SSID	
Client Isolation	
Country Code *	
HW Mode	IEEE 802.11b
Channel	1
BW 40 MHz	
WMM	
Authentication	open
Encryption	none
WEP Key Type	ASCII
WEP Default Key	1
WEP Key 1	
WEP Key 2	
WEP Key 3	
WEP Key 4	
WPA PSK Type	256-bit secret
WPA PSK	
RADIUS Auth Server IP	
RADIUS Auth Password	
RADIUS Auth Port *	1812
RADIUS Acct Server IP *	
RADIUS Acct Password *	
RADIUS Acct Port *	1813
RADIUS EAP Authentication	EAP-PEAP/MSCHAPv2
RADIUS CA Certificate	
RADIUS Local Certificate	
RADIUS Local Private Key	
RADIUS Identity	
RADIUS Password	
Access List	disabled
Accept/Deny List	
Syslog Level	informational
Extra options *	

** can be blank*

Apply

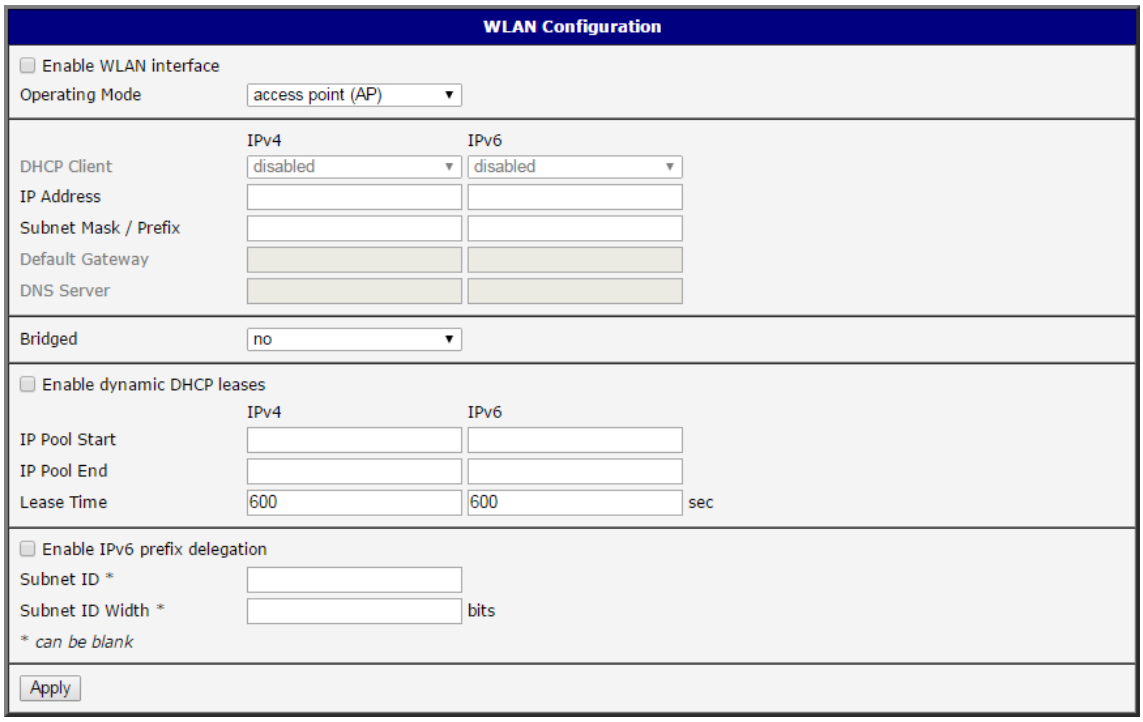
Obrázek 27: Konfigurace WiFi

4.6 WLAN konfigurace

Tato položka je dostupná pouze tehdy, je-li v routeru osazen WiFi modul.

Volbou položky *WLAN* v sekci *Configuration* webového rozhraní routeru lze vyvolat stránku s konfigurací WiFi sítě a DHCP serveru fungujícím na této síti. Zaškrtávací box *Enable WLAN interface* v úvodu stránky slouží k aktivaci WiFi LAN rozhraní.

Konfigurační stránka je rozdělena do sloupců IPv4 a IPv6. Jde o nastavení souběhu protokolů IPv4 a IPv6, nezávislý dual stack. Je možné nastavit jeden z protokolů nebo oba. Položky konfigurace a rozdíly v nastavení IPv6 a IPv4 jsou popsány v tabulkách níže.



Obrázek 28: WLAN konfigurace

Položka	Popis
Operating Mode	Režim WiFi modulu: • **access point (AP)** – Router se stane přístupovým bodem, ke kterému je možné se připojit jinými zařízeními v režimu host *station (STA)*. • **station (STA)** – Router se stane klientskou stanicí, tzn. že přijímá datové pakety z dostupného access pointu (AP) a naopak ty, které přijdou po kabelu, odesílá prostřednictvím wifi sítě.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
DHCP Client	Aktivuje/deaktivuje DHCP klienta. Pokud je povolen v IPv6 sloupci, jedná se o DHCPv6 klienta.
IP Address	Pevně nastavená IP adresa WiFi routeru. Ve sloupci IPv4 je nutné použít zápis adresy ve formátu IPv4, ve sloupci IPv6 ve formátu IPv6. Zkrácené zápisy IPv6 adres jsou povoleny.
Subnet Mask / Prefix	Specifikuje masku sítě v případě IPv4. Ve sloupci IPv6 je nutno vyplnit prefix – jedno číslo v rozsahu 0 až 128.
Default Gateway	Výchozí brána – při zadání IP adresy výchozí brány se všechny pakety, pro které nebyl nalezen záznam ve směrovací tabulce, odesílají na tuto adresu. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
DNS Server	Adresa, na kterou jsou přeposlány všechny DNS dotazy. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
Bridged	Aktivace režimu bridge: • **no** – Není aktivován režim bridge (výchozí hodnota). WLAN síť není propojena s LAN sítí routeru. • **yes** – Režim bridge je aktivován. WLAN síť je propojena s jednou či více LAN sítěmi routeru. V tomto případě se ignoruje nastavení většiny položek z této tabulky a místo toho se přebírá nastavení vybraného síťového rozhraní (LAN).

Tabulka 29: Konfigurace WLAN

Ve spodní části tohoto konfiguračního formuláře lze zaškrtnutím položky *Enable dynamic DHCP leases* povolit dynamické přidělování IP adres pomocí DHCP (DHCPv6) serveru. Zároveň je možné specifikovat hodnoty popsané v následující tabulce:

Item	Description
IP Pool Start	Začátek rozsahu IP adres, které budou přidělovány DHCP klientům. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
IP Pool End	Konec rozsahu IP adres, které budou přidělovány DHCP klientům. Je třeba použít odpovídající zápis adresy ve sloupci IPv4 a IPv6.
Lease Time	Čas v sekundách, po který smí klient IP adresu používat.

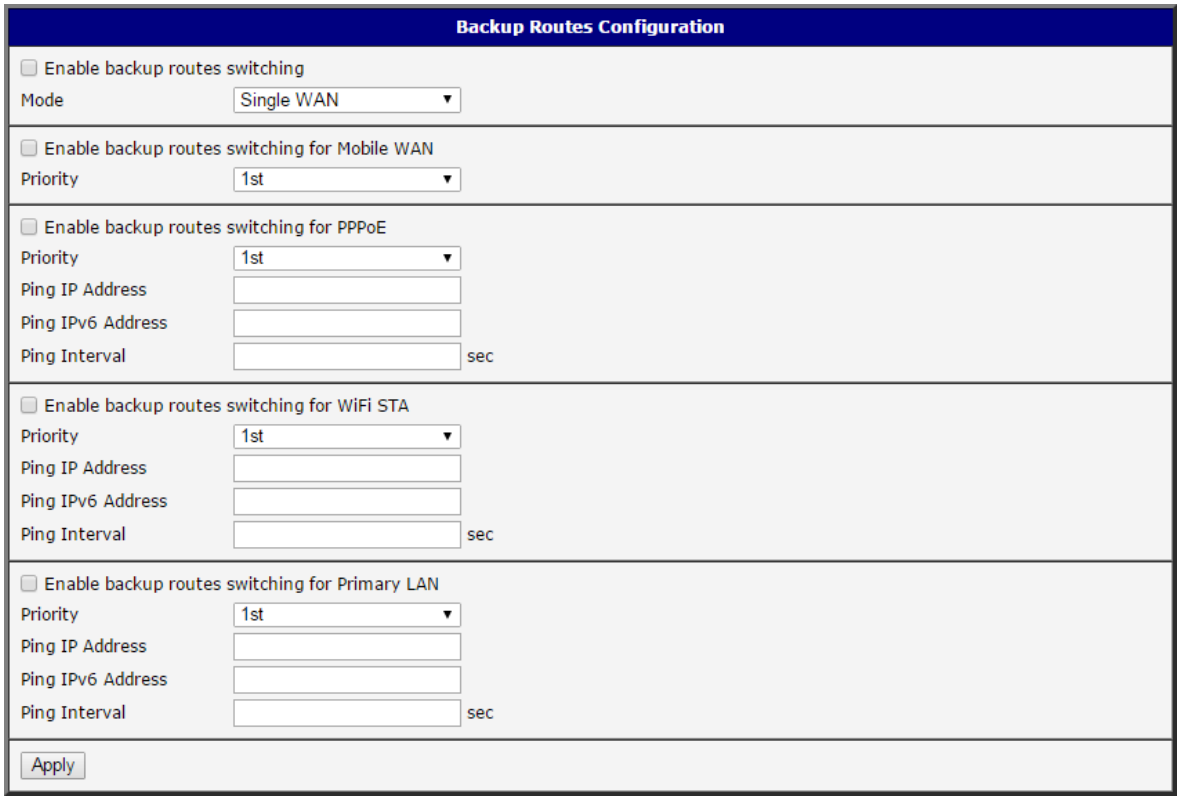
Tabulka 30: Konfigurace DHCP serveru

Viz kapitolu 4.1.2 pro více informací o funkci *IPv6 Prefix Delegation* – delegace IPv6 prefixu. Funguje v routeru automaticky, jedná se o pokročilé nastavení, které pravděpodobně nebude třeba konfigurovat.

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

4.7 Zálohované připojení (Backup Routes)

Pomocí konfiguračního formuláře na stránce *Backup Routes* je možné nastavit zálohování primárního připojení do internetu (mobilní sítě) jiným typem připojení. Je také možno aktivovat režim více připojení do internetu (*Multiple WANs*). Každému způsobu připojení lze definovat určitou prioritu. Vlastní přepínání se provádí na základě nastavených priorit a stavu kontroly spojení.



Obrázek 29: Backup Routes Configuration

Položka	Popis
Enable backup routes switching	Pokud je zaškrtnuto, výchozí cesta je vybrána dle nastavení níže. Pokud není zaškrtnuto, systém záložních cest pracuje ve zpětně kompatibilním módu a výchozí cesta se vybírá na základě implicitních priorit (popsaných níže).
Mode	• **Single WAN** – Výchozí režim. Pouze jedno síťové rozhraní může být použito pro WAN komunikaci (připojení do internetu) v daný čas. Jiná rozhraní jsou použita až pokud připojení přes preferované rozhraní selže. • **Multiple WANs** – Více síťových rozhraní může být připojeno do internetu (WAN) najednou. Odpovědi na komunikaci přijatou z WAN jsou potom odesílány přes stejné rozhraní, odkud požadavky přišly. Komunikace tak zůstává vždy na daném rozhraní. Komunikace, jež je iniciována z routeru nebo ze sítě za routerem, je vždy do WAN odesílána přes rozhraní s nejvyšší prioritou dle nastavení níže.

Tabulka 31: Backup Routes Configuration

Jednotlivá rozhraní je nutné do systému záložních cest přidat zaškrtnutím *Enable* u příslušného rozhraní: *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for PPPoE*, *Enable backup routes switching for WiFi STA* nebo *Enable backup routes switching for Primary LAN*. Takto přidaná (aktivovaná rozhraní) jsou pak použita v režimu *Single WAN* nebo *Multiple WANs* podle jejich explicitně nastavených priorit a podle stavu kontroly spojení (pokud je zapnuta vyplněním IP adresy pro ping).

Položka	Popis
Priority	Priorita pro daný typ připojení.
Ping IP Address	Cílová IPv4 adresa nebo doménové jméno ping dotazů pro kontrolu spojení.
Ping IPv6 Address	Cílová IPv6 adresa nebo doménové jméno ping dotazů pro kontrolu spojení.
Ping Interval	Časové intervaly mezi odesílanými ping dotazy.

Tabulka 32: Backup Routes Interface Configuration

Pozor! Chcete-li v systému záložních cest využívat také připojení do mobilní sítě (*Mobile WAN*), je nutné u nastavení *Mobile WAN* nastavit kontrolu spojení (*Check Connection*) na *enabled + bind*, viz kap. 4.3.1.

Navíc se u síťových rozhraní, příslušejících k jednotlivým záložním cestám, kontroluje příznak "RUNNING". Tato kontrola řeší např. odpojení ethernetového kabelu. Je možné vyplnit pouze jednu nebo obě adresy pro kontrolní ping u každého rozhraní (IPv4 a IPv6) – v závislosti na IP protokolu použitém u jednotlivých rozhraní a u WAN připojení. Všechny změny v nastavení se projeví po stisknutí tlačítka *Apply*.

4.7.1 Implicitní priority systému záložních cest

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:

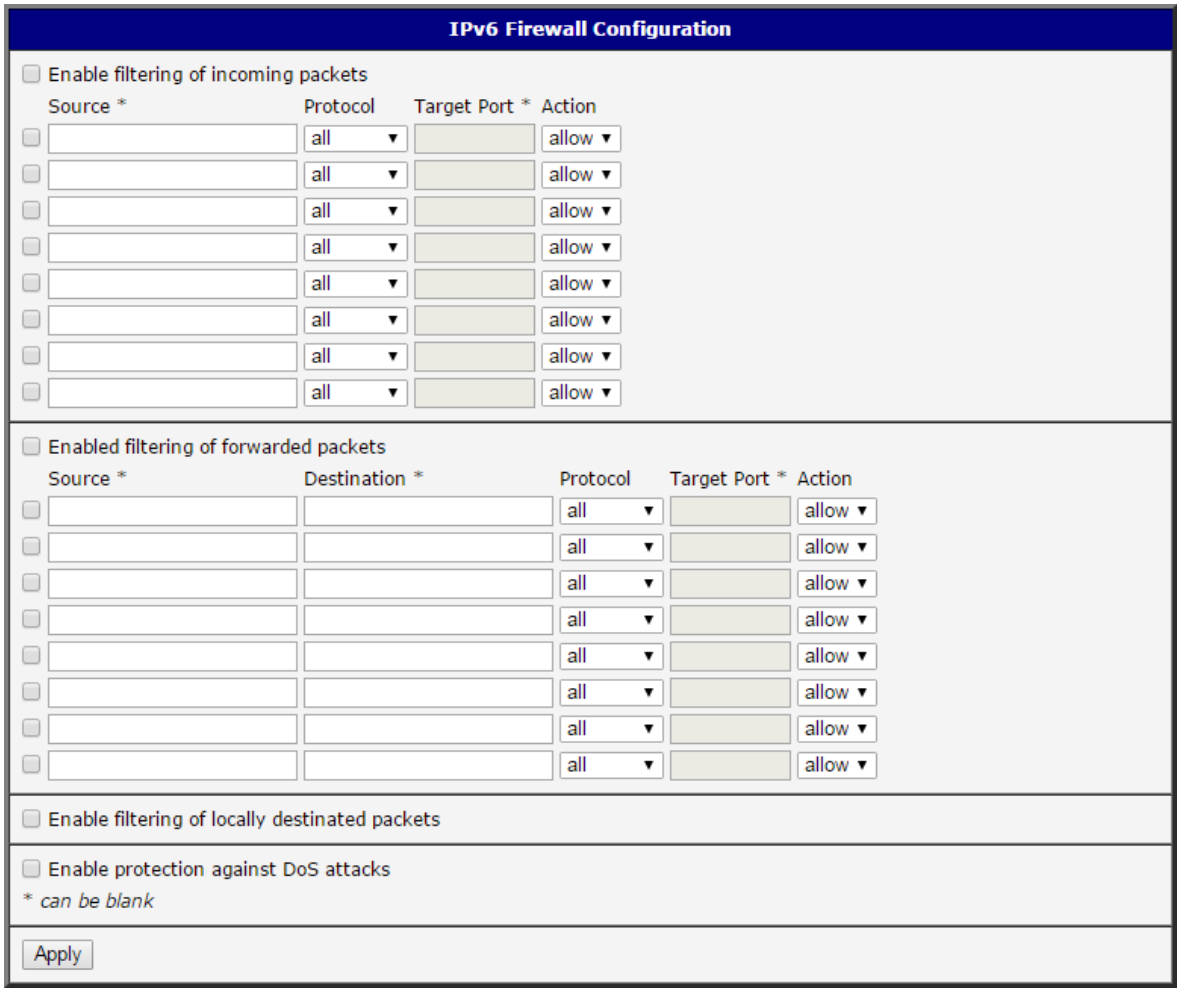
- Mobile WAN (usbX)
- PPPoE (ppp0)
- WiFi STA (wlan0)
- Primary LAN (eth0)

Příklad při použití implicitních priorit: Primary 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* ani *Enable WiFi* na stránce *WiFi* (nebo je WiFi používána v režimu AP).

Poznámka: Je nutné vzít v potaz, že i síťové rozhraní určené pro LAN se může stát WAN síťovým rozhraním, a to i při vypnutém systému *Backup Routes* (z důvodu výchozích priorit v režimu zpětné kompatibility). Komunikace z WAN síťového rozhraní může být v takovém případě blokována v závislosti na nastavení *NAT* a *Firewall*.

4.8 Firewall

Prvním bezpečnostním prvkem, na který příchozí pakety narazí, je kontrola povolených zdrojových IP adres a cílových portů. K dispozici je nezávislý IPv4 a IPv6 firewall, protože v routeru je implementován souběh IPv4 a IPv6 protokolů – dual stack. Kliknete-li v menu nalevo na položku *Firewall*, rozbalí se volby *IPv4* a *IPv6*. Na obrázku níže je zobrazen formulář konfigurace IPv6 firewallu – *IPv6 Firewall Configuration*. Konfigurační pole obou formulářů *IPv4 Firewall Configuration* a *IPv6 Firewall Configuration* mají stejný význam.



Obrázek 30: Konfigurace firewallu – IPv6 firewall

Lze specifikovat IP adresy, ze kterých je možný vzdálený přístup na router a vnitřní síť připojenou za routerem. Je-li zaškrtnuta položka *Enable filtering of incoming packets* (nachází se v úvodu konfiguračního formuláře *Firewall*), je tento bezpečnostní prvek zapnut a dochází ke kontrole veškerého datového toku vstupujícího do routeru vůči tabulce s IP adresami. To znamená, že se vstupujícími bude nakládáno podle pravidel specifikovaných v tabulce. Definovat lze až osm pravidel pro vstupující pakety. Nastavují se tyto parametry:

Položka	Popis
Source	IP adresa, na kterou je pravidlo aplikováno. Na stránce *IPv4 Firewall Configuration* jde o IPv4 adresu, na stránce *IPv6 Firewall Configuration* jde o IPv6 adresu.
Protocol	Protokol, pro který pravidlo platí: • **all** – Pravidlo platí pro všechny protokoly. • **TCP** – Pravidlo platí pro protokol TCP. • **UDP** – Pravidlo platí pro protokol UDP. • **ICMP/ICMPv6** – Pravidlo platí pro protokol ICMP. V případě *IPv6 Firewall Configuration* je k dispozici volba ICMPv6.
Target Port	Číslo portu, pro který pravidlo platí.
Action	Pravidlo – typ akce: • **allow** – Přístup povolen. • **deny** – Přístup zakázán.

Tabulka 33: Filtrování příchozích paketů

Následující část konfiguračního formuláře určuje politiku přeposílání. Pokud položka *Enabled filtering of forwarded packets* není zaškrtnuta, jsou pakety automaticky akceptovány a přeposílány dál podle směrovací tabulky. Pokud je tato položka povolena a příchozí paket je adresován na jiné síťové rozhraní, jsou na něj aplikována pravidla v této druhé tabulce. V případě, že bude podle pravidel v tabulce akceptován (existuje pravidlo pro jeho přeposílání), bude odeslán dále podle směrovací tabulky. Pokud pravidlo pro přeposlání paketu neexistuje, bude paket zahozen.

V tabulkách pro definici pravidel lze povolit také veškerý provoz v rámci zvoleného protokolu (specifikuje se pouze protokol), nebo vytvářet přísnější pravidla specifikováním položek pro zdrojové či cílové IP adresy a portu.

Položka	Popis
Source	IP adresa zdrojového zařízení, na kterou je pravidlo aplikováno. Na stránce *IPv4 Firewall Configuration* jde o IPv4 adresu, na stránce *IPv6 Firewall Configuration* jde o IPv6 adresu.
Destination	IP adresa cílového zařízení, na kterou je pravidlo aplikováno. Na stránce *IPv4 Firewall Configuration* jde o IPv4 adresu, na stránce *IPv6 Firewall Configuration* jde o IPv6 adresu.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Protocol	Protokol, pro který pravidlo platí: • **all** – Pravidlo platí pro všechny protokoly. • **TCP** – Pravidlo platí pro protokol TCP. • **UDP** – Pravidlo platí pro protokol UDP. • **ICMP/ICMPv6** – Pravidlo platí pro protokol ICMP. V případě *IPv6 Firewall Configuration* je k dispozici volba ICMPv6.
Target Port	Číslo portu, pro který pravidlo platí.
Action	Pravidlo – typ akce: • **allow** – Přístup povolen. • **deny** – Přístup zakázán.

Tabulka 34: Filtrování forwardingu

Dále je možné filtrovat dotazy na služby, které v routeru nejsou. Je-li aktivována položka *Enable filtering of locally destinated packets*, každý takový paket se bez jakékoliv informace automaticky zahodí.

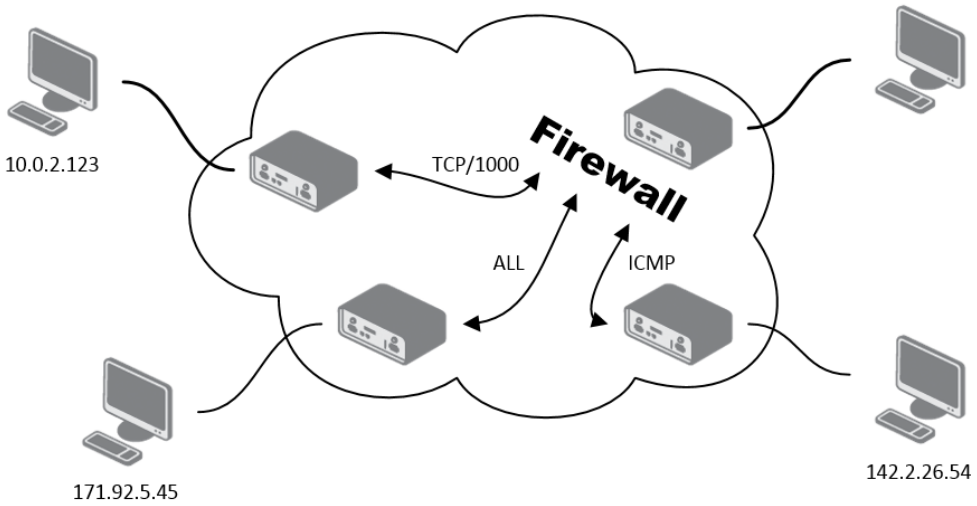
Pomocí položky *Enable protection against DoS attacks* se aktivuje ochrana proti DoS útokům (tj. útokům, při nichž je cílový systém zahlcen velkým množstvím nesmyslných dotazů), která limituje počet spojení na pět za sekundu.

4.8.1 Příklad nastavení IPv4 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 portu 1000.
- z adresy 142.2.26.54 pomocí protokolu ICMP.

Topologie příkladu a vyplněný konfigurační formulář je na obrázcích níže.



Obrázek 31: Topologie příkladu nastavení IPv4 firewallu

IPv4 Firewall Configuration

☑ Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
☑	171.92.5.45	all		allow
☑	10.0.2.123	TCP	100	allow
☑	142.2.26.54	ICMP		allow
☐		all		allow
☐		all		allow
☐		all		allow
☐		all		allow
☐		all		allow

☐ Enabled filtering of forwarded packets

	Source *	Destination *	Protocol	Target Port *	Action
☐			all		allow
☐			all		allow
☐			all		allow
☐			all		allow
☐			all		allow
☐			all		allow
☐			all		allow
☐			all		allow

☐ Enable filtering of locally destinated packets

☐ Enable protection against DoS attacks

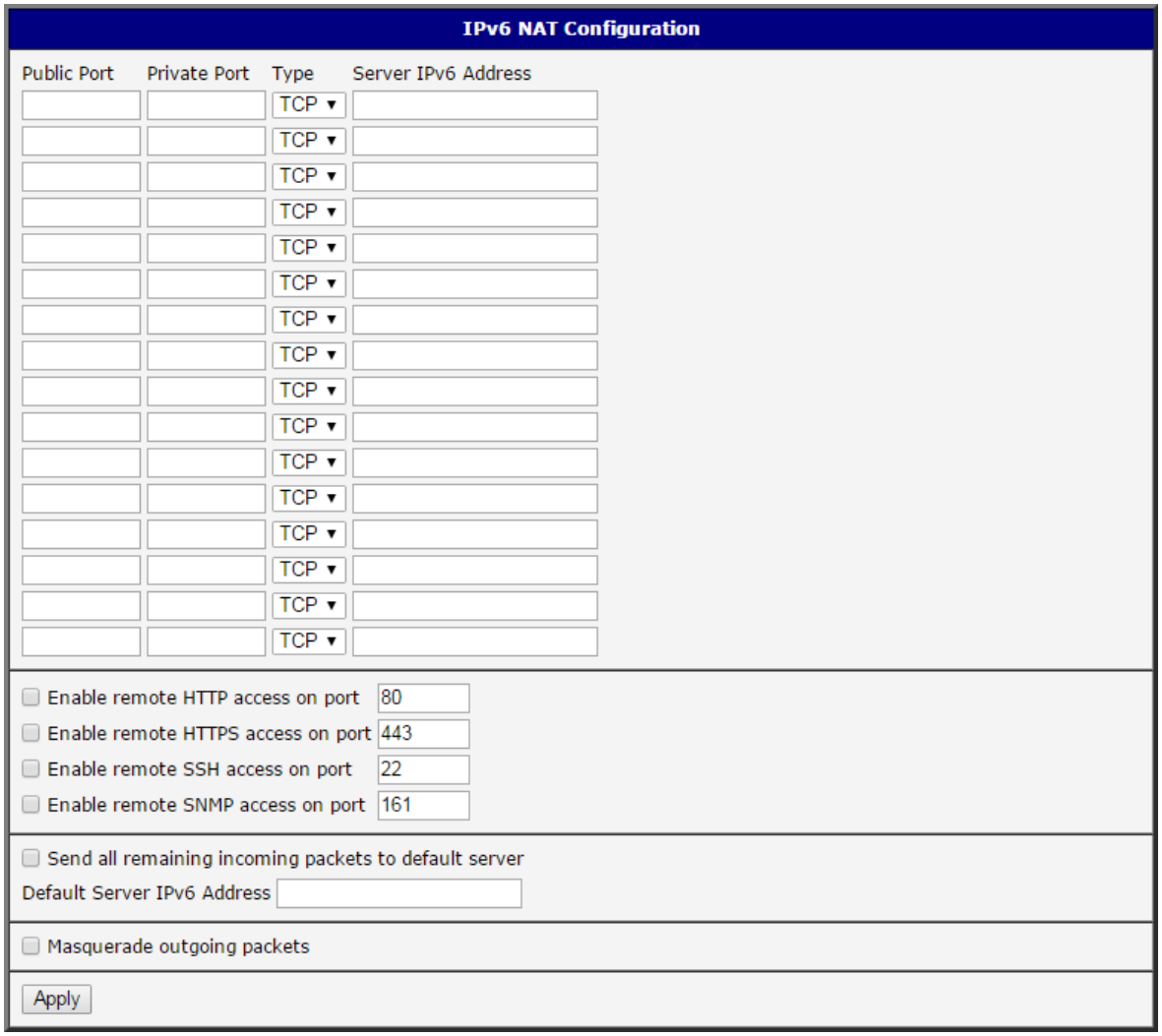
** can be blank*

Apply

Obrázek 32: Příklad nastavení IPv4 firewallu

4.9 NAT konfigurace

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. Je zde oddělené nastavení pro IPv4 a IPv6 NAT, protože v routeru je implementován nezávislý souběh IPv4 a IPv6 protokolů (dual stack). Položka NAT v menu nalevo se rozbalí a lze kliknutím na *IPv6* položku nastavit také IPv6 NAT – viz obrázek níže. Okno obsahuje šestnáct položek pro definici překladu adres.



Obrázek 33: Konfigurace NAT – IPv6 NAT Configuration

Položka	Popis
Public Port	Vnější port pro překlad adres.
Private Port	Vnitřní port pro překlad adres.
Type	Volba protokolu – TCP nebo UDP.
Server IPv4 address	Pouze na stránce *IPv4 NAT Configuration*. IPv4 adresa, kam budou přeposílána příchozí data.
Server IPv6 address	Pouze na stránce *IPv6 NAT Configuration*. IPv6 adresa, kam budou přeposílána příchozí data.

Tabulka 35: Konfigurace překladu adres (NAT)

Pokud je potřeba nastavit více než šestnáct pravidel pro NAT, je možné vložit do Startup Script (položka *Startup Script* na stránce *Scripts* v sekci *Configuration*) následující skript (IPv4 NAT):

```
iptables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT
--to-destination [IPADDR]:[PORT_PRIVATE]
```

kde je třeba místo [PORT_PUBLIC] a [PORT_PRIVATE] vložit konkrétní čísla portů a místo [IPADDR] vložit IP adresu. Pro IPv6 NAT lze použít ekvivalentní příkaz `ip6tables` se stejnými parametry:

```
ip6tables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT
--to-destination [IP6ADDR]:[PORT_PRIVATE]
```

Povolením následujících voleb a zadáním čísla portu je umožněn vzdálený přístup k routeru z internetu.

Položka	Popis
Enable remote HTTP access on port	Nastavuje **pouze přesměrování** z HTTP na HTTPS (ve výchozí konfiguraci zakázáno).
Enable remote HTTPS access on port	Umožňuje konfiguraci routeru přes zabezpečený webový protokol *HTTPS* (ve výchozí konfiguraci zakázáno).
Enable remote SSH access on port	Umožňuje přístup přes *SSH* (ve výchozí konfiguraci zakázáno).
Enable remote SNMP access on port	Umožňuje dotazovat se SNMP agenta (ve výchozí konfiguraci zakázáno).

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Masquerade outgoing packets	Tato volba (alternativní název pro systém překladu adres NAT) zapíná systém překladu adres NAT.

Pozor! *Enable remote HTTP access on port* aktivuje **pouze přesměrování z protokolou HTTP na protokol HTTPS**. Router nepodporuje pro přístup ke konfiguraci nezabezpečený protokol HTTP. Pro přístup k webové konfiguraci je tedy nutné vždy povolit *Enable remote HTTPS access on port*. Pro přístup k webové konfiguraci z internetu nikdy nepovolujte pouze položku HTTP (konfigurace routeru by pak nebyla z internetu přístupná), ale buď pouze HTTPS, nebo HTTPS a přesměrování z HTTP.

Následující položky slouží k nastavení routování veškeré příchozí komunikace z mobilního spojení (Mobile WAN) na počítač s definovanou IP adresou.

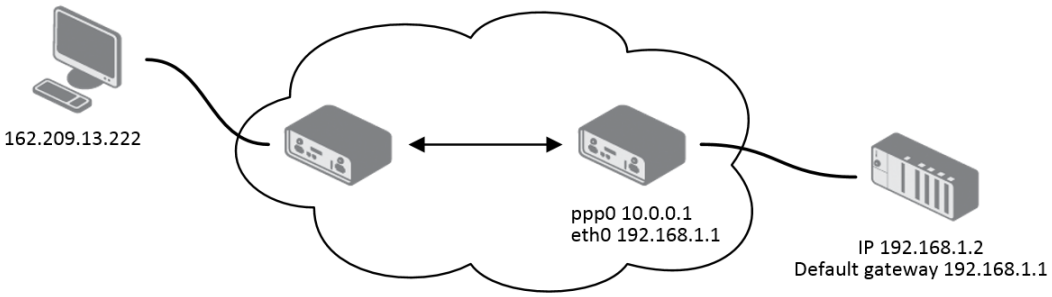
Položka	Popis
Send all remaining incoming packets to default server	Zaškrtnutím této položky a nastavením položky *Default Server IPv4/IPv6 Address* lze uvést router do režimu, kdy bude směrovat veškerou příchozí komunikaci z mobilního spojení na počítač s definovanou IP adresou.
Default Server IPv4 Address	Pouze na stránce *IPv4 NAT Configuration*. Výchozí IPv4 adresa pro směrování komunikace.
Default Server IPv6 Address	Pouze na stránce *IPv6 NAT Configuration*. Výchozí IPv6 adresa pro směrování komunikace.

Tabulka 37: Konfigurace jednotného přeposílání

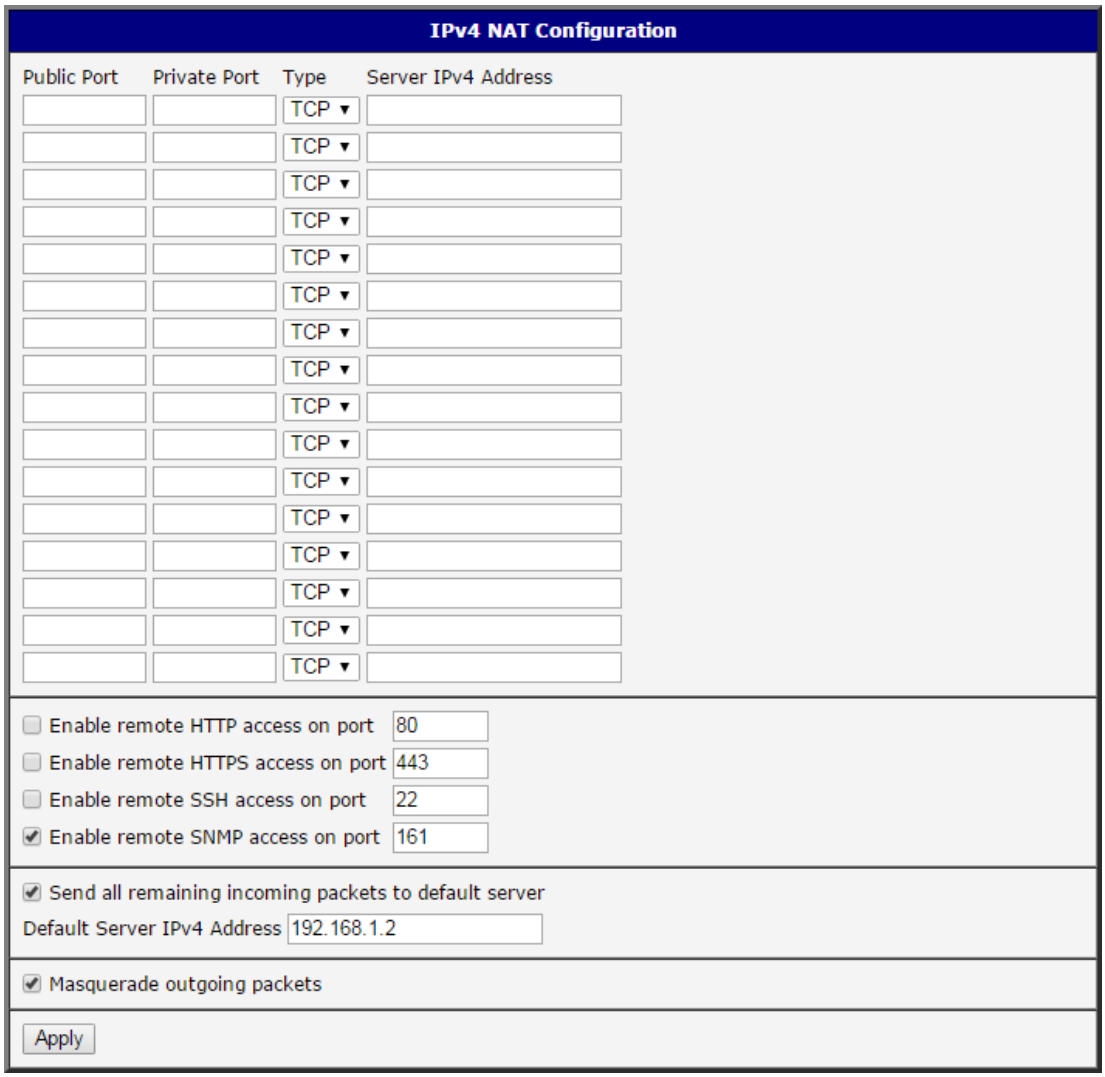
4.9.1 Příklady NAT konfigurace

Příklad 1: IPv4 NAT konfigurace s jedním připojeným zařízením

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.



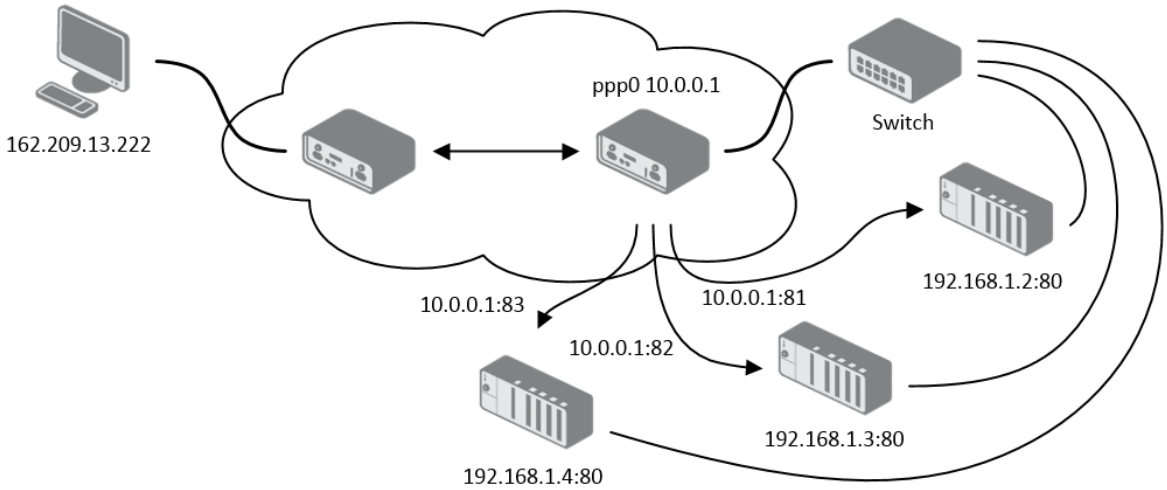
Obrázek 34: Topologie konfigurace NAT pro příklad 1



Obrázek 35: NAT konfigurace pro příklad 1

Příklad 2: IPv4 NAT konfigurace s více zařízeními na routeru

Při této konfiguraci definují adresy *Server IP Address* zařízení zapojená 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 který chceme přistoupit. Při požadavku na port 80 se zkoumají jednotlivé vnější porty (Public Port). Protože tam tento port není definován a není nastavena ani *Default Server IP address*, žádost na port 80 se provede s neúspěšným výsledkem. Kdyby byl proveden požadavek na port 443 (HTTPS) a byla by zaškrtnuta volba *Enable remote HTTPS access*, po projití veřejných portů (kde tento port není definován) by se otevřelo webové rozhraní routeru.



Obrázek 36: Topologie konfigurace NAT pro příklad 2

IPv4 NAT Configuration

Public Port	Private Port	Type	Server IPv4 Address
81	80	TCP	192.168.1.2
82	80	TCP	192.168.1.3
83	80	TCP	192.168.1.4
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

- [ ] Enable remote HTTP access on port 80
- [ ] Enable remote HTTPS access on port 443
- [ ] Enable remote SSH access on port 22
- [x] Enable remote SNMP access on port 161

- [ ] Send all remaining incoming packets to default server

Default Server IPv4 Address

- [x] Masquerade outgoing packets

Apply

Obrázek 37: NAT konfigurace pro příklad 2

4.10 OpenVPN tunel

OpenVPN tunel umožňuje zabezpečené (šifrované) propojení dvou sítí LAN do jedné, která se tváří jako homogenní. Router umožňuje vytvořit až čtyři OpenVPN tunely, jejich konfiguraci lze vyvolat volbou položky *OpenVPN* v menu. V menu se pod touto položkou rozbalí čtyři další konfigurační stránky: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. Souběh protokolů IPv4 a IPv6 je podporován (dual stack).

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. • **UDPv6** – OpenVPN bude komunikovat protokolem UDP přes IPv6. • **TCPv6 server** – OpenVPN bude komunikovat protokolem TCP přes IPv6 v režimu server. • **TCPv6 client** – OpenVPN bude komunikovat protokolem TCP přes IPv6 v režimu klient.
UDP/TCP port	Port příslušného protokolu.
Remote IP Address	IPv4, IPv6 adresa nebo doménové jméno protější strany tunelu.
Remote Subnet	IPv4 adresa sítě za protější stranou tunelu.
Remote Subnet Mask	IPv4 maska sítě za protější stranou tunelu.
Redirect Gateway	Přidá (přepíše) výchozí bránu (deafult gateway). Všechny pakety jsou potom posílány na tuto bránu tunelem, pokud v sobě nemají specifikovanou jinou výchozí bránu.
Local Interface IP Address	Definuje IPv4 adresu lokálního rozhraní. **Pro zachování správného směrování doporučujeme vyplnit jakoukoli IPv4 adresu z lokálního rozsahu i když je používán pouze IPv6 tunel.**
Remote Interface IP Address	Definuje IPv4 adresu rozhraní protější strany tunelu. **Pro zachování správného směrování doporučujeme vyplnit jakoukoli IPv4 adresu z lokálního rozsahu i když je používán pouze IPv6 tunel.**
Remote IPv6 Subnet	IPv6 adresa sítě za protější stranou tunelu. Ekvivalent položky *Remote Subnet* v IPv4 sekci.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Remote IPv6 Subnet Prefix Length	IPv6 prefix sítě za protější stranou tunelu. Ekvivalent položky *Remote Subnet Mask* v IPv4 sekci.
Local Interface IPv6 Address	IPv6 adresa lokálního rozhraní.
Remote Interface IPv6 Address	IPv6 adresa 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. Parametr je možné nastavit pouze při ověřování username/password nebo při použití certifikátu X.509. Po této časové periodě router mění šifrování tunelu, aby se zajistila trvalá bezpečnost.
Max Fragment Size	Definuje 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. • **applied** – NAT pravidla jsou aplikována na OpenVPN tunel.

Pokračování na následující straně

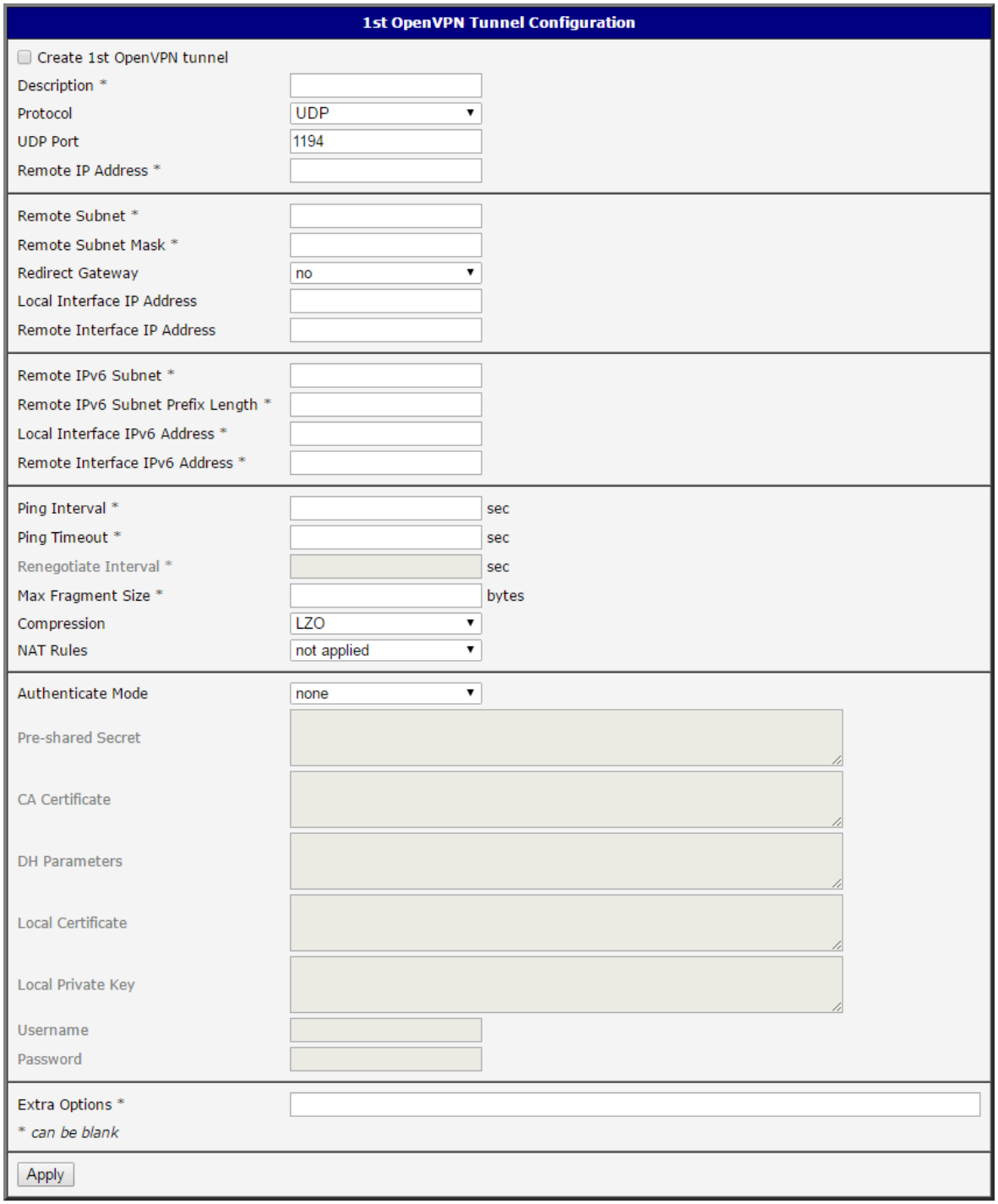
Pokračování z předchozí strany

Položka	Popis
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*. • **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* lze definovat doplňující parametry OpenVPN tunelu jako například DHCP options apod. Parametry jsou uvozeny dvěma pomlčkami. Pro možné parametry viz nápověda – v routeru přes SSH příkazem `openvpnd --help`.

Tabulka 38: Konfigurace OpenVPN tunelu

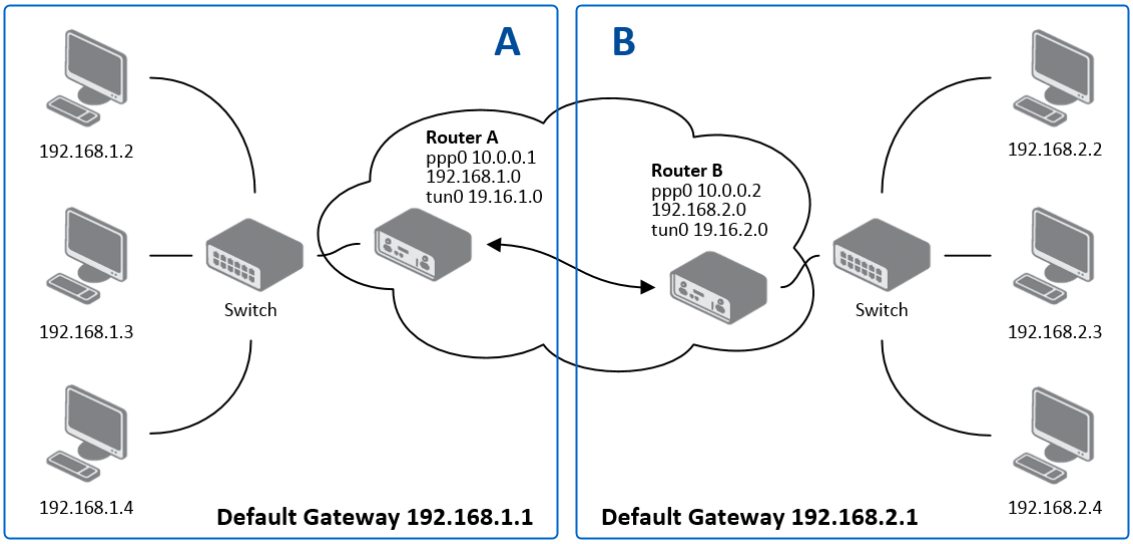
Podmínkou pro sestavení tunelu je, aby aktuálně nastavená cesta do WAN byla aktivní (v případě mobilního spojení musí dojít k jeho úspěšnému navázání) a to i v případě, že samotný tunel nevede do WAN.

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



Obrázek 38: Konfigurace OpenVPN tunelu

4.10.1 Příklad konfigurace OpenVPN tunelu v IPv4 síti



Obrázek 39: 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 39: Příklad konfigurace OpenVPN tunelu

Příklady nastavení všech různých možností konfigurací a autentizací OpenVPN lze nalézt v aplikační příručce *OpenVPN tunel* [5].

4.11 IPsec tunel

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 menu se pod touto položkou rozbalí čtyři další konfigurační stránky: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. Jsou podporovány IPv4 a IPv6 tunely (dual stack). Je možné provozovat IPv6 provoz uvnitř IPv4 tunelu a naopak.

Chcete-li šifrovat data mezi místní a vzdálenou podsítí, zadejte příslušné hodnoty do kolonky *Subnet* na obou routerech. Chcete-li zašifrovat tok dat mezi routery, ponechte *Local Subnet* a *Remote Subnet* pole prázdné.

Pokud zadáte informaci o protokolu a portu v poli *Local Protocol/Port*, router zapouzdří pouze pakety odpovídající nastavení.

Položka	Popis
Description	Název (popis) tunelu.
Host IP Mode	• **IPv4** – Router komunikuje s protější stranou tunelu pomocí IPv4 protokolu. • **IPv6** – Router komunikuje s protější stranou tunelu pomocí IPv6 protokolu.
Remote IP Address	IPv4, IPv6 adresa nebo doménové jméno protější strany tunelu, na základě volby *Host IP Mode* výše.
Remote ID	Identifikátor (ID) protější strany tunelu. Skládá se ze dvou částí: *hostname* a *domain-name* (více informací pod tabulkou).
Tunnel IP Mode	• **IPv4** – Uvnitř tunelu probíhá IPv4 komunikace. • **IPv6** – Uvnitř tunelu probíhá IPv6 komunikace.
First Remote Subnet	IPv4 nebo IPv6 adresa sítě za protější stranou tunelu, na základě volby *Tunel IP Mode* výše.
First Remote Subnet Mask/Prefix	IPv4 maska sítě za protější stranou tunelu, nebo IPv6 prefix (číslo od 0 do 128).
Second Remote Subnet	IPv4 nebo IPv6 adresa druhé sítě za protější stranou tunelu, na základě volby *Tunel IP Mode* výše. Pouze pro *IKE Protocol* = IKEv2.
Second Remote Subnet Mask/Prefix	IPv4 maska druhé sítě za protější stranou tunelu nebo IPv6 prefix (číslo od 0 do 128). Pouze pro *IKE Protocol* = IKEv2.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Remote Protocol/Port	Protokol/Port protější strany tunelu. Zadávejte ve tvaru *číslo protokolu*/*číslo portu*, např. 17/1701 pro UDP (protokol 17) a port 1701. Je možné zadat pouze číslo protokolu, nicméně výše uvedený formát je preferován.
Local ID	Identifikátor (ID) lokální strany tunelu. Skládá ze dvou částí: *hostname* a *domain-name* (více informací pod tabulkou).
First Local Subnet	IPv4 nebo IPv6 adresa lokální sítě, na základě volby *Tunel IP Mode* výše.
First Local Subnet Mask/Prefix	IPv4 maska lokální sítě, nebo IPv6 prefix (číslo od 0 do 128).
Second Local Subnet	IPv4 nebo IPv6 adresa druhé lokální sítě, na základě volby *Tunel IP Mode* výše. Pouze pro *IKE Protocol* = IKEv2.
Second Local Subnet Mask/Prefix	IPv4 maska druhé lokální sítě nebo IPv6 prefix (číslo od 0 do 128). Pouze pro *IKE Protocol* = IKEv2.
Local Protocol/Port	Protokol/Port lokální sítě. Zadávejte ve tvaru *číslo protokolu*/*číslo portu*, např. 17/1701 pro UDP (protokol 17) a port 1701. Je možné zadat pouze číslo protokolu, nicméně výše uvedený formát je preferován.
Encapsulation Mode	Mód IPsecu (dle způsobu zapouzdření) – zvolit lze *tunnel* (zapouzdřen celý IP datagram) nebo *transport* (pouze IP hlavička).
Force NAT Traversal	Umožňuje vynutit NAT traversal (UDP zapouzdření ESP paketů). (*Enabled*).
IKE Protocol	Definuje verzi protokolu IKE (IKEv1/IKEv2, IKEv1 nebo IKEv2).
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. **Vzhledem ke snížené bezpečnosti doporučujeme *aggressive* mód nepoužívat!**
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.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
IKE Hash	Hashovací algoritmus – MD5, SHA1, SHA256, SHA384 nebo SHA512.
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, SHA1, SHA256, SHA384 nebo SHA512.
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.
Debug	Množství hlášek vypisovaných do System Logu. Silent (výchozí) je vypnuto, audit, control, control-more, raw, private (vypisuje nejvíce informací včetně tajných klíčů). Pro více podorbností viz dokumentaci strongSwan.

Tabulka 40: Konfigurace IPsec tunelu

Nepřehlédněte:

- Pokud nejsou vyplněny parametry *Remote Subnet* a *Local Subnet*, pouze pakety mezi lokální a vzdálenou IP adresou jsou zapouzdřeny, takže pouze komunikace mezi oběma routery je šifrována.
- Pokud jsou vyplněny parametry *Remote Protocol/Port* a *Local Protocol/Port*, pouze pakety odpovídající vyplněným hodnotám jsou zapouzdřeny.

Tuto proceduru je možné využít pro generování certifikátů a klíčů bez hesla (password phrase):

```
******************** certification authority ************************
openssl rand -out private/.rand 1024
openssl genrsa -des3 -out private/ca.key 2048
openssl req -new -key private/ca.key -out tmp/myrootca.req
openssl x509 -req -days 7305 -sha1 -extensions v3_ca -signkey
private/ca.key -in tmp/myrootca.req -out ca.crt

******************** server cert ************************************
openssl genrsa -out private/server.key 2048
openssl req -new -key private/server.key -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt

******************** client cert ************************************
openssl genrsa -out private/client.key 2048
openssl req -new -key private/client.key -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt
```

Níže je vypsána procedura pro generování certifikátů a klíčů s heslem "router" (password phrase), certifikační autorita zůstává nezměněna:

```
******************** server cert ************************************
openssl genrsa -des3 -passout pass:router -out private/server.pem 2048
openssl req -new -key private/server.pem -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt

******************** client cert ************************************
openssl genrsa -des3 -passout pass:router -out private/client.pem 2048
openssl req -new -key private/client.pem -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt
```

Podporovány jsou následující typy identifikátorů (ID) obou stran tunelů (tj. položky *Remote ID* a *Local ID*):

- IP adresa (např. 192.168.1.1)
- DN (např. C=CZ,O=CompanyName,OU=TP,CN=A)

- FQDN (např. @director.companyname.cz) – **před FQDN vždy musí být znak @**
- User FQDN (např. director@companyname.cz)

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

1st IPsec Tunnel Configuration

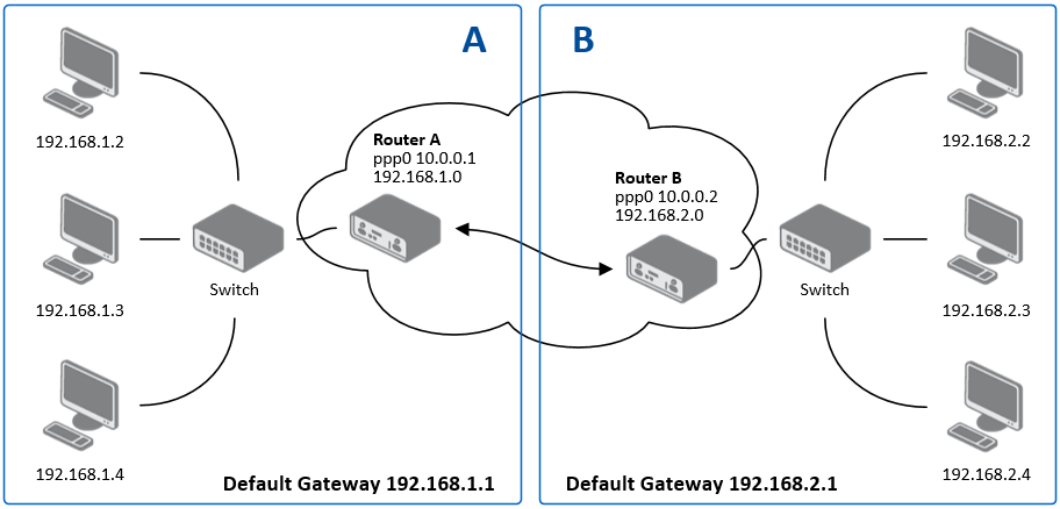
☐ Create 1st IPsec tunnel	
Description *	
Host IP Mode	IPv4
Remote IP Address *	
Tunnel IP Mode	IPv4
Remote ID *	
First Remote Subnet *	
First Remote Subnet Mask *	
Second Remote Subnet *	
Second Remote Subnet Mask *	
Remote Protocol/Port *	
Local ID *	
First Local Subnet *	
First Local Subnet Mask *	
Second Local Subnet *	
Second Local Subnet Mask *	
Local Protocol/Port *	
Encapsulation Mode	tunnel
Force NAT Traversal	no
IKE Protocol	IKEv1
IKE Mode	main
IKE Algorithm	auto
IKE Encryption	3DES
IKE Hash	MD5
IKE DH Group	2
ESP Algorithm	auto
ESP Encryption	DES
ESP Hash	MD5
PFS	disabled
PFS DH Group	2
Key Lifetime	3600 sec
IKE Lifetime	3600 sec
Rekey Margin	540 sec
Rekey Fuzz	100 %
DPD Delay *	sec
DPD Timeout *	sec
Authenticate Mode	pre-shared key
Pre-shared Key	
CA Certificate	
Remote Certificate	
Local Certificate	
Local Private Key	
Local Passphrase *	
Debug	control
** can be blank*	

Obrázek 40: Konfigurace IPsec tunelu

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*.

4.11.1 Příklad konfigurace IPSec tunelu v IPv4 síti



Obrázek 41: Topologie příkladu konfigurace IPsec tunelu

Konfigurace IPSec tunelu:

Konfigurace	A	B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
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 41: Příklad konfigurace IPsec tunelu

Příklady nastavení různých možností konfigurací a autentizací IPsec tunelu lze nalézt v aplikační příručce *IPsec tunel* [6].

4.12 GRE tunel

GRE je nešifrovaný protokol. GRE přes IPv6 není podporováno.

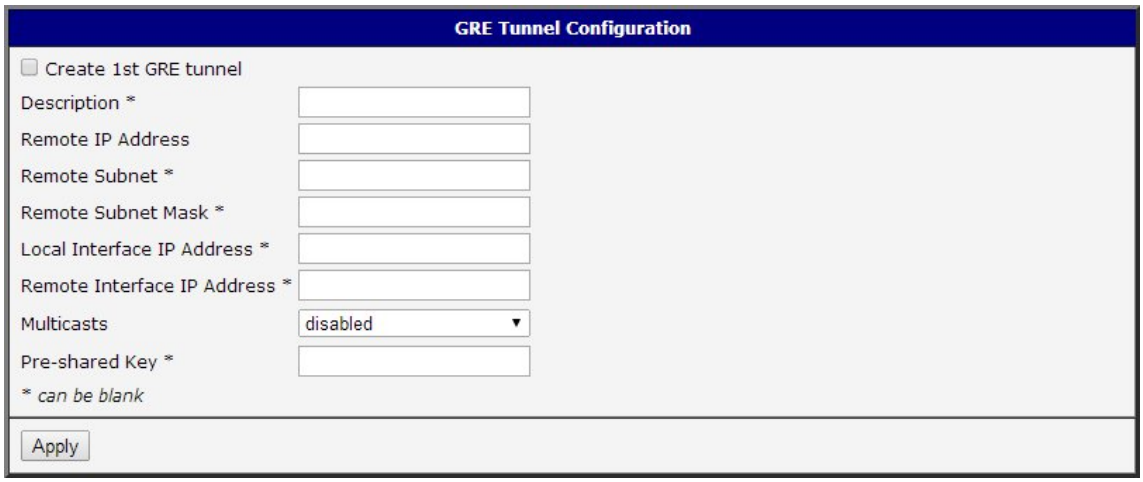
GRE tunel vytváří propojení dvou sítí LAN do jedné, která se tváří jako homogenní. Router umožňuje vytvořit až čtyři GRE tunely, jejichž konfiguraci je možné vyvolat volbou položky *GRE* v menu. V menu se pod touto položkou rozbalí čtyři další konfigurační stránky: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*.

Položka	Popis
Description	Název tunelu.
Remote IP Address	IP adresa protější strany tunelu.
Remote Subnet	Adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Local Interface IP Address	Interní IP adresa lokální strany tunelu.
Remote Interface IP Address	Interní IP adresa protější strany tunelu.
Multicasts	Povoluje, resp. zakazuje multicast: • **disabled** – Posílání multicastu je zakázáno. • **enabled** – Posílání multicastu je povoleno.
Pre-shared Key	Volitelná položka, která definuje 32 bit sdílený klíč v číselném formátu, 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 42: Konfigurace GRE tunelu

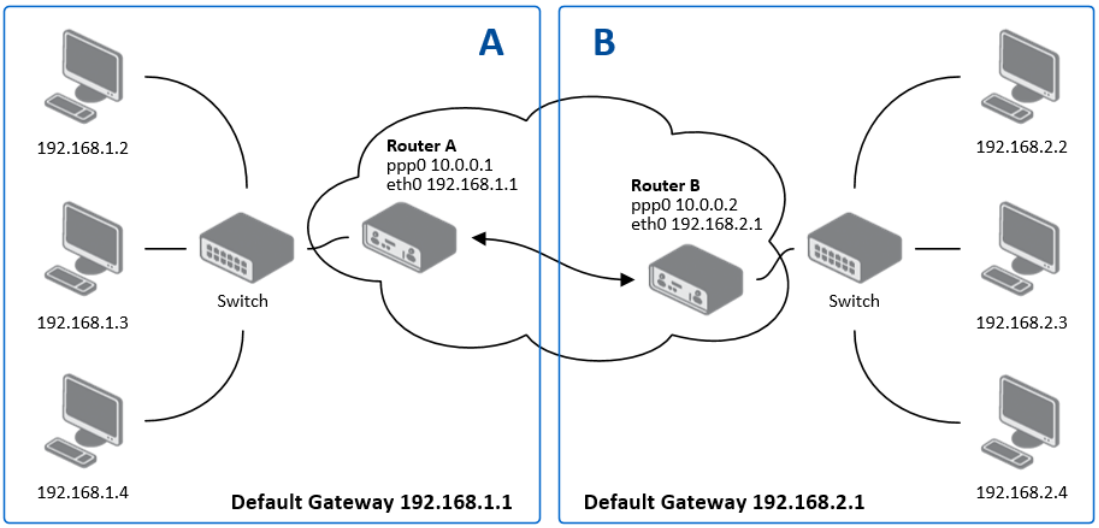
Pozor, GRE tunel neprojde přes překlad adres NAT.

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



Obrázek 42: GRE Tunnel Configuration

4.12.1 Příklad konfigurace GRE tunelu



Obrázek 43: 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 43: Příklad konfigurace GRE tunelu

Příklady nastavení různých možností konfigurací GRE tunelu lze nalézt v aplikační příručce *GRE tunel* [7].

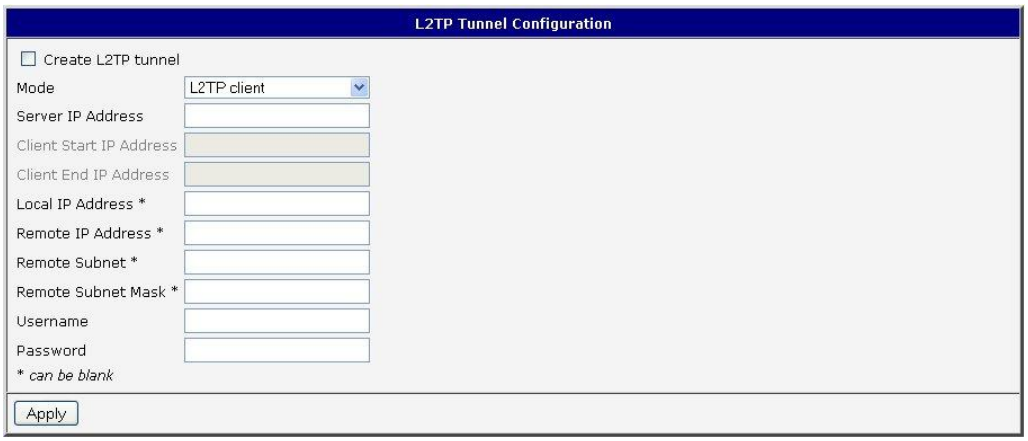
4.13 L2TP tunel

L2TP je nešifrovaný protokol. L2TP přes IPv6 není podporováno.

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*.

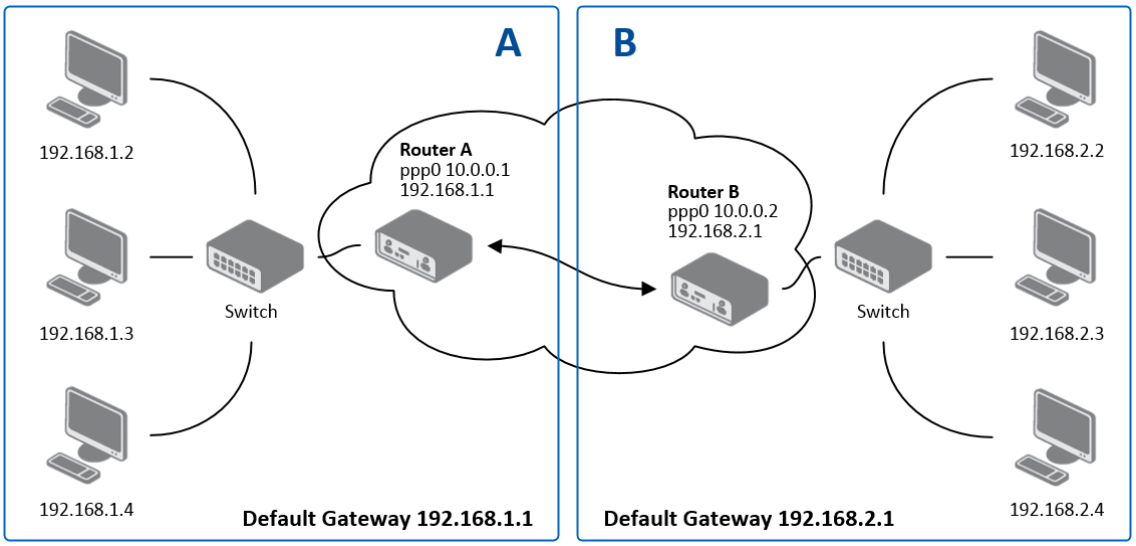
Položka	Popis
Mode	Mód L2TP tunelu na straně routeru: • **L2TP server** – Lze definovat počáteční a konečnou IP adresu rozsahu nabízenou serverem. • **L2TP client** – Lze definovat IP adresu server.
Server IP Address	Adresa serveru.
Client Start IP Address	První IP adresa v rozsahu nabízeném serverem 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 44: Konfigurace L2TP tunelu



Obrázek 44: Konfigurace L2TP tunelu

4.13.1 Příklad konfigurace L2TP tunelu



Obrázek 45: 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	192.168.2.5	—
Client End IP Address	192.168.2.254	—
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	username	username
Password	password	password

Tabulka 45: Příklad konfigurace L2TP tunelu

4.14 PPTP tunel

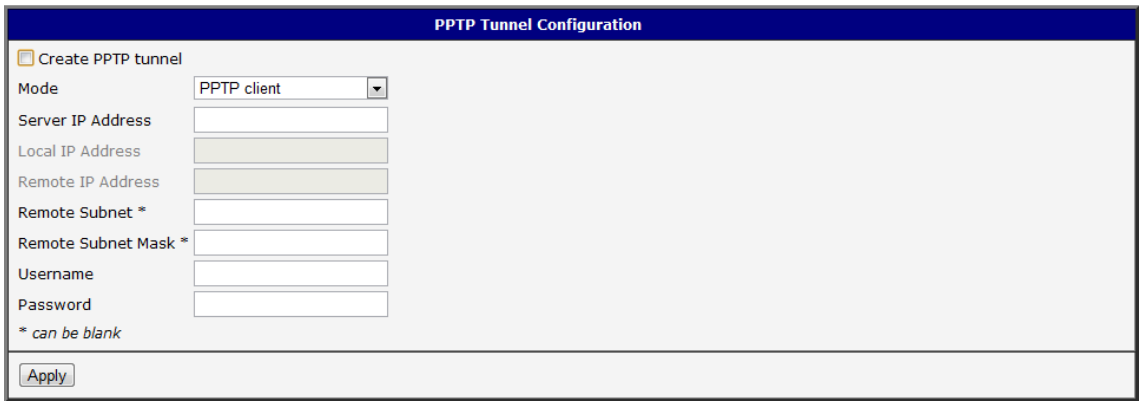
PPTP je nešifrovaný protokol. PPTP přes IPv6 není podporováno.

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 46: Konfigurace PPTP tunelu

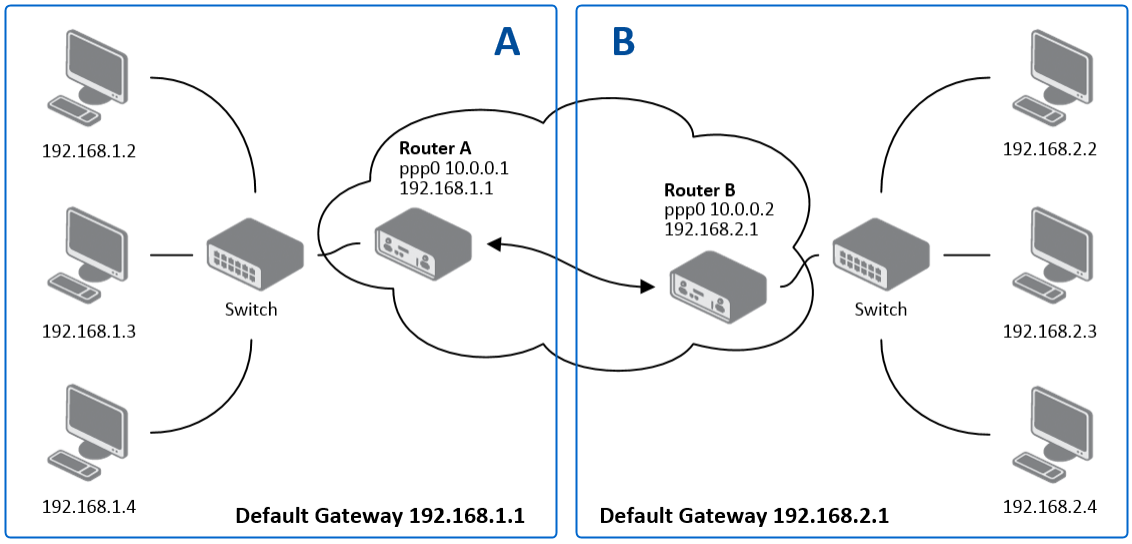
Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 46: Konfigurace PPTP tunelu

Firmware routeru podporuje *PPTP passthrough*, což znamená, že je možné vytvářet tunel „přes“ router.

4.14.1 Příklad konfigurace PPTP tunelu



Obrázek 47: 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	192.168.2.1	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Tabulka 47: Příklad konfigurace PPTP tunelu

4.15 Services

4.15.1 DynDNS

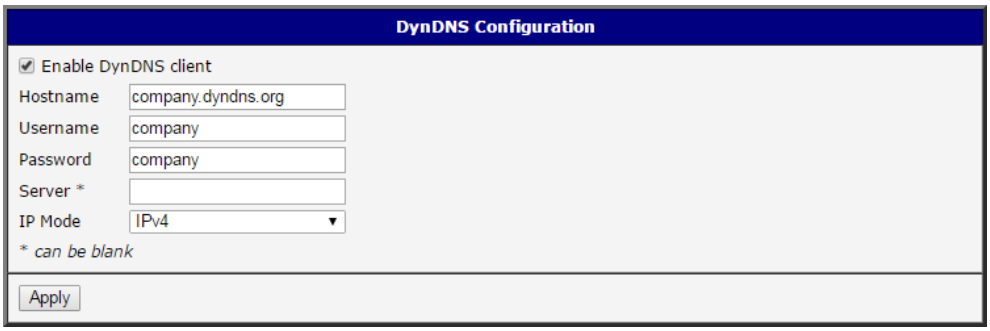
Díky službě DynDNS je možné k routeru vzdáleně přistupovat pomocí vlastního doménového jména, jednoduchého k zapamatování narozdíl od IP adresy. Tento klient monitoruje IP adresu routeru a kdykoli se IP adresa změní, aktualizuje záznam u služby DynDNS. Aby služba DynDNS správně fungovala, je nutné aby měl router veřejnou IP adresu (statickou nebo dynamickou) a je nutné mít aktivní účet na www.dyndns.org (Remote Access service). Je možné využít i jiné služby pro Dynamický DNS záznam – viz tabulka níže, položka Server.

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

Položka	Popis
Hostname	Doména třetího řádu registrovaná 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. Možné další servery: www.spdns.de, www.dnsdynamic.org, www.noip.com. Zůstane-li nevyplněno, je použit výchozí server members.dyndns.org.
IP Mode	Výběr použité verze IP protokolu: • **IPv4** – Bude použit pouze IPv4 protokol (výchozí). • **IPv6** – Bude použit pouze IPv6 protokol. • **IPv4/IPv6** – Souběh IPv4 a IPv6 protokolů – dual stack.

Tabulka 48: Konfigurace DynDNS

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



Obrázek 48: Příklad nastavení DynDNS

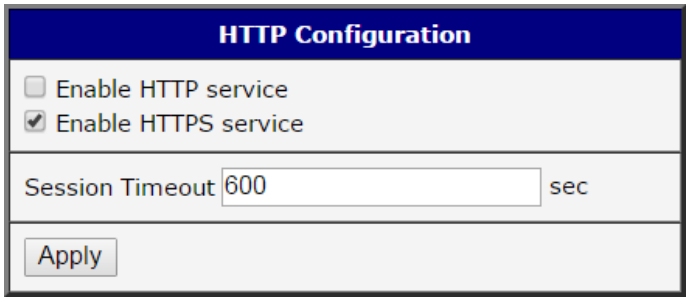
Pro vzdálený přístup ke konfiguraci routeru je nutné tento přístup povolit ještě v konfiguraci NAT (ve spodní části formuláře), viz kap. 4.9.

4.15.2 HTTP

HTTP protokol (Hypertext Transfer Protocol) je internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. Tento protokol je využit pro přístup k webovému serveru, který slouží k uživatelské konfiguraci routeru. Doporučené je ovšem použití nadstavby tohoto protokolu, protokolu HTTPS, který umožňuje zabezpečit přenášená data pomocí šifrování. Konfigurační okno HTTP a HTTPS služby je možno otevřít volbou položky *HTTP*, která se nachází ve složce menu *Services*. Ve výchozím stavu je protokol HTTPS povolen a protokol HTTP zakázán. Pokud je v tomto výchozím nastavení iniciována komunikace s využitím protokolu HTTP, je automaticky přesměrována na zabezpečenou formu komunikace s využitím HTTPS protokolu.

Položka	Popis
Enable HTTP service	Povolení služby HTTP.
Enable HTTPS service	Povolení služby HTTPS.
Session Timeout	Maximální doba nečinnosti, po kterém je spojení ukončeno.

Tabulka 49: Parametry konfigurace HTTP a HTTPS služeb



Obrázek 49: Konfigurace HTTP a HTTPS služeb

4.15.3 NTP

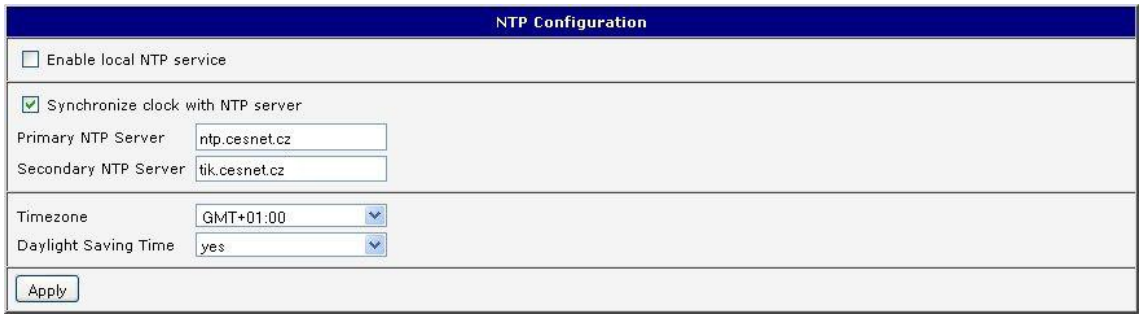
Konfiguraci NTP klienta lze vyvolat volbou položky *NTP* v menu. NTP (Network Time Protocol) umožňuje pravidelně nastavovat přesný čas do routeru ze serverů, které přesný čas na síti poskytují. Jsou podporovány také IPv6 NTP servery.

- 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	IPv4 adresa, IPv6 adresa nebo doménové jméno primárního NTP serveru.
Secondary NTP Server Address	IPv4 adresa, IPv6 adresa nebo doménové jméno 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 50: Konfigurace NTP

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



Obrázek 50: Příklad nastavení NTP

4.15.4 SNMP

Vyvoláním položky *SNMP* je možná konfigurace SNMP agenta v1/v2 nebo v3, který zasílá informace o routeru, případně o stavu I/O vstupů routeru.

SNMP (Simple Network Managment Protocol) poskytuje stavové informace o prvcích sítě, jakými jsou routery nebo koncové počítače. v1, v2 a v3 jsou různé verze protokolu SNMP. Verze v3 zajišťuje šifrovanou zabezpečovanou komunikaci, ovšem notifikační zprávy (např. o událostech – Trap) šifrovány nejsou. Pro povolení služby SNMP zatrhněte položku *Enable SNMP agent*. Posílání notifikačních zpráv na IPv6 adresu je podporováno.

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 51: 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.

U SNMP v1/v2 je možné nadefinnovat různé heslo pro čtení (*Read*) a zápis i čtení (*Write*), jedná se o dvě různé komunity. U SNMPv3 je možné nadefinovat dva SNMP uživatele, kdy jeden má obdobně právo pouze ke čtení (*Read*) a druhý ke čtení i k zápisu (*Write*). Položky v následující tabulce lze nastavit pro každého uživatele zvlášť. Nejedná se o uživatele webového rozhraní routeru, ale pouze o SNMP přístup.

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 52: Konfigurace SNMPv3

Dále je možné zaškrtnutím volby *Enable I/O extension* sledovat stav I/O vstupů na routeru.

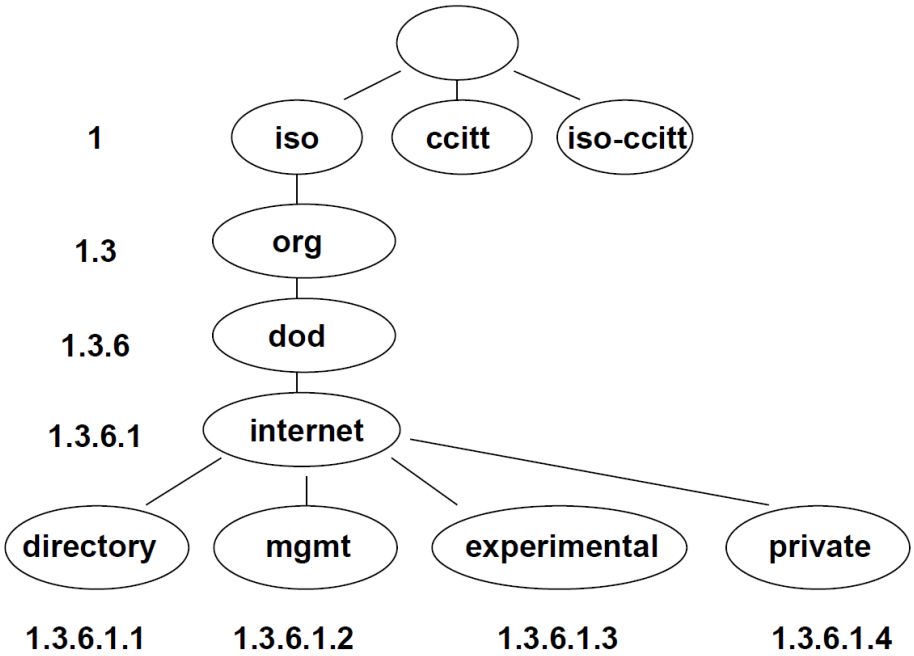
Volba položky *Enable M-BUS extension* a zadání paramterů *Baudrate*, *Parity* a *Stop Bits* umožňuje sledovat stav měřících zařízení připojených přes rozhraní MBUS. Momentálně není dostupný rozšiřující port MBUS, ale je možné použít externí RS232/MBUS konverter.

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	IPv4 nebo IPv6 adresa.
Period	Interval odesílání statistických informací (v minutách)

Tabulka 53: Konfigurace SNMP (R-SeeNet)

OID (Object Identifier) je označení pro číselný identifikátor, díky kterému je každá hodnota v SNMP jednoznačně identifikována. OID je tvořeno posloupností čísel oddělených tečkou. Tvar každého OID je dán hodnotou identifikátoru nadřazeného prvku, jež je doplněna o tečku a aktuální číslo. Je tedy patrné, že vzniká stromová struktura. Na následujícím obrázku je znázorněna základní stromová struktura, na jejímž základě jednotlivá OID vznikají.



Obrázek 51: Základní struktura OID

SNMP hodnoty, které jsou specifické pro firmu Conel, tvoří strom, jenž začíná hodnotou OID = .1.3.6.1.4.1.30140, což lze slovně interpretovat jako:

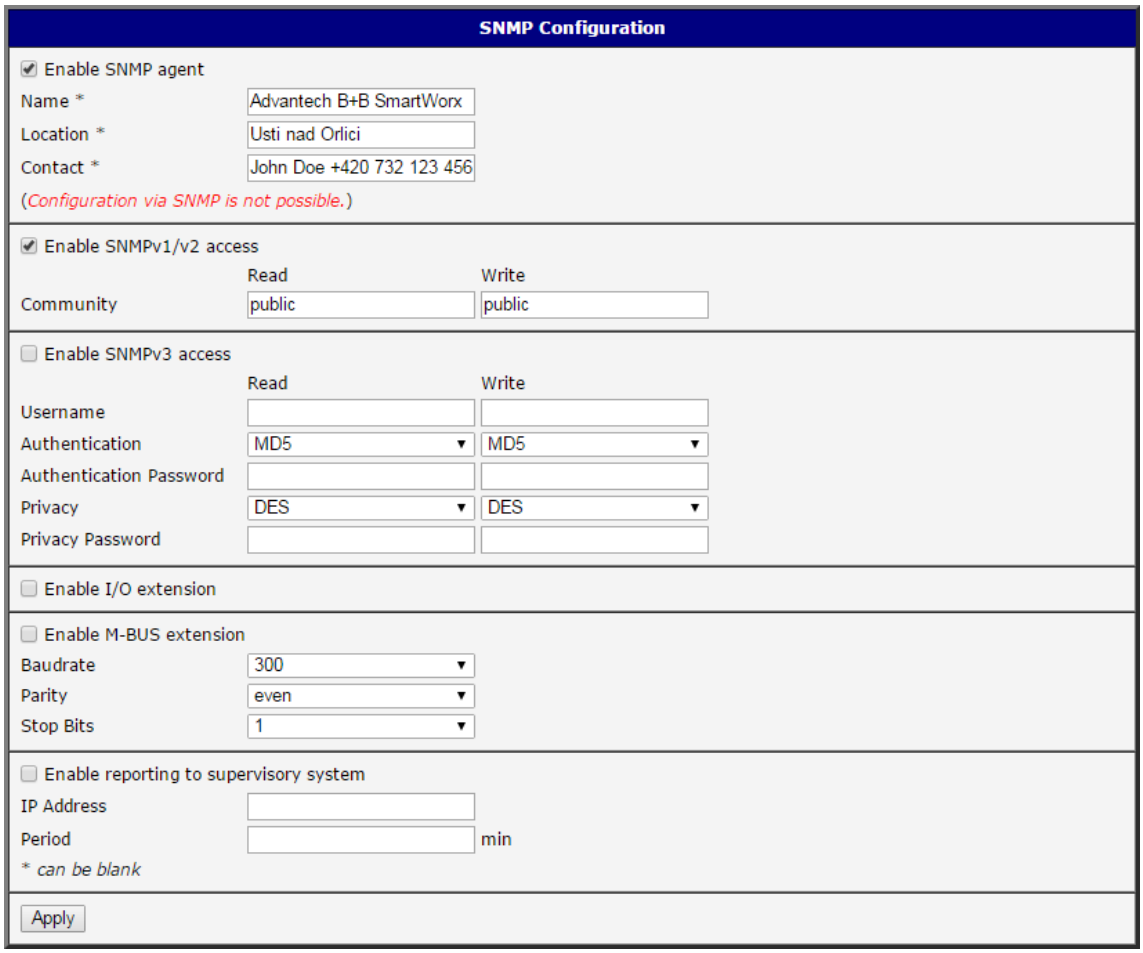
iso.org.dod.internet.private.enterprises.conel

To znamená, že je možné z routeru vyčíst např. informaci o jeho vnitřní teplotě (OID hodnota 1.3.6.1.4.1.248.40.1.3.3) nebo o napájecím napětí (OID 1.3.6.1.4.1.248.40.1.3.4). Pro binární vstupy a výstup je pak využit následující rozsah OID hodnot:

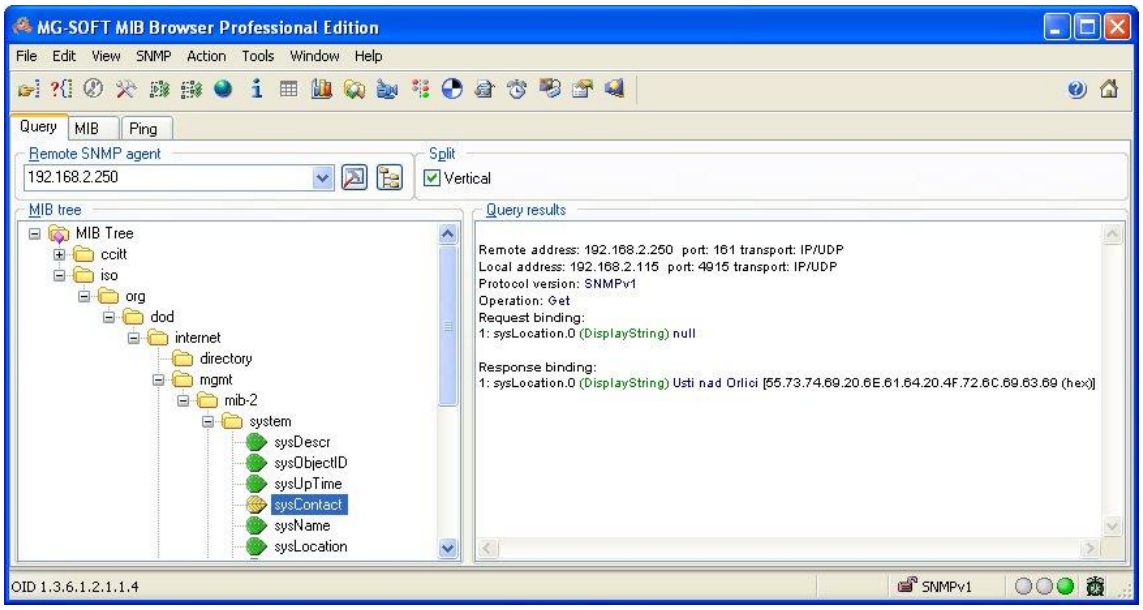
OID	Význam
.1.3.6.1.4.1.30140.2.3.1.0	Binární vstup BIN0 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binární výstup OUT0 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.3.3.0	Binární vstup BIN1 (hodnoty 0,1)

Tabulka 54: Vnitřní proměnné pro binární vstupy a výstup

Seznam dostupných a podporovaných OID a další podrobnosti naleznete v aplikační příručce *SNMP Object Identifier* [8].



Obrázek 52: Příklad SNMP konfigurace



Obrázek 53: 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

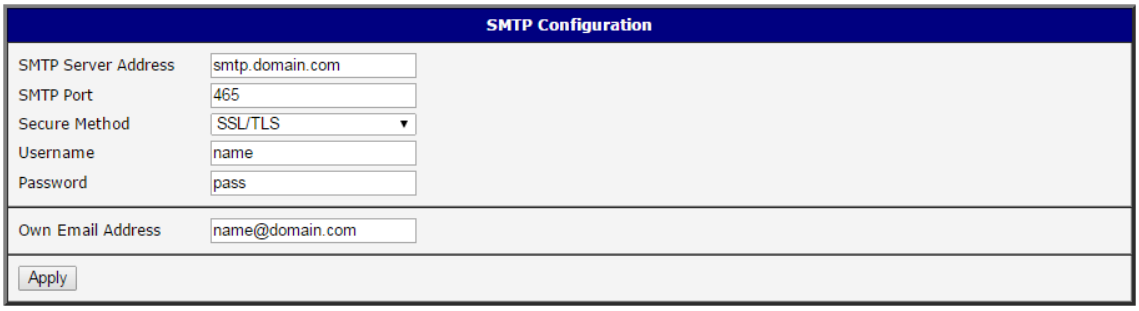
4.15.5 SMTP

Vyvoláním položky *SMTP* je možná konfigurace SMTP (Simple Mail Transfer Protocol) klienta, pomocí kterého se nastavuje odesílání e-mailů. Je možné použít i IPv6 e-mailové servery.

Položka	Popis
SMTP Server Address	IPv4 adresa, IPv6 adresa nebo doménové jméno SMTP serveru.
SMTP Port	Port, na němž SMTP server naslouchá
Secure Method	Metoda zabezpečení – žádná, SSL/TLS nebo STARTTLS. SMTP server musí danou metodu zabezpečení podporovat.
Username	Uživatelské jméno k e-mailovému účtu.
Password	Heslo k emailovému účtu. Může obsahovat speciální znaky: * + , - . / : = ? ! # % [ ] _ { } ~ a nemůže obsahovat tyto speciální znaky: “ $ & ’ ( ) ; < >
Own Email Address	Email odesílatele.

Tabulka 55: Konfigurace SMTP klienta

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



Obrázek 54: Příklad konfigurace SMTP klienta

Samotné emaily lze posílat ze Startup skriptu (položka *Scripts – Startup Script* v sekci *Configuration*) nebo v SSH rozraní pomocí příkazu *email* s následujícími parametry:

- -t E-mailová adresa příjemce
- -s Předmět zprávy (předmět zprávy musí být ohraničen uvozovkami)
- -m Zpráva (zpráva musí být ohraničena uvozovkami)
- -a Soubor přílohy
- -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 john@doe.com -s "System Log" -m "Attached" -a /var/log/messages
```

Tento příkaz odešle e-mail na adresu jogn@doe.com s předmětem zprávy *"System Log"*, tělem zprávy *"Attached"* a s přílohou soubor messages se zprávami System Logu z routeru z adresáře /var/log/.

4.15.6 SMS

SMS konfigurace se vyvolá volbou položky *SMS* v 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.
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 binárního vstupu routeru.

Tabulka 56: Konfigurace posílání SMS

Po zaškrtnutí volby *Enable remote control via SMS* je možné ovládat router pomocí SMS zpráv. 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 následně smažou.

Položka	Popis
Phone Number 1	Definuje první telefonní číslo, ze kterého bude možné ovládat router pomocí SMS zpráv.
Phone Number 2	Definuje druhé telefonní číslo, ze kterého bude možné ovládat router pomocí SMS zpráv.
Phone Number 3	Definuje třetí telefonní číslo, ze kterého bude možné ovládat router pomocí SMS zpráv.

Tabulka 57: Ovládání pomocí SMS zpráv

- Pokud není vyplněno žádné telefonní číslo, je možné pouze znovu spustit 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 kartu
go online sim 2	Přepnutí na druhou SIM kartu
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 profile std	Nastavení standardního profilu
set profile alt1	Nastavení alternativního profilu 1
set profile alt2	Nastavení alternativního profilu 2
set profile alt3	Nastavení alternativního profilu 3
reboot	Reboot routeru
get ip	Odešle odpověď s IP adresou SIM karty

Tabulka 58: Význam ovládacích SMS

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

Položka	Význam
Baudrate	Komunikační rychlost na sériovém rozhraní.

Tabulka 59: Posílání/příjem SMS zpráv na sériovém rozhraní

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.

Položka	Význam
TCP Port	TCP port, na kterém bude povoleno posílání/příjem SMS zpráv.

Tabulka 60: Posílání/příjem zpráv na zadaném TCP portu

Práce s SMS zprávami

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 Advantech B+B SmartWorx. 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)

Pokračování na následující straně

Pokračování z předchozí strany

AT příkaz	Popis
AT+COPS?	Identifikuje aktuálně dostupné mobilní sítě
AT+CPIN	Dotazování a zadávání PIN kódu
AT+CPMS	Definuje 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 61: AT příkazy pro práci s SMS

Podrobnější popis těchto příkazů a příklady jejich použití najdete v aplikační příručce pojmenované *AT příkazy* [9].

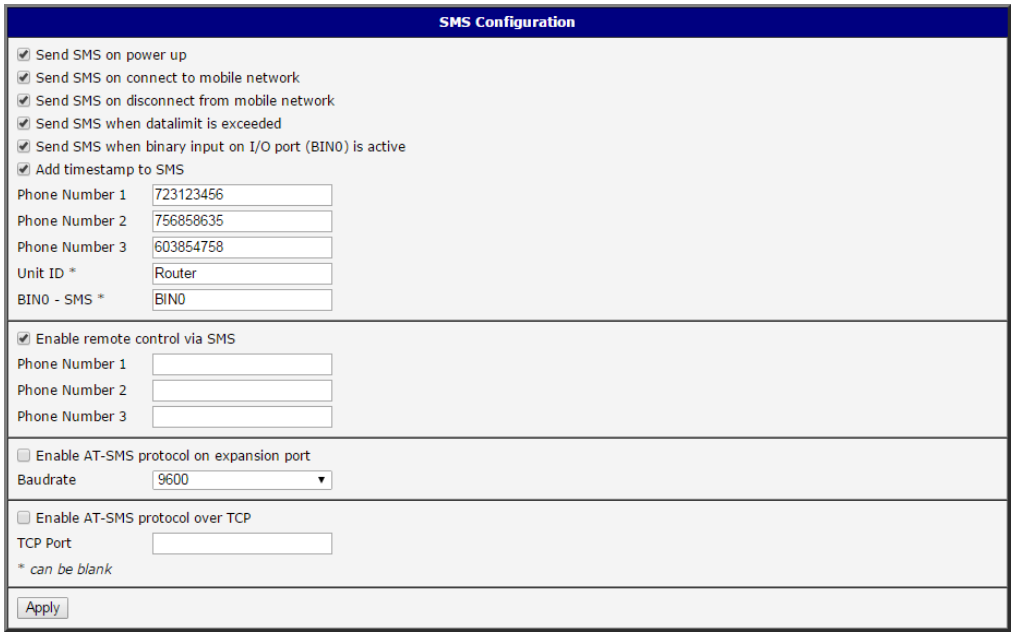
Příklady SMS konfigurace

Příklad 1 Nastavení posílání SMS

Po zapnutí napájení (*Power up*) přijde na uvedené telefonní číslo sms ve tvaru:
Router (Unit ID) has been powered up. Signal strength –xx dBm.

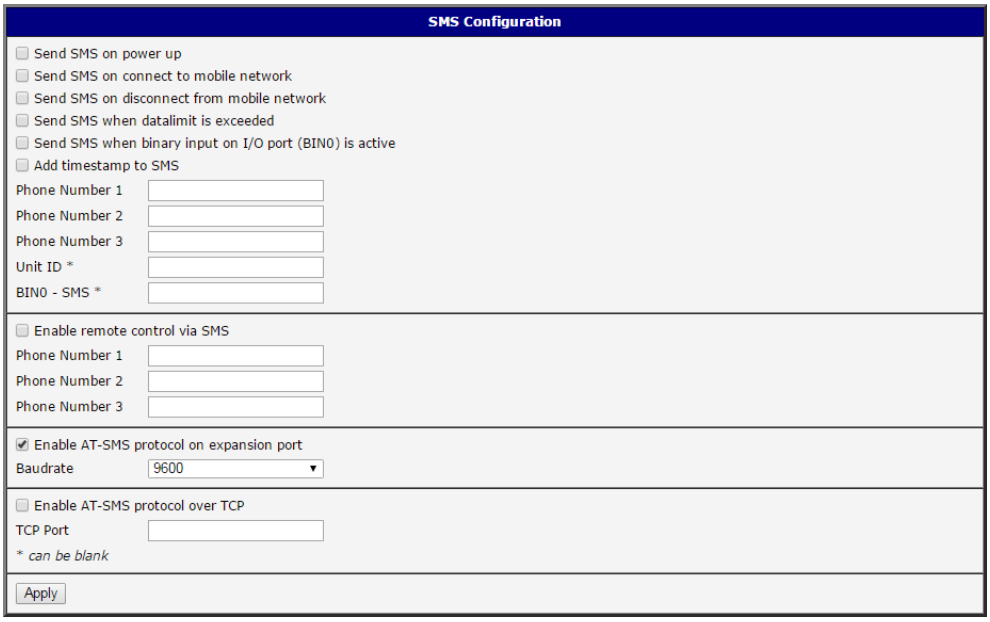
Při sestavení spojení přijde na uvedené telefonní číslo SMS ve tvaru:
Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

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



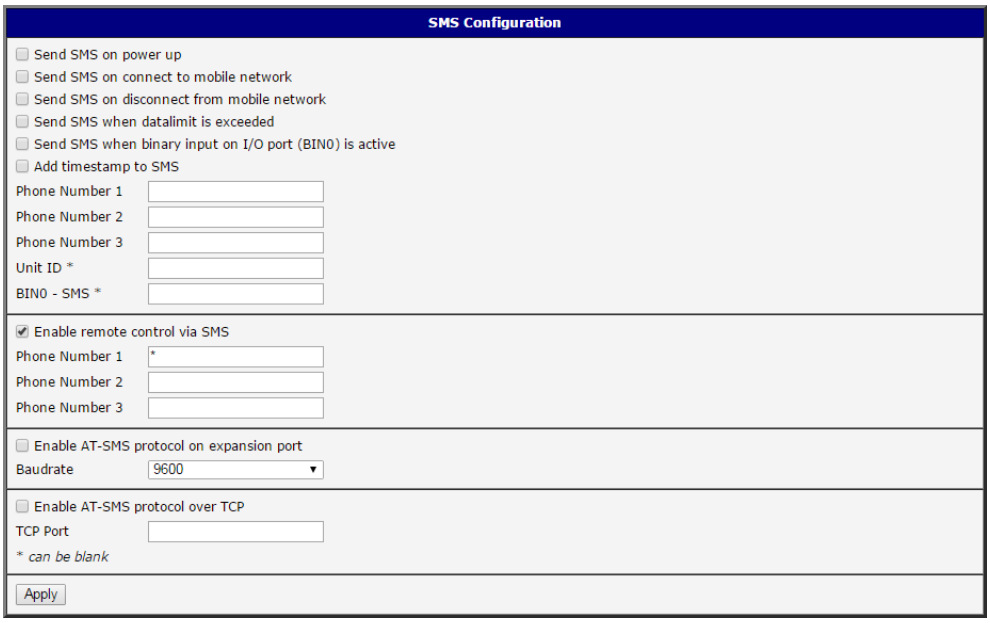
Obrázek 55: Konfigurace SMS pro příklad 1

Příklad 2 Posílání SMS přes sériové rozhraní



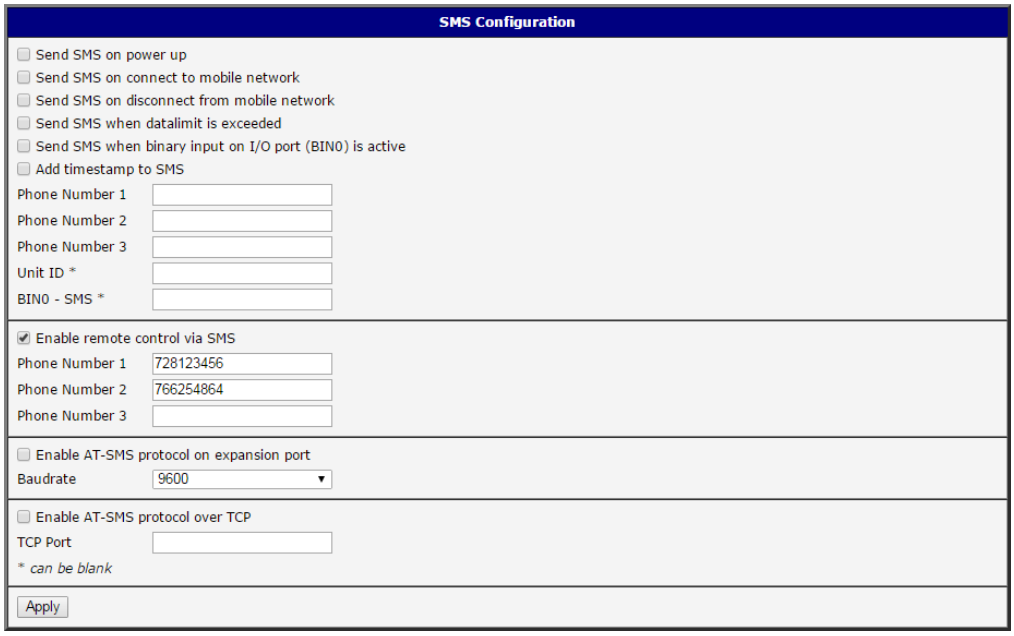
Obrázek 56: Konfigurace SMS pro příklad 2

Příklad 3 Nastavení pro ovládání routeru SMS zprávami z libovolného tel. čísla



Obrázek 57: Konfigurace SMS pro příklad 3

Příklad 4 Nastavení pro ovládání routeru SMS zprávami ze dvou tel. čísel



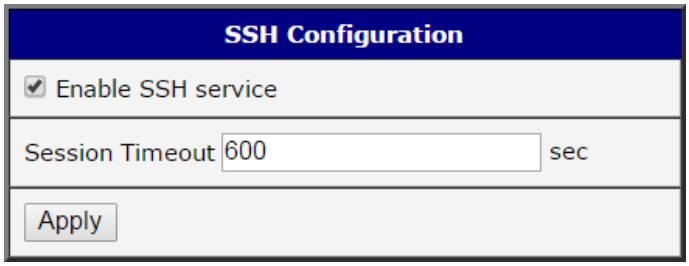
Obrázek 58: Konfigurace SMS pro příklad 4

4.15.7 SSH

SSH protokol (Secure Shell) umožňuje realizovat zabezpečené vzdálené připojení k routeru Konfiguraci SSH serveru lze vyvolat volbou položky *SSH* ve složce *Services*. Zaškrtnutím položky *Enable SSH service* dojde k povolení SSH serveru na routeru.

Položka	Popis
Enable SSH service	Povolení služby SSH.
Session Timeout	Maximální doba nečinnosti, po kterém je spojení ukončeno.

Tabulka 62: Parametry konfigurace SSH služby



Obrázek 59: Konfigurace SSH služby

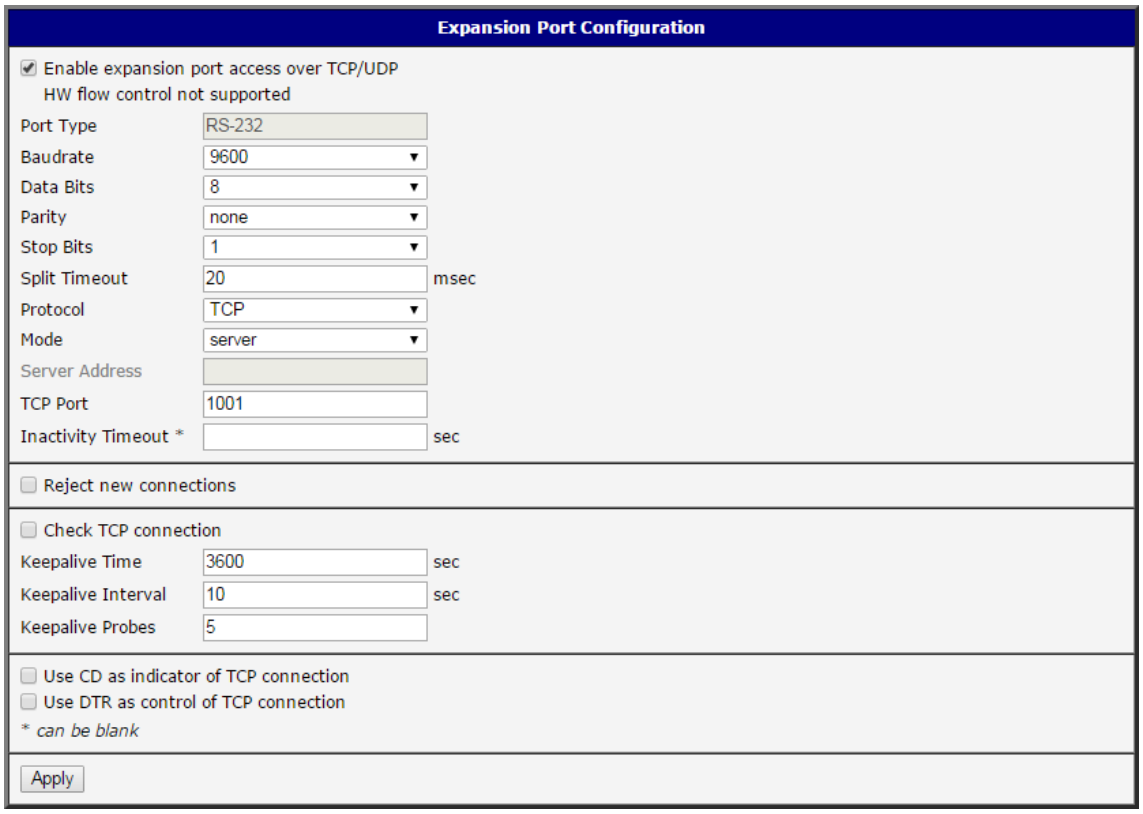
4.16 Konfigurace sériového rozhraní

Konfiguraci sériového rozhraní RS232 (konektor DB9) je možné vyvolat volbou položky *Expansion Port*.

V horní části okna konfigurace lze povolit přístup na volitelný port a pod položkou *Port Type* je zobrazen typ volitelného portu. Další položky popisuje následující tabulka. V routeru je podpora IPv6 TCP/UDP klienta/serveru.

Položka	Popis
Baudrate	Specifikuje 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	Definuje 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. Lze zadat IPv4 nebo IPv6 adresu.
TCP Port	TCP/UDP port na kterém probíhá komunikace.
Inactivity Timeout	Časový úsek, po kterém se přeruší TCP/UDP spojení v případě neaktivity.

Tabulka 63: Konfigurace sériového rozhraní



Obrázek 60: Konfigurace volitelného portu

Je-li zvolena položka *Reject new connections*, veškerá další spojení jsou odmítána. Není tedy možné návazat více spojení najednou.
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 volitelného portu – *Check TCP connection*

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

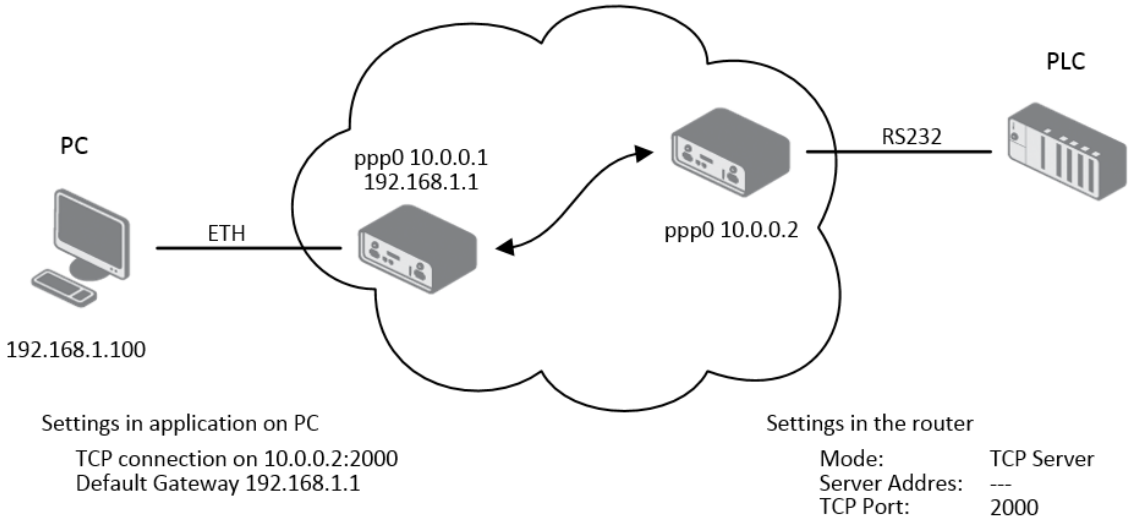
Při zaškrtnutí položky *Use DTR as control of TCP connection* se aktivuje funkce řízení TCP spojení pomocí signálu DTR (CD na straně routeru).

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

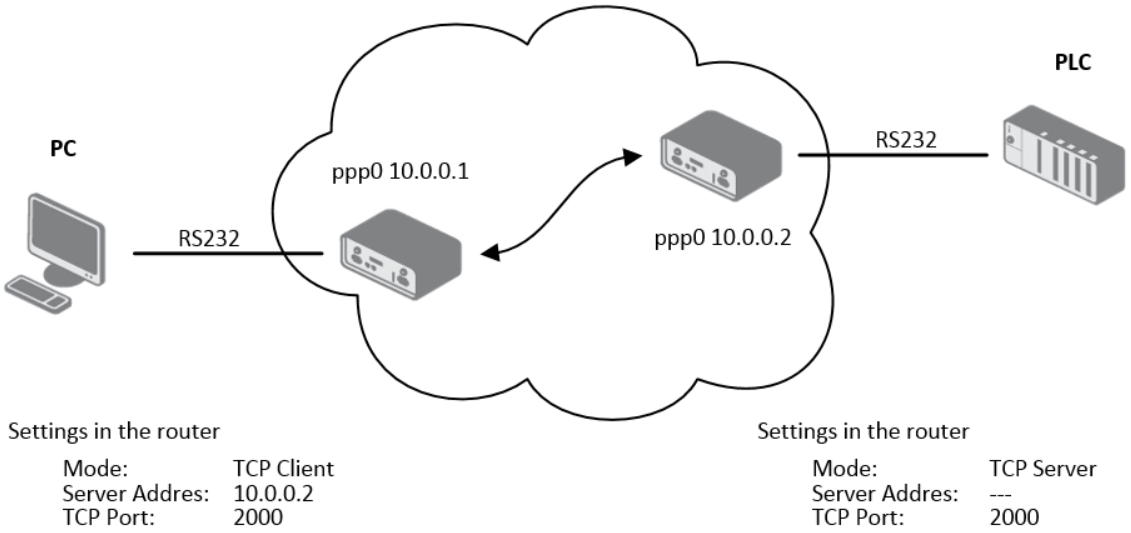
Tabulka 66: Popis signálu DTR

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

4.16.1 Příklady konfigurace sériového rozhraní



Obrázek 61: Příklad nastavení komunikace z Ethernetu na sériovou linku



Obrázek 62: Příklad konfigurace sériového rozhraní

4.17 Skripty (Scripts)

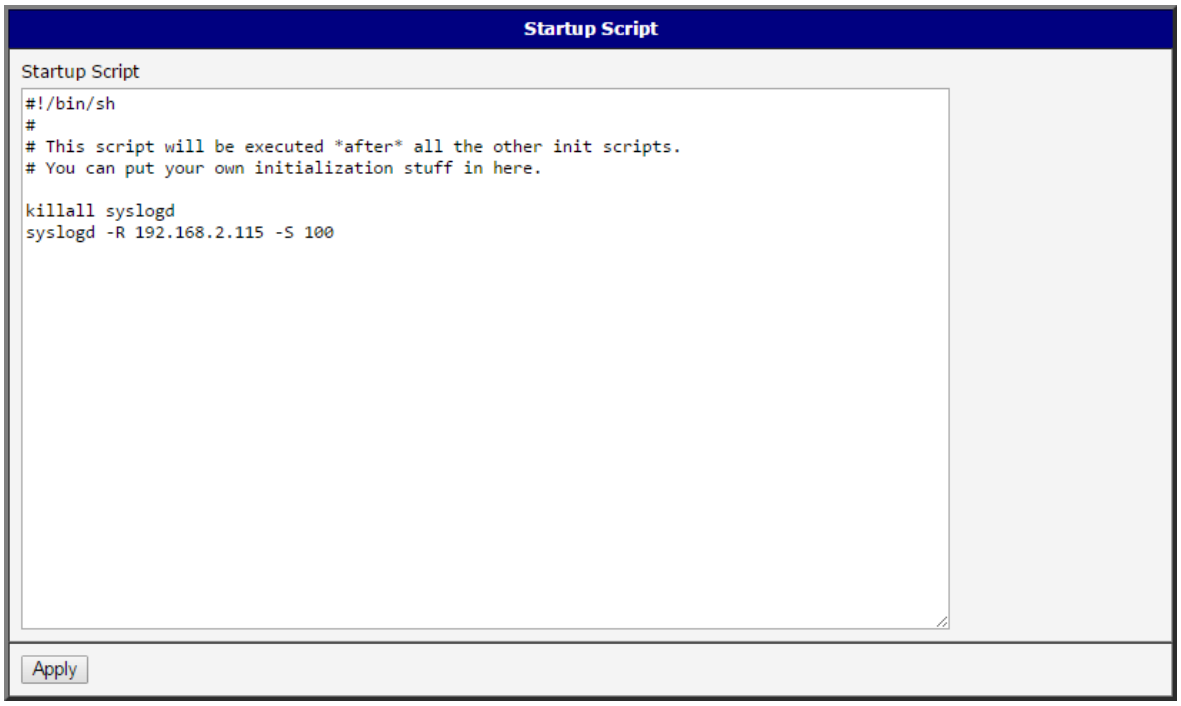
Na stránce *Scripts* v sekci *Configuration* lze definovat vlastní shellové skripty, které jsou spoštěny ve specifických situacích. Položka *Scripts* v menu se po kliknutí rozvine a objeví se možnosti *Startup Script*, *Up/Down IPv4* a *Up/Down IPv6*, které je možno definovat. V routeru je implementován nezávislý IPv4 a IPv6 dual stack. Pro více příkladů skriptů a seznam možných příkazů a programů viz aplikační příručku *Commands and Scripts* [1].

4.17.1 Startup Script

V okně *Startup Script* je možné vytvářet vlastní skripty, které budou spuštěny vždy po init skriptech po startu nebo rebootu routeru. Změny v nastavení se projeví po stisknutí tlačítka *Apply*.

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

4.17.2 Příklad Startup skriptu



Obrázek 63: Příklad Startup scriptu

Při startu routeru je zastaven program syslogd a následně je spuštěn se vzdáleným logováním na adresu 192.168.2.115 a omezený výpisem na 100 záznamů. Přidejte tyto řádky do pole *Startup Script*:

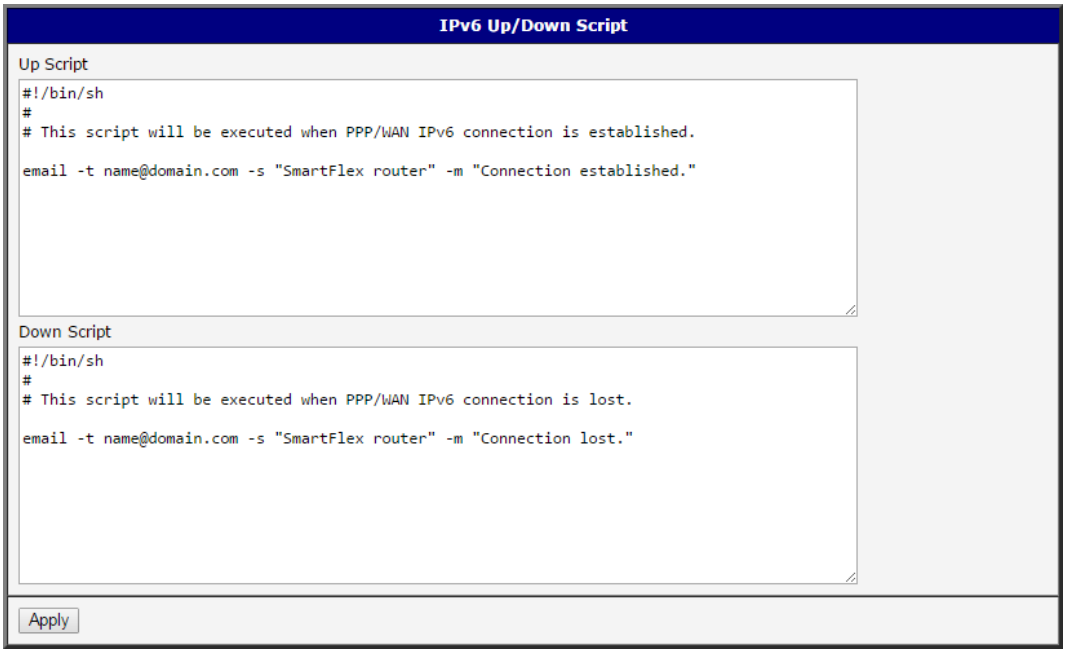
```
killall syslogd
syslogd -R 192.168.2.115 -S 100
```

4.17.3 Up/Down script

Na stránce *Up/Down IPv4* a *Up/Down IPv6* je možné vytvářet vlastní skripty, které jsou spouštěny když dojde k (mobilnímu) připojení nebo odpojení od internetu. V routeru je implementován nezávislý souběh protokolů IPv4 a IPv6 – dual stack. Proto lze nastavit Up/Down skripty nezávisle, takže *IPv4 Up/Down Script* se spouští pouze při připojení/odpojení pomocí IPv4 a *IPv6 Up/Down Script* pouze při připojení/odpojení pomocí IPv6. Skripty zapsané v poli *Up Script* budou spuštěny po inicializaci WAN připojení do internetu. Do pole *Down Script* se zapisují skripty, které budou spuštěny při výpadku nebo po ztrátě připojení.

Změny v nastavení se projeví až po stisknutí tlačítka *Apply*. I zde je nutné provést reboot routeru, aby se skripty spouštěly.

4.17.4 Příklad IPv6 Up/Down skriptu



Obrázek 64: Příklad IPv6 Up/Down skriptu

Po navázání nebo ztrátě IPv6 připojení do internetu router odešle e-mail s informací o navázání nebo ztrátě spojení. Je nutné také předtím nastavit *SMTP*.

Tento řádek přidejte do pole *Up Script*:

```
email -t name@domain.com -s "Router" -m "Connection up."
```

Tento řádek přidejte do pole *Down Script*:

```
email -t name@domain.com -s "Router" -m "Connection down."
```

4.18 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 z HTTP(S) nebo FTP(S) serveru, kde je konfigurační soubor nebo firmware uložen. Jsou podporovány také IPv6 servery. Adresou v položce *Base URL*, je specifikován protokol, který se má použít: HTTP, HTTPS, FTP nebo FTPS. 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
Base URL	Umožňuje zadat základní část doménového jména, IPv4 nebo IPv6 adresu serveru, ze které se bude firmware nebo konfigurace routeru stahovat. Určuje i komunikační protokol (HTTP, HTTPS, FTP nebo FTPS).
Unit ID	Název stahované konfigurace (název souboru bez přípony). 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*. Správné jméno souboru firmware je vypsáno na stránce *Update Firmware* v sekci *Administration*. Viz kapitola 6.11

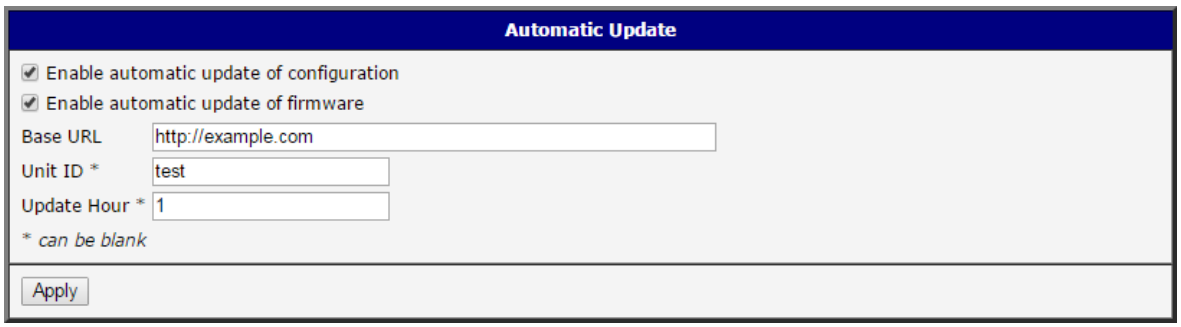
Na HTTP(S)/FTP(S) server je nutné vždy nahrát dva soubory – .bin a .ver. Pokud by byl na server nahrán pouze soubor s příponou .bin a HTTP by při pokusu o stahování neexistujícího souboru .ver odeslalo chybnou odpověď *200 OK* (místo očekávané *404 Not Found*), pak je zde vysoké riziko, že router bude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

Aktualizace firmware může způsobit nekompatibilitu uživatelských modulů. Pokud jsou využívány, je doporučeno je aktualizovat na nejnovější verzi. Informace o kompatibilitě uživatelského modulu s verzí firmware je v úvodu aplikační příručky k příslušnému uživatelskému modulu.

4.18.1 Příklad nastavení automatické aktualizace

V následujícím příkladu router zjišťuje, jestli je k dispozici nový firmware nebo konfigurace a případně provádí aktualizaci každý den v 1:00 ráno. Příklad je uveden pro router SmartStart.

- Soubor firmware: http://example.com/SPECTRE-v3L-LTE.bin
- Konfigurační soubor: http://example.com/test.cfg

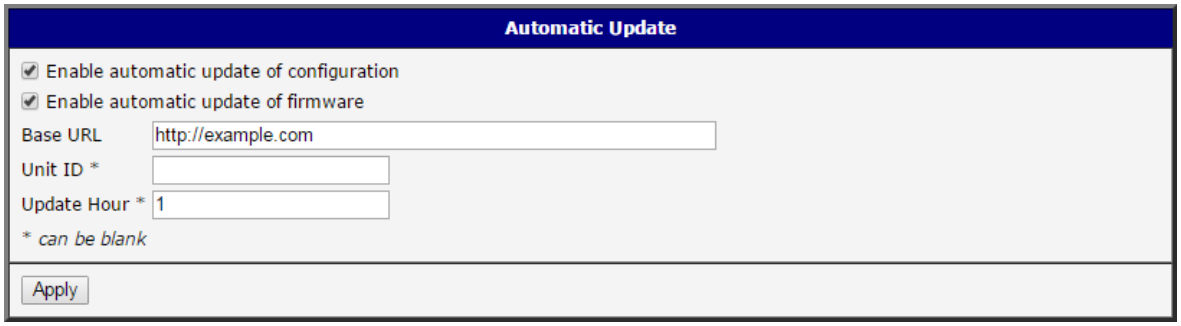


Obrázek 65: Příklad automatické aktualizace 1

4.18.2 Příklad nastavení automatické aktualizace na základě MAC adresy

V následujícím příkladu router zjišťuje, jestli je k dispozici nový firmware nebo konfigurace a případně provádí aktualizaci každý den v 1:00 ráno. Příklad je uveden pro router SmartStart s MAC adresou 00:11:22:33:44:55.

- Soubor firmware: http://example.com/SPECTRE-v3L-LTE.bin
- Konfigurační soubor: http://example.com/00.11.22.33.44.55.cfg

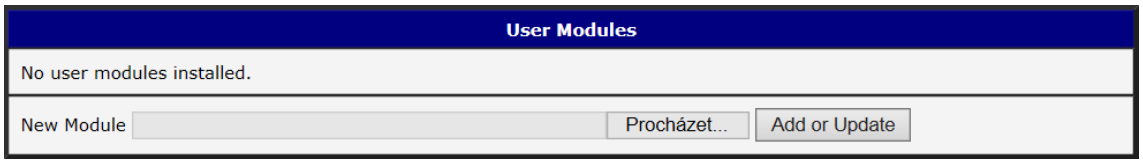


Obrázek 66: Příklad automatické aktualizace 2

5. Přizpůsobení

5.1 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 or Update*.

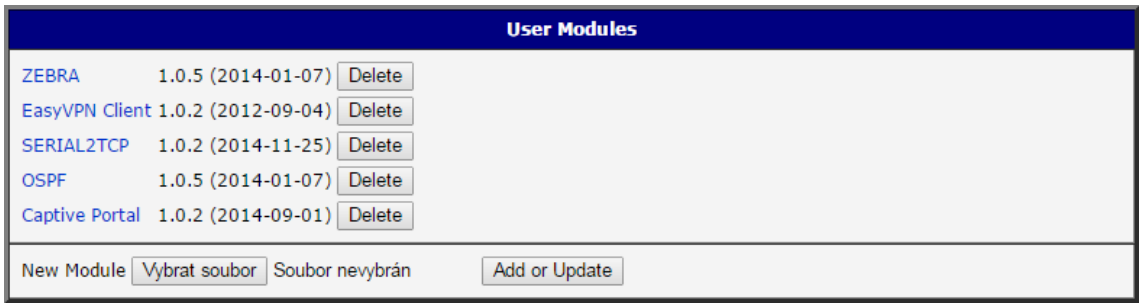


Obrázek 67: User modules

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 *Programming of User Modules* [10].



Obrázek 68: Přidány uživatelské moduly

Dostupné jsou například tyto a další uživatelské moduly. Uživatelské moduly lze stáhnout na webových stránkách www.bb-smartcellular.cz, lze si je také nechat na zakázku naprogramovat.

Název modulu	Popis
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.
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 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).
IS-IS	Doplňuje podporu protokolu IS-IS.

Tabulka 68: Uživatelské moduly

Pozor, v některých případech může aktualizace firmware způsobit nekompatibilitu používaných uživatelských modulů, protože některé z nich jsou závislé na verzi použitého kernelu apod. (jedná se např. o moduly *SmsBE* a *PoS Configuration*). Je doporučeno uživatelské moduly aktualizovat na nejnovější verzi.

Informace o kompatibilitě uživatelského modulu s verzí firmware je v úvodu aplikační příručky k příslušnému uživatelskému modulu.

6. Administrace

6.1 Uživatelé

Tento konfigurační formulář není dostupný pro uživatele mající roli *User*!

Pro správu uživatelských účtů je k dispozici položka *Users* v části *Administration* hlavního menu. První část formuláře obsahuje přehled již existujících uživatelů. V tabulce níže je popsán význam všech dostupných tlačítek, které v této části jsou.

Tlačítko	Popis
Lock	Zamyká uživatelský účet. Poté se uživatel nemůže přihlásit do routeru (přístup je zakázán jak přes webové rozhraní tak pomocí SSH).
Change Password	Pomocí tohoto tlačítka lze změnit heslo příslušného uživatele.
Delete	Umožňuje smazat účet příslušného příslušného uživatele.

Tabulka 69: Přehled uživatelů

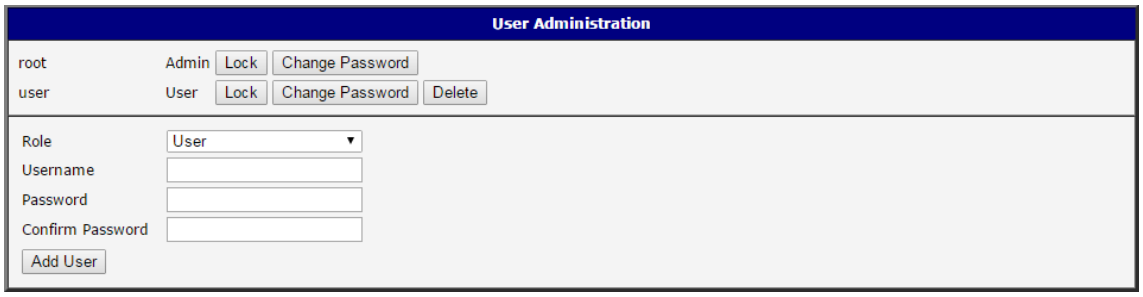
Pozor! Pokud uzamknete účet všem uživatelům s oprávněním *Admin*, nebude již možné tyto účty odemknout! To rovněž znamená, že stránka *Users* bude všem uživatelům nedostupná, protože uživatelé s oprávnění admin budou mít zamknuté účty a uživatelé users nemají dostatečné oprávnění.

Ve druhé části je k dispozici formulář, pomocí něhož lze přidávat nové uživatele. Všechny položky jsou popsány v tabulce níže.

Položka	Popis
Role	Definuje typ uživatelského účtu: • **User** – Uživatel se základním oprávněním. • **Admin** – Uživatel s administrátorským oprávněním.
Username	Uživatelské jméno pro přihlášení do webového rozhraní routeru.
Password	heslo pro přihlášení do webového rozhraní routeru.
Confirm Password	Potvrzení hesla uvedeného v kolonce výše.

Tabulka 70: Přidání nového uživatele

Běžní uživatelé nemohou přistupovat k routeru pomocí Telnetu, SSH a SFTP. Zároveň mají pouze „read only“ oprávnění pro FTP přístup.

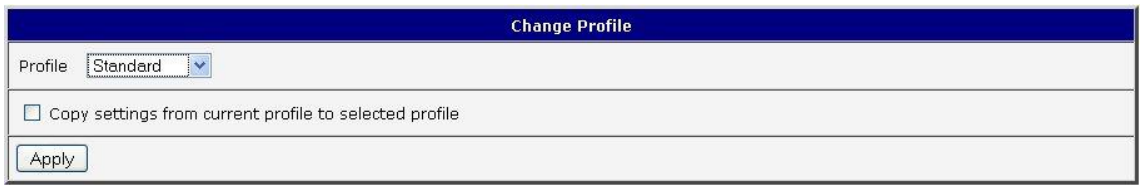


Obrázek 69: Users

6.2 Změna profilu

Profily umožňují přepínání mezi mezi různými konfiguracemi routeru – to lze využít například pro nastavení několika různých režimů 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 rozhraní routeru.

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.

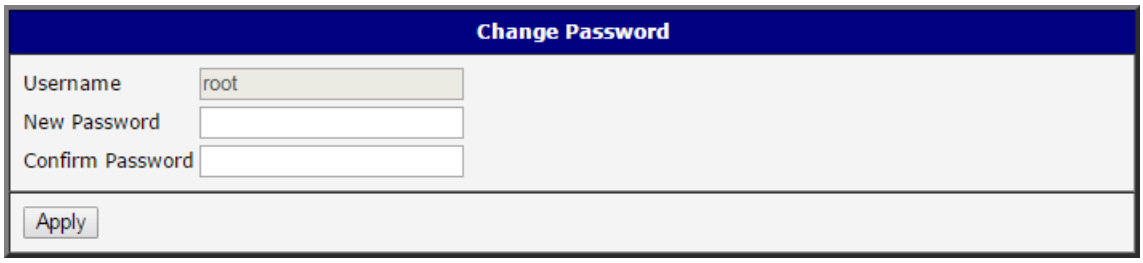


Obrázek 70: Změna profilu

6.3 Změna přístupového hesla

Dialog pro změnu hesla lze vyvolat volbou položky *Change Password* v menu. Heslo je nutné zadat dvakrát, nové heslo se uloží až po stisknutí tlačítka *Apply*.

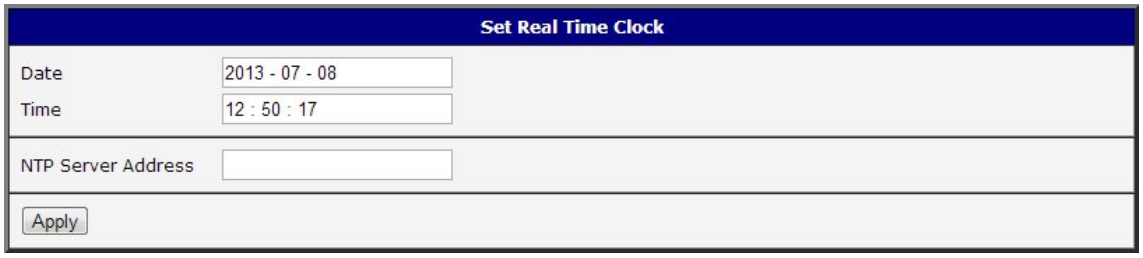
V základním nastavení routeru je heslo nastaveno defaultně na *root*. **Pro zajištění bezpečnosti sítě spravované routerem je nutné standardní heslo změnit.**



Obrázek 71: Změna přístupového hesla

6.4 Nastavení vnitřních hodin

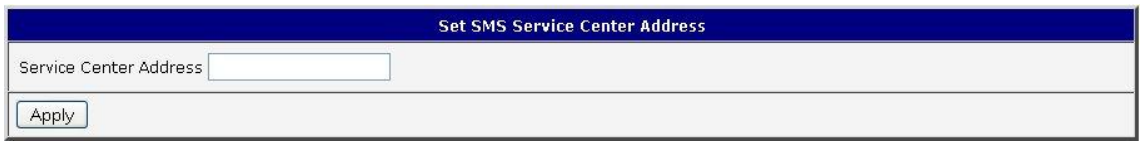
Jednorázové nastavení vnitřních hodin routeru lze vyvolat volbou položky *Set Real Time Clock* v menu. Hodiny a datum lze nastavit ručně prostřednictvím položek *Date* a *Time*. Údaje zadávejte vždy ve formátu, který je znázorněn na obrázku níže. Hodiny lze seřídit také podle zadaného NTP serveru po stisknutí tlačítka *Apply*. IPv4, IPv6 adresa nebo doménové jméno jsou podporovány.



Obrázek 72: Nastavení vnitřních hodin

6.5 Nastavení SMS centra

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.

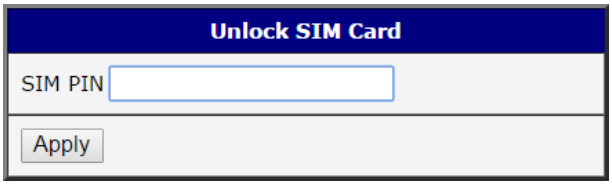


Obrázek 73: Nastavení SMS centra

6.6 Odemknutí SIM karty

Odemčení SIM karty je možno provést na administrační stránce *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*.

Po třech neúspěšných pokusech při zadání PIN kódu je SIM karta zablokována. Odblokování SIM karty pomocí PUK kódu je popsáno v následující kapitole.

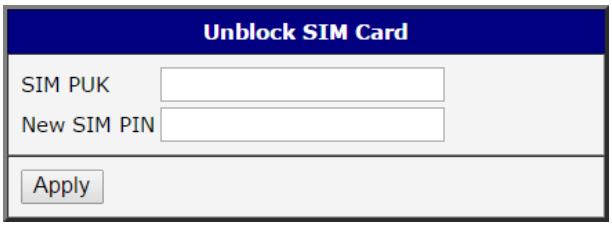


Obrázek 74: Odemknutí SIM karty

6.7 Odblokování SIM karty

Odblokování SIM karty je možno provést na administrační stránce *Unblock SIM Card*. Zde je možné odblokovat SIM kartu, případně pouze změnit její PIN kód. V obou případech je nutné zadat jak PUK kód do pole *SIM PUK*, tak nový SIM kód do pole *New SIM PIN*. K odemknutí SIM karty a nastavení nového SIM kódu dojde po kliknutí na tlačítko *Apply*.

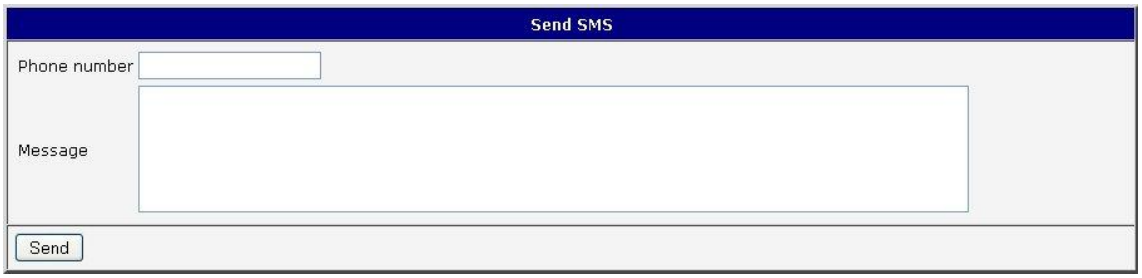
Po třech neúspěšných pokusech při zadání PUK kódu je SIM karta trvale zablokována.



Obrázek 75: Odblokování SIM karty

6.8 Poslání SMS zprávy

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*. Lze posílat pouze zprávy standartní délky 160 znaků. (Pro posílání dlouhých SMS lze využít např. uživatelský modul pduSMS).



Obrázek 76: Poslání SMS zprávy

SMS zprávu je též možno odeslat prostřednictvím CGI skriptu. Podrobnosti o tomto způsobu posílání SMS zpráv naleznete v příručce *Commands and Scripts* [1].

6.9 Zálohování konfigurace

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

6.10 Obnovení konfigurace

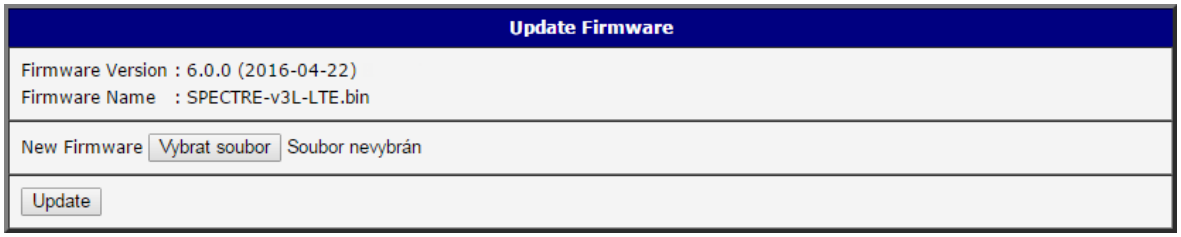
Pokud je potřeba obnovit konfiguraci routeru, je možné v položce *Restore Configuration* vybrat z vašeho počítače konfigurační soubor pomocí tlačítka *Procházet*.

Obrázek 77: Obnovení konfigurace

6.11 Aktualizace firmware

Informace o verzi firmware a pokyny pro jeho aktualizaci lze vyvolat volbou položky *Update Firmware* v menu. Je zde vypsána aktuální verze firmware a jméno souboru, které musí mít soubor firmware použitý k aktualizaci. Nový firmware je vybrán přes položku *Procházet* z vašeho počítače (soubor firmware je tedy nutné mít v počítači uložený) a následným stisknutím tlačítka *Update* je aktualizace spuštěna.

Během aktualizace firmwaru musí být zajištěno trvalé napájení. Při výpadku napájení by mohlo dojít k poškození routeru. Celková doba aktualizace může trvat až pět minut. Je nutné vždy použít firmware s názvem souboru vypsaným zde pod položkou *Firmware Name*!



Obrázek 78: Aktualizace firmware

Nahráním firmware jiného přístroje by mohlo dojít k poškození routeru!

Během aktualizace firmwaru se vypíše následující výpis, který informuje o aktuálním průběhu. Postup programování FLASH paměti je znázorněn přibývajícími procenty:

Firmware Update

Do not turn off the router during the firmware update.
The firmware update can take up to 5 minutes to complete.

Uploading firmware to RAM... ok
Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH... 3 %

Po dokončení aktualizace firmware je router automaticky restartován:

Firmware Update

Do not turn off the router during the firmware update.
The firmware update can take up to 5 minutes to complete.

Uploading firmware to RAM... ok
Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH... ok
Updating u-boot environment... ok

Reboot in progress

Continue here after reboot.

Počínaje FW 5.1.0 je doplněn mechanismus zabraňující vícenásobnému spuštění aktualizace firmware. Aktualizace firmware může způsobit nekompatibilitu uživatelských modulů. Pokud jsou využívány, je doporučeno je aktualizovat na nejnovější verzi. Informace o kompatibilitě uživatelského modulu s verzí firmware je v úvodu aplikační příručky k příslušnému uživatelskému modulu.

6.12 Reboot

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

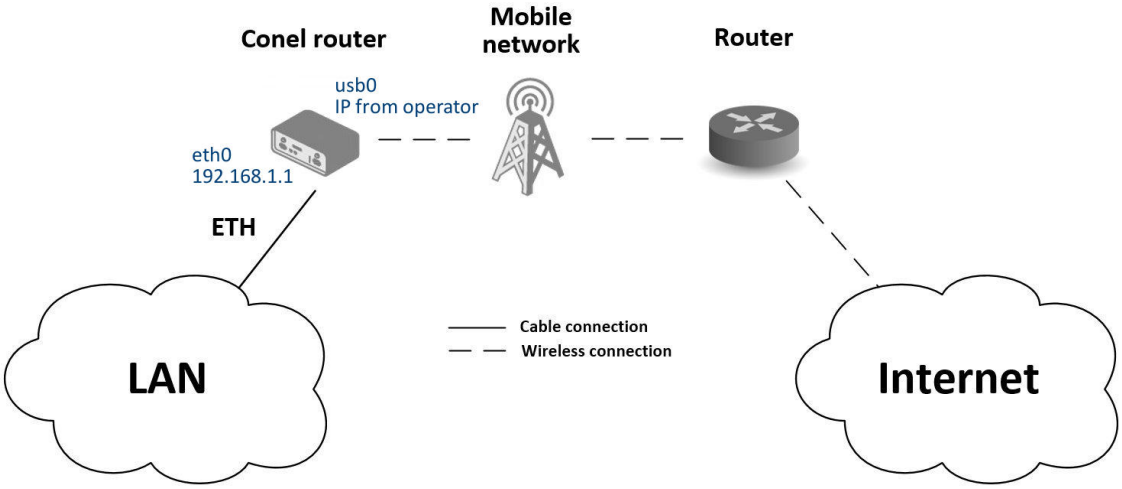
Reboot
The reboot process will take about 20 seconds to complete.
Reboot

Obrázek 79: Reboot

7. Konfigurace v typických situacích

Ač má Advantech B+B SmartWorx router široké možnosti využití, je nejčastěji používán v typických situacích uvedených v této kapitole. Příklady zahrnují všechny položky, jež je nutno pro danou funkcionalitu v routeru nastavit. Příklady jsou uvedeny pro použití v IPv4 sítích.

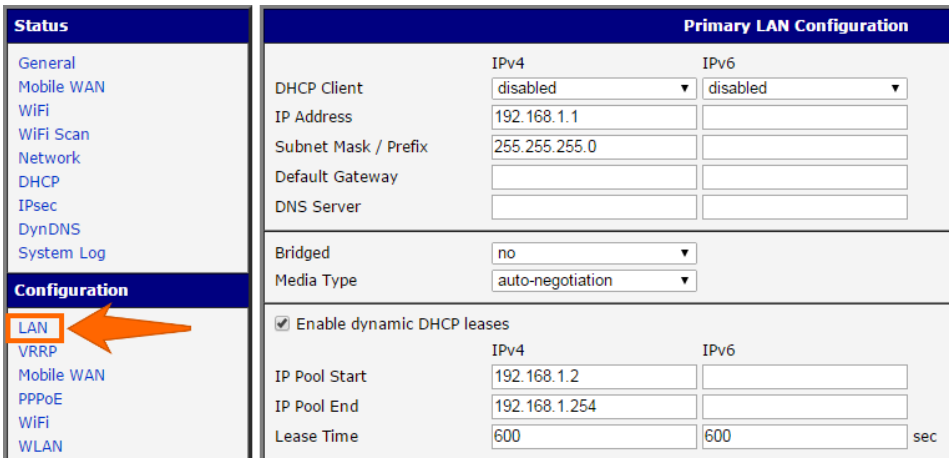
7.1 Přístup na internet z LAN



Obrázek 80: Přístup na internet z LAN – topologie příkladu

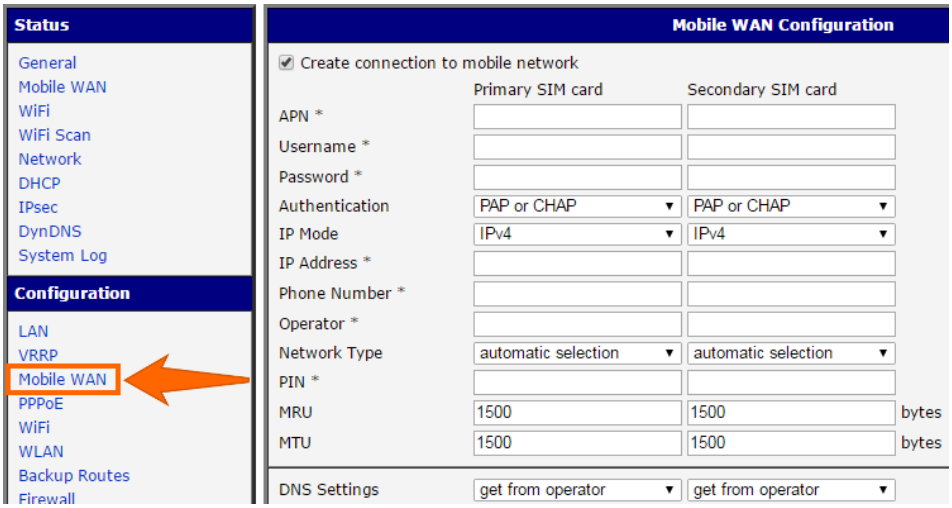
Na obrázku výše je naznačena topologie tohoto jednoduchého příkladu. Pro připojení do internetu přes mobilní síť je nutné mít od operátora SIM kartu s datovým tarifem. Tato základní funkcionalita routeru v tomto případě **nevyžaduje žádnou konfiguraci**. Stačí zezadu routeru zasunout SIM kartu do slotu SIM1 (Primary SIM card), ke konektoru ANT přišroubovat příslušnou anténu a připojit počítač (nebo switch a počítače) k routeru na rozhraní ETH0 (LAN). Po zapnutí routeru je nutno chvíli vyčkat, než se připojí do mobilní sítě a k internetu. To signalizují LED diody na předním panelu routeru (WAN a DAT). Konfiguraci je pak možné provádět pod položkami *LAN* a *Mobile WAN* ve webovém rozhraní routeru v sekci *Configuration*.

Konfigurace LAN IP adresa routeru na rozhraní eth0 je z výroby nastavena na 192.168.1.1. Po přihlášení do routeru lze toto nastavení změnit pod položkou *LAN* v sekci *Configuration*, viz obr. 81 V tomto konkrétním případě není třeba žádného nastavení, z výroby je také zapnut DHCP server, který přiděluje připojeným zařízením IP adresy, takže první připojený počítač dostane adresu 192.168.1.2 atd. Možnosti dalšího nastavení jsou popsány v kapitole 4.1.



Obrázek 81: Přístup na internet z LAN – konfigurace LAN

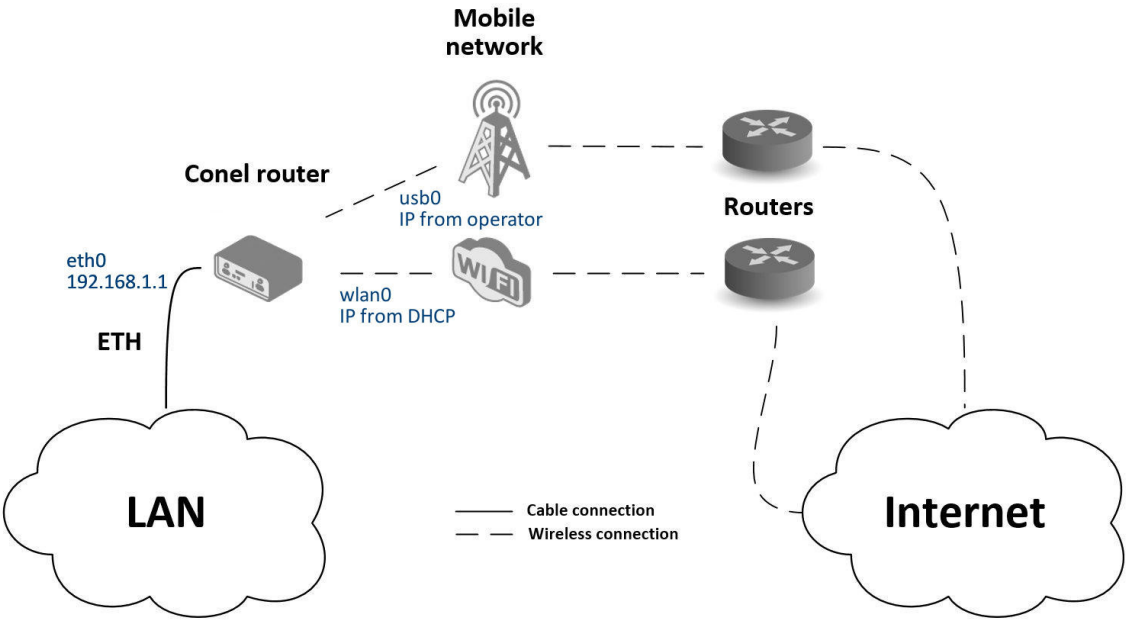
Konfigurace Mobile WAN Připojení do mobilní sítě se konfiguruje pod položkou *Mobile WAN* v sekci *Configuration*, viz obr. 82. V tomto případě (záleží na použité SIM kartě) lze ponechat konfigurační formulář nevyplněný, pouze musí být zaškrtnuto *Create connection to mobile network*, což je z výroby nastaveno. Pro podrobnější nastavení viz kap. 4.3.1.



Obrázek 82: Přístup na internet z LAN – konfigurace Mobile WAN

Správnou funkci připojení lze ověřit v routeru pod položkou *Mobile WAN* v sekci *Status*, kde jsou informace o operátorovi, síle signálu apod. a úplně dole by měla být vypsána zpráva o úspěšném spojení – *Connection successfully established.* Pod položkou *Network* je pak vidět vytvořené interní rozhraní usb0 pro připojení do mobilní sítě, IP adresa přiřazená operátorem a dole také routovací tabulka. Počítače v LAN za routerem mají nyní přístup k internetu.

7.2 Zálohovaný přístup na internet z LAN



Obrázek 83: Zálohovaný přístup na internet z LAN – topologie příkladu

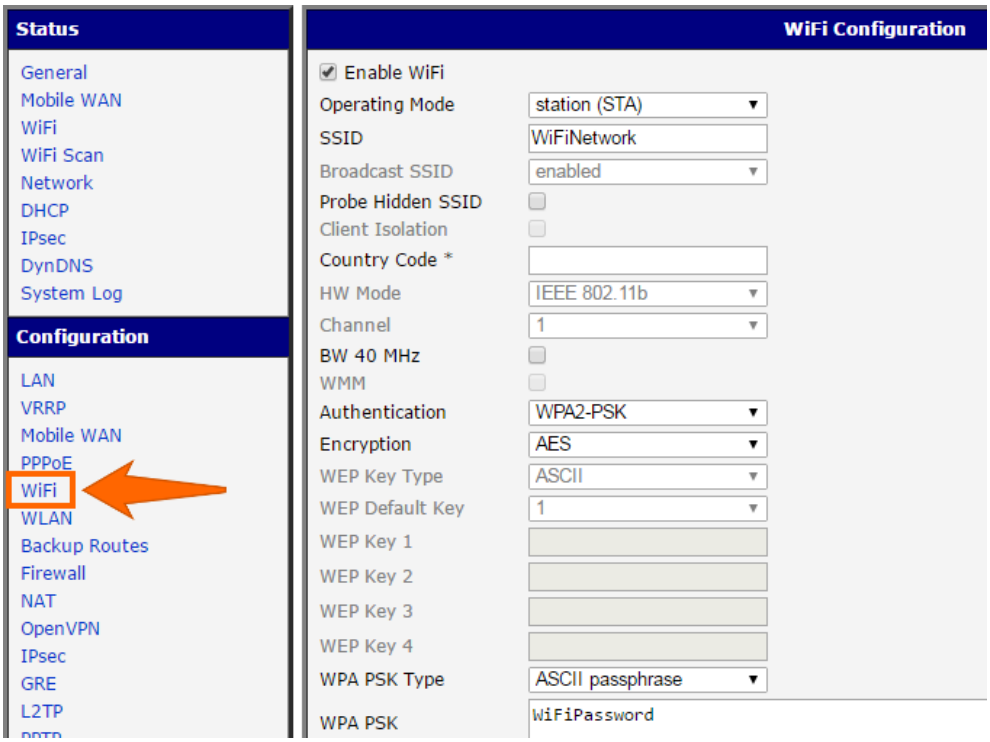
Nejprve je třeba nastavit jednotlivá připojení do internetu pod položkami *LAN* pro ethernetové rozhraní, *WLAN* a *WiFi* pro WiFi připojení a *Mobile WAN* pro mobilní připojení. Následně je možné nastavit priority záložních cest pod položkou *Backup Routes*.

Konfigurace LAN Pod položkou *LAN* lze ponechat nastavení z výroby jako v předchozí situaci. Změny se projeví kliknutím na *Apply*. Podrobné nastavení *LAN* je popsáno v kapitole 4.1.

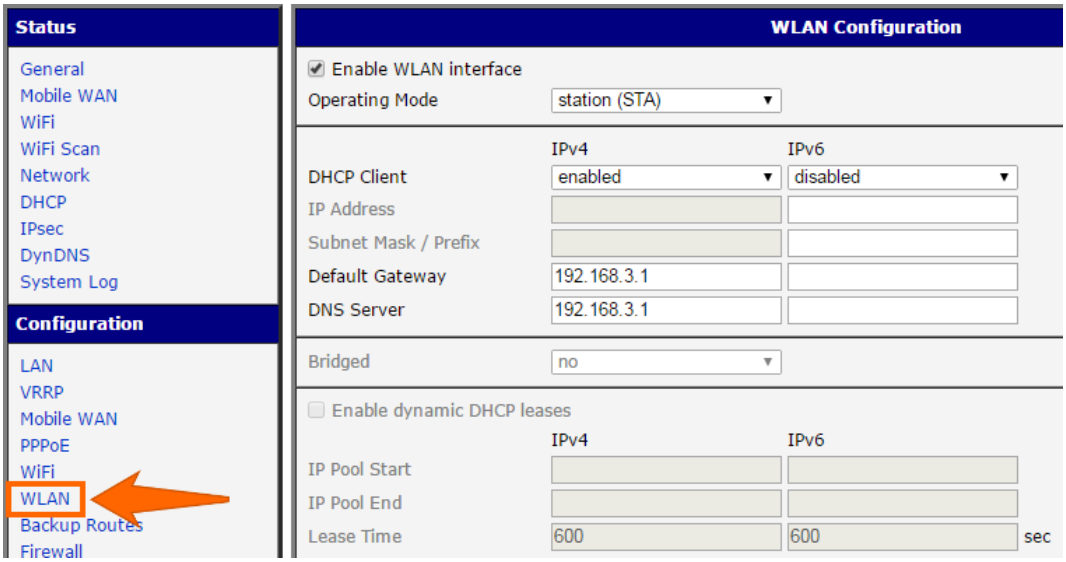
Konfigurace WLAN a WiFi Nejprve je nutné povolit rozhraní wlan0 pod položkou *WLAN*, viz obr. 85. Zde je nutno zaškrtnout *Enable WLAN interface*, *Operating Mode* nastavit na *station (STA)*, povolit DHCP klienta a vyplnit výchozí bránu a DNS server pro přístup k internetu. Nakonec je nutné vše potvrdit tlačítkem *Apply*. Podrobnější nastavení *WLAN* je popsáno v kapitole 4.6.

Konfigurace připojení k WiFi síti je pak možná pod položkou *WiFi*, viz obr. 84. Zde je nutné povolit WiFi zaškrtnutím *Enable WiFi*, nastavit údaje pro správné připojení (*SSID*, typ zabezpečení, heslo) a potvrdit tlačítkem *Apply*. Popis podrobnějšího nastavení *WiFi* lze nalézt v kapitole 4.5.

Ověření úspěšného připojení k WiFi síti je možné pod položkou *WiFi* v sekci *Status*. V případě úspěšného připojení zde bude vypsáno `wpa_state=COMPLETED`.



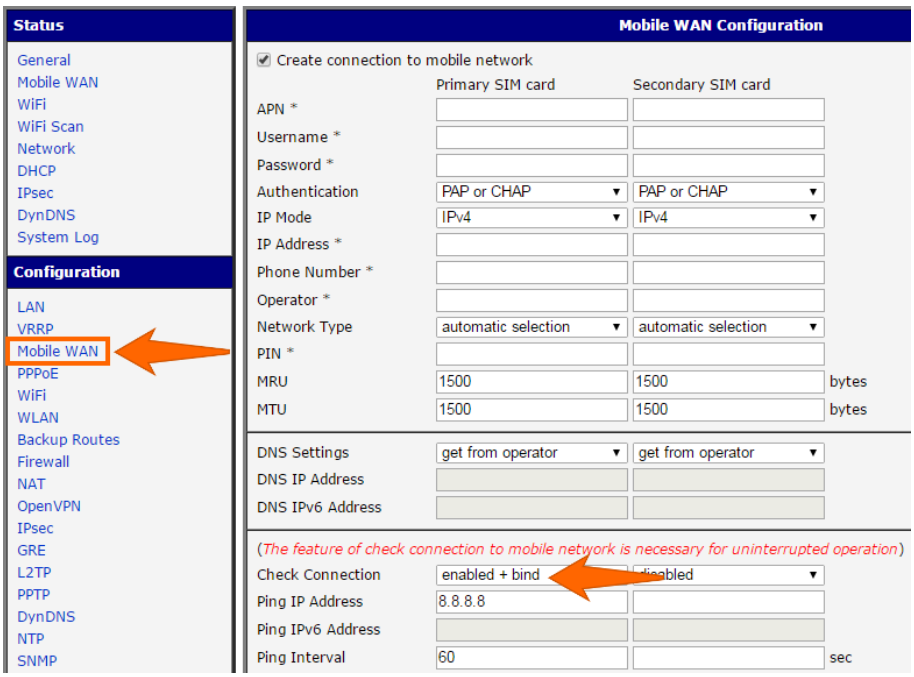
Obrázek 84: Zálohovaný přístup na internet z LAN – konfigurace WiFi



Obrázek 85: Zálohovaný přístup na internet z LAN – konfigurace WLAN

Konfigurace Mobile WAN Pro konfiguraci připojení do mobilní sítě stačí do routeru vložit SIM kartu do slotu SIM1 a připojit anténu ke konektoru ANT, jako v předchozím případě (závisí na použité SIM).

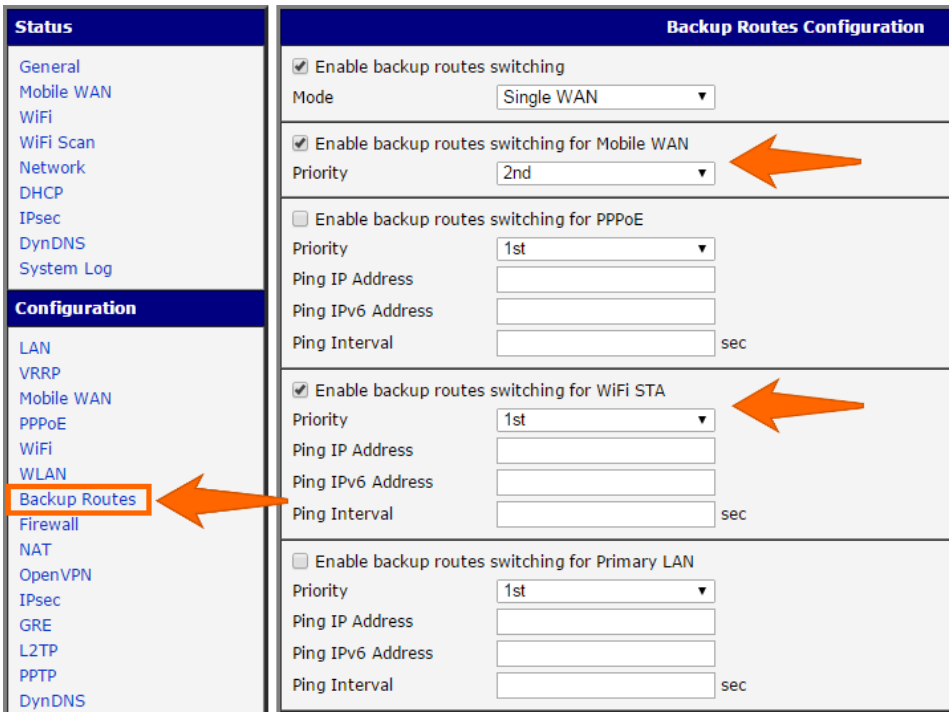
Pro použití v systému záložních cest je však nutné aktivovat kontrolu spojení pod položkou *Mobile WAN*, viz obr. 86. Volbu *Check connection* je nutné nastavit na *enable + bind* a doplnit IP adresu např. DNS serveru operátora nebo některého jistě dostupného serveru a časový interval kontroly spojení. Pro podrobnější nastavení viz kapitola 4.3.1.



Obrázek 86: Zálohovaný přístup na internet z LAN – konfigurace Mobile WAN

Konfigurace Backup Routes Nakonec je třeba definovat priority záložních cest. V této situaci byla zvolena nejvyšší priorita pro připojení přes WiFi wlan0 a potom přes mobilní připojení (rozhraní usb0). Tomu odpovídá nastavení pod položkou *Backup Routes* na obr. 87.

Systém záložních cest je nejprve třeba aktivovat zaškrtnutím *Enable backup routes switching* a dále je třeba u každé záložní cesty povolit opět její použití a nastavit prioritu. Nakonec je nutné nastavení potvrdit kliknutím na *Apply*. Pro podrobnější nastavení záložních cest viz kapitola 4.7.



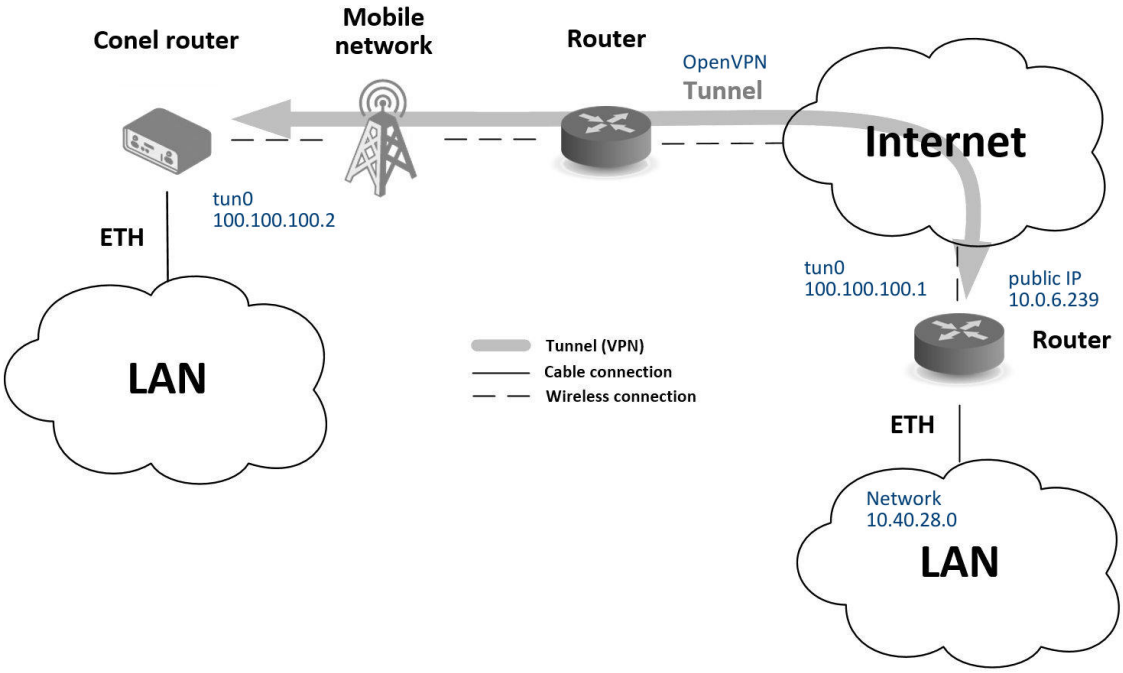
Obrázek 87: Zálohovaný přístup na internet z LAN – konfigurace Backup Routes

Takto nastavený router nyní slouží počítačům v LAN pro zálohovaný přístup k internetu. Nastavená síťová rozhraní lze ověřit pod položkou *Network* v sekci *Status*. Zde by měla být vidět aktivní rozhraní eth0 (připojení do LAN), wlan0 (WiFi připojení k internetu) a usb0 (mobilní připojení k internetu) včetně IP adres a dalších údajů.

V dolní části lze sledovat směrovací tabulku, na níž jsou vidět odpovídající změny v případě, že WiFi připojení selže (výchozí cesta se změní na usb0) – použije se mobilní připojení.

Záložní cesty fungují i bez aktivace systému záložních cest pod položkou *Backup Routes*, ovšem s implicitní prioritou jednotlivých rozhraní, jež je odlišná od priorit zvolených v této situaci, viz kapitola 4.7.

7.3 Zabezpečené propojení sítí nebo využití VPN



Obrázek 88: Zabezpečené propojení sítí – topologie příkladu

Pod pojmem VPN (Virtual Private Network) se rozumí zabezpečené (šifrované) a autentizované (ověřené) spojení dvou sítí LAN do jedné, takže se chová jako jediná homogenní LAN. Ke spojení sítí dochází nejčastěji přes veřejnou nedůvěryhodnou síť (internet), viz obr. 88. V Advantech B+B SmartWorx routerech lze za tímto účelem použít více způsobů (protokolů). Jsou jimi:

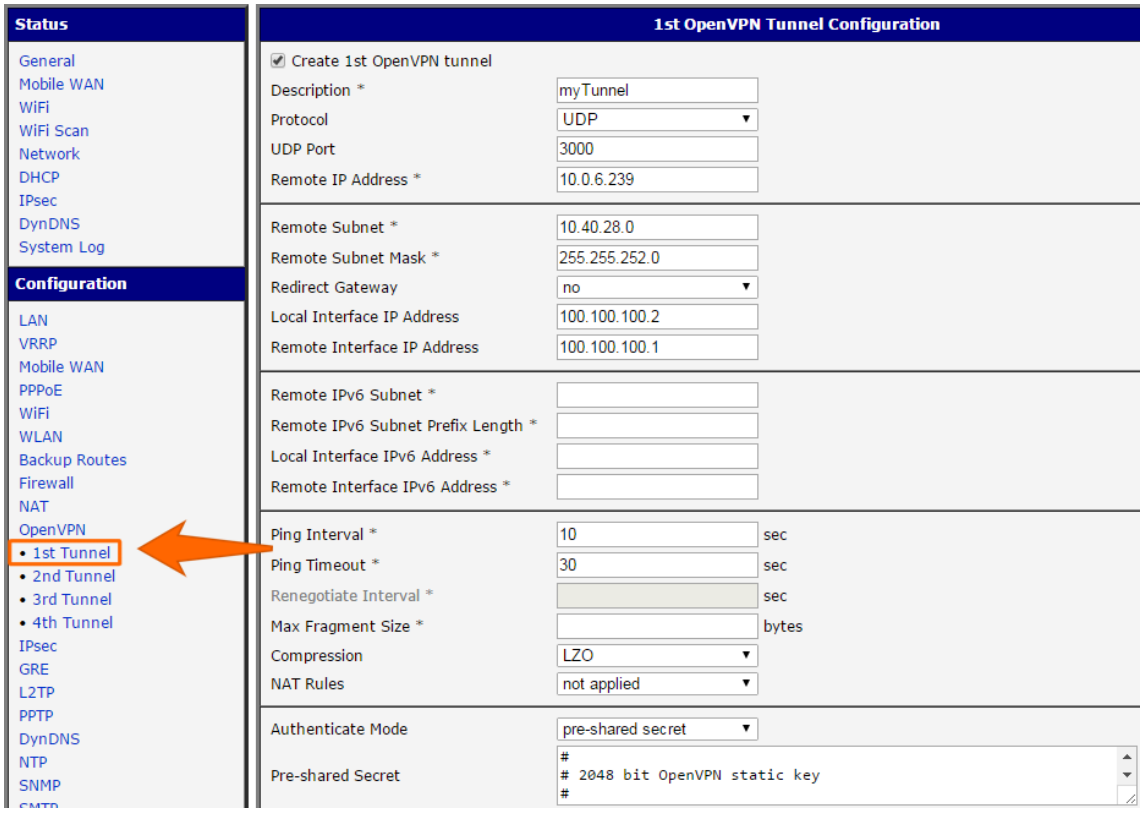
- *OpenVPN* (též položka konfigurace ve webovém rozhraní routeru), viz kapitola 4.10 nebo aplikační příručka [5],
- *IPsec* (též položka konfigurace ve webovém rozhraní routeru), viz kapitola 4.11 nebo aplikační příručka [6].

Z nešifrovaných tunelů umožňuje Advantech B+B SmartWorx router použití *GRE*, *PPTP* a *L2TP* tunelů. V kombinaci s IPsec tunelem lze k vytvoření VPN použít i GRE nebo L2TP tunel.

Na obr. 88 je uveden příklad OpenVPN tunelu. Předpoklady pro konfiguraci tohoto příkladu jsou následující: znalost IP adresy protějšího tunelu, znalost adresy protější sítě (nepovinné) a znalost sdíleného klíče. Pro připojení k OpenVPN tunelu je nutné v routeru nastavit položky *Mobile WAN* a *OpenVPN*.

Konfigurace Mobile WAN Připojení do mobilní síti je možné nastavit stejným způsobem jako v předchozích situacích (router se připojí sám po zasunutí SIM karty do slotu *SIM1* a připojení antény ke konektoru *ANT*), konfigurace je případně dostupná pod položkou *Mobile WAN* v sekci *Configuration* (viz kap. 4.3.1), kde musí být spojení povoleno.

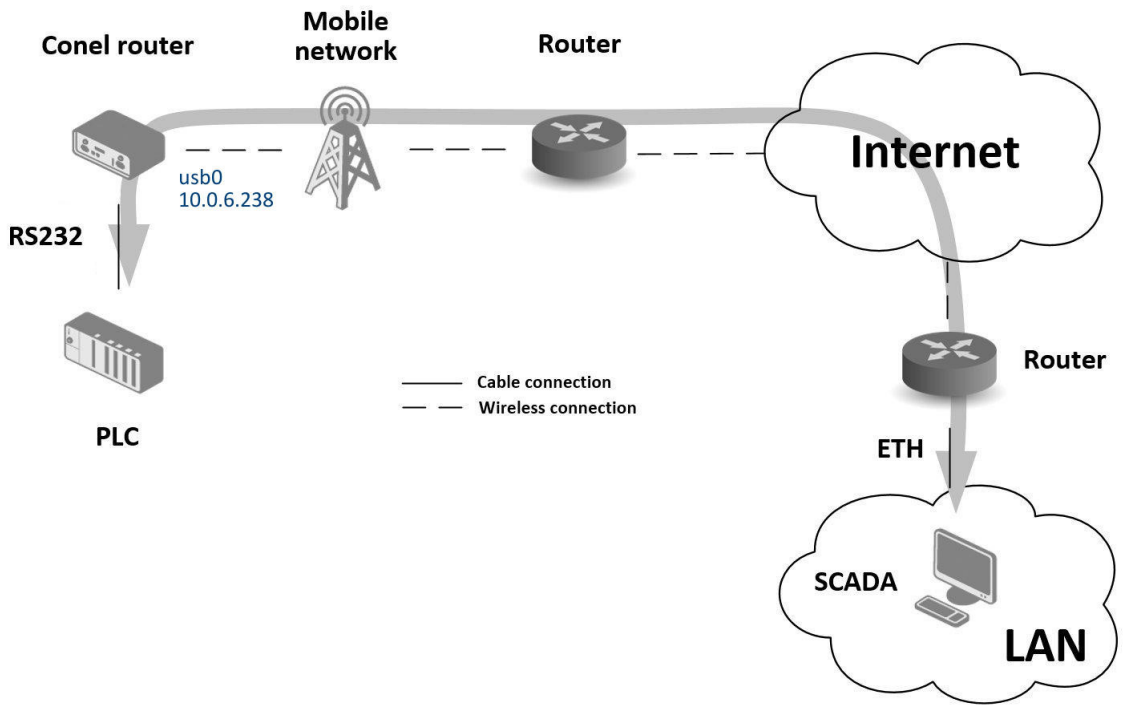
Konfigurace OpenVPN Konfigurace připojení k OpenVPN tunelu je dostupná pod položkou *OpenVPN* v sekci *Configuration*. Zde je vybrán první ze dvou tunelů a ten je nutno povolit zaškrtnutím *Create 1st OpenVPN tunnel*, viz obr. 89. Zde je nutno vyplnit protokol a port (dle údajů o protějším konci tunelu nebo OpenVPN serveru). Dále veřejnou IP adresu protějšího konce tunelu a vzdálenou podsíť včetně masky (není nutné). Důležitými položkami jsou *Local* a *Remote Interface IP Address*, kam se vyplňují rozhraní konců tunelu. V tomto případě byl znám sdílený klíč (*pre-shared secret*), který je nutno nastavit pod položkou *Authentication Mode* a samotný klíč vložit do pole *Pre-shared Secret*. Nastavení je nutno potvrdit kliknutím na tlačítko *Apply*. Pro podrobnější nastavení viz kapitola 4.10 nebo aplikační příručku [5].



Obrázek 89: Zabezpečené propojení sítí – konfigurace OpenVPN

Pod položkou *Network* v sekci *Status* lze ověřit aktivované rozhraní tun0 s nastavenými adresami konců tunelu. Úspěšné spojení přes tunel lze ověřit v *System Logu*, kde by mělo být vypsáno `Initialization Sequence Completed`. Nyní by měly být sítě propojeny, což lze také ověřit např. programem `ping` mezi IP adresami konců tunelu (po připojení do konzole routeru přes SSH).

7.4 Serial Gateway



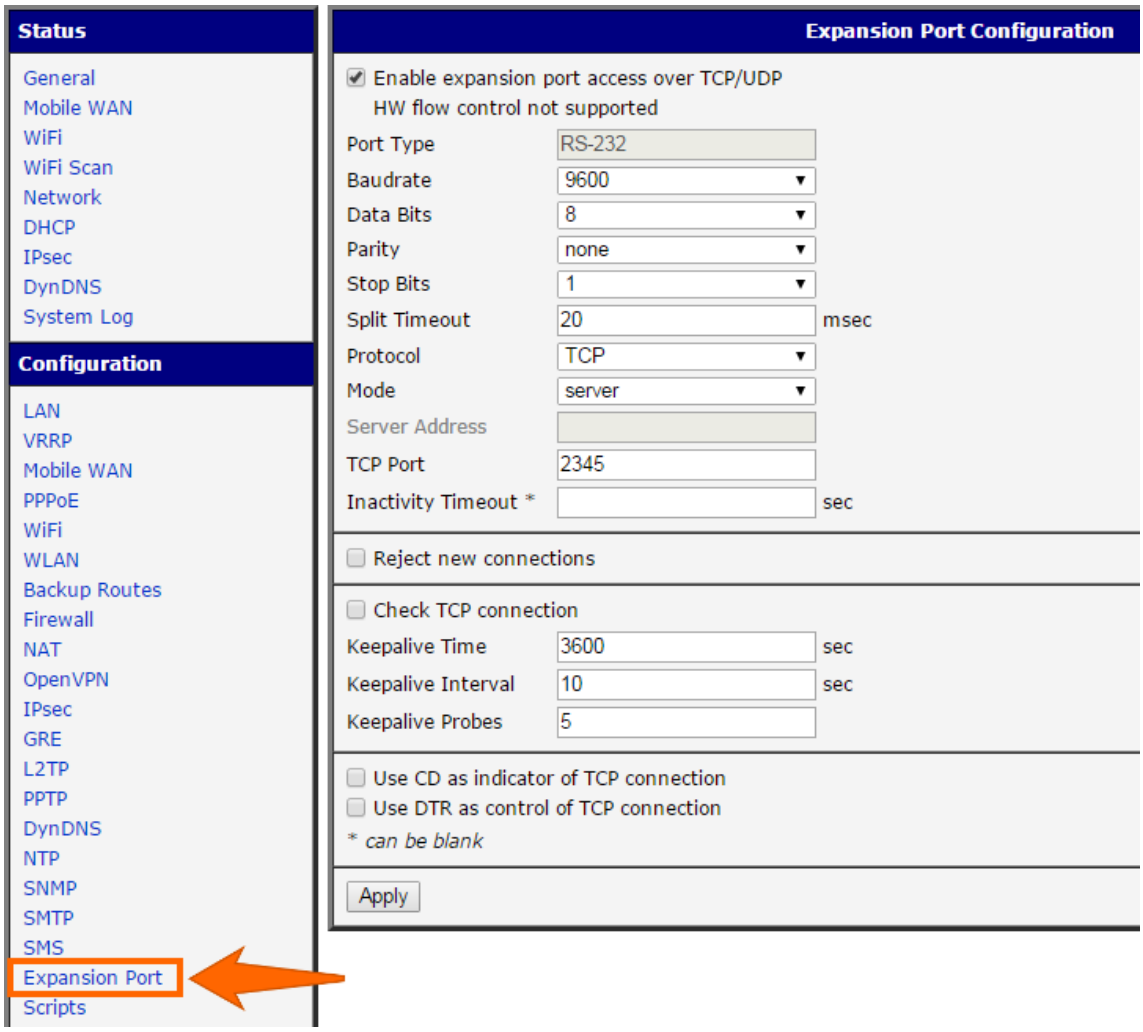
Obrázek 90: Serial Gateway – topologie příkladu

Pomocí Serial Gateway (sériové brány) lze umožnit zařízením se sériovým rozhraním přístup do internetu nebo do jiné sítě, aby mohla tato zařízení (měřidla, PLC apod.) odesílat a přijímat data. Situace je naznačena na obr. 90. V této situaci je nutné, aby Advantech B+B SmartWorx router disponoval rozhraním RS232.

Nastavení funkce se pak provádí pod položkami *Mobile WAN* a *Expansion Port* v sekci *Configuration*. Ve zde popsané situaci router disponuje rozhraním RS232.

Konfigurace Mobile WAN Konfigurace mobilního připojení je v tomto případě stejná jako v předchozích situacích. Stačí zasunout SIM kartu do routeru (na pozici SIM1) a připojit anténu ke konektoru ANT. Žádná další konfigurace není nutná (závisí na SIM kartě), případně viz kap. 4.3.1.

Konfigurace Expansion Port Konfigurace rozhraní RS232 je přístupná pod položkou *Expansion Port*, viz obr. 91. Zde je nutné port aktivovat zaškrtnutím *Enable expansion port 1 access over TCP/UDP*. Je možné upravit parametry sériové komunikace (v tomto případě není nutné). Důležité jsou položky *Protocol*, *Mode* a *Port*, kde se nastavují parametry komunikace dál do sítě nebo internetu. V této situaci byl zvolen protokol TCP a router bude pracovat v režimu serveru, který bude naslouchat na TCP portu 2345. Nastavení je nutné potvrdit tlačítkem *Apply*.



Obrázek 91: Serial Gateway – konfigurace Expansion Port

Ke komunikaci se sériovým zařízením (PLC) se nyní z PC (v obr. 90 označeným SCADA) stačí připojit jako TCP klient na IP adresu 10.0.6.238, port 2345 (veřejná IP použité SIM karty, odpovídá rozhraní usb0 routeru). Zařízení spolu nyní mohou komunikovat. Kontrola spojení je možná v *System Logu* (sekce *Status*), kde bude při úspěšném sestavení TCP spojení zpráva *TCP connection established* apod.

8. Seznam pojmů a zkratek

Backup Routes Tato funkce umožňuje uživateli 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.

DHCP Dynamic Host Configuration Protocol (DHCP) je název protokolu z rodiny TCP/IP nebo označení odpovídajícího DHCP serveru či klienta. Používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě. DHCP server přiděluje počítačům pomocí DHCP protokolu zejména IP adresu, masku sítě, implicitní bránu a adresu DNS serveru. Platnost přidělených údajů je omezená, proto je na počítači spuštěn DHCP klient, který jejich platnost prodlužuje.

DHCP client Dotazuje se DHCP serveru na síťovou konfiguraci.

DHCP server Odpovídá na dotazy DHCP klientů ohledně síťové konfigurace.

Digitální certifikát Digitální certifikát je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč, který vydává certifikační autorita. Uchovává se ve formátu X.509, který (kromě jiného) obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu (tvůrci digitálního podpisu, tj. certifikační autoritě). Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení (HTTPS, VPN atp.). Na základě principu přenosu důvěry je možné důvěřovat neznámým certifikátům, které jsou podepsány důvěryhodnou certifikační autoritou.

DNS Domain Name System (DNS) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefonii) a slouží dnes de fakto jako distribuovaná databáze síťových informací. Systém DNS umožňuje efektivně udržovat decentralizované databáze doménových jmen a jejich překlad na IP adresy. Stejně tak zajišťuje zpětný překlad IP adresy na doménové jméno – PTR záznam.

DynDNS client Služba DynDNS umožňuje vzdálený přístup k routeru pomocí snadno zapamatovatelného uživatelského jména (hostname). DynDNS klient sleduje IP adresu routeru a aktualizuje ji vždy, jakmile se změní.

GRE Generic Routing Encapsulation (GRE) je protokol ze skupiny TCP/IP (transportní vrstva, IP protokol číslo 47) určený k zapouzdření paketů jednoho protokolu do protokolu jiného. Používá se ve VPN, k přenosu IPv6 paketů v síti IPv4 a k tunelování obecně. Protokol je bezstavový, původně jej navrhla firma Cisco a je definován v RFC 2784.

HTTP Hypertext Transfer Protocol (HTTP) je internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. Samotný protokol HTTP neumožňuje šifrování ani zabezpečení integrity dat. Pro zabezpečení HTTP se často používá TLS spojení nad TCP. Toto použití je označováno jako HTTPS.
Hypertext je způsob strukturování textu, který není lineární. Obsahuje tzv. hyperlinky neboli (hypertextové) odkazy. Rovněž odkazuje i na jiné informace v systému a umožňuje snadné publikování, údržbu a vyhledávání těchto informací. Nejznámějším takovým systémem je World Wide Web (WWW).

HTTPS Hypertext Transfer Protocol Secure (HTTPS) je nadstavba síťového protokolu HTTP,

která umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany. HTTPS používá protokol HTTP, přičemž přenášená data jsou šifrována pomocí SSL nebo TLS a standardní port na straně serveru je 443.

IP adresa IP adresa je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol). V současné době je nejrozšířenější verze IPv4, která používá 32bitové adresy zapsané dekadicky po jednotlivých oktetech (osmicích bitů). Z důvodu nedostatku IP adres je postupně nahrazován protokolem IPv6, který používá 128-bitové IP adresy zapsané hexadecimálně.

IP masquerade Jedná se o typ překladu adres (viz NAT).

IP masquerading viz NAT.

IPsec Internet Protocol Security (IPsec) je název bezpečnostního rozšíření IP protokolu založené na autentizaci a šifrování každého IP datagramu. Router umožňuje zvolit typ zapouzdření (tunnel nebo transport), IKE mód (main nebo aggressive), IKE algoritmus, IKE šifrování, ESP algoritmus, ESP šifrování and mnohem více. Lze nakonfigurovat až čtyři různé tunely.

IPv4 Internet Protocol version 4 (IPv4) je čtvrtá revize IP (Internet Protocol) a zároveň jeho první verze, která se masivně rozšířila. Spolu s IPv6 vytvářejí základ pro komunikaci v rámci sítě Internet. IPv4 je popsána IETF v RFC 791 (září 1981), které nahradilo RFC 760. Jedná se o datově orientovaný protokol, který je používán v sítích s přepojováním paketů (např. Ethernet). Jde o protokol přepravující data bez záruky, tj. negarantuje ani doručení ani zachování pořadí ani vyloučení duplicit. Zajištění těchto záruk je ponecháno na vyšší vrstvě, kterou představuje protokol TCP. Stejně tak je na vyšší vrstvě ponechána kontrola integrity dat, protože IPv4 datagram nese pouze informaci o kontrolním součtu hlavičky datagramu se služebními údaji.

IPv6 Internet Protocol version 6 (IPv6) je označení nastupujícího protokolu pro komunikaci v současném Internetu (resp. v počítačových sítích, které Internet vytvářejí). IPv6 nahrazuje dosluhující protokol IPv4. Přináší zejména masivní rozšíření adresního prostoru (tj. možnost přidělit všem zařízením jejich vlastní IPv6 adresu) a zdokonalení schopnosti přenášet vysokorychlostně data.
IPv6 adresy se zapisují kompaktněji v šestnáctkové soustavě a jednotlivé dvojice bajtů (čtveřice šestnáctkových číslic) se pro větší názornost oddělují dvojtečkami. Takže IPv6 adresa může vypadat třeba takto:
2001:0db8:85a3:0042:1000:8a2e:0370:7334.
Aby se zápis ještě o něco zkrátil, lze v jednotlivých čtveřicích vynechávat počáteční nuly. Pokud se vyskytne několik po sobě jdoucích nulových skupin, lze je nahradit dvojicí dvojteček. Ta se však v zápisu každé adresy smí objevit jen jednou, aby byl jednoznačný.

L2TP Layer 2 Tunneling Protocol (L2TP) je tunelovací protokol pro podporu VPN. Sám o sobě neobsahuje žádné šifrování, pouze vytváří tunel. Komunikuje na UDP portu 1701. Často se používá dohromady s IPsec, který zajišťujte důvěrnost (šifrování) a autentizaci.

LAN Local area network (LAN) označuje počítačovou síť, která pokrývá malé geografické území (např. domácnosti, malé firmy). Přenosové rychlosti jsou vysoké, řádově Gb/s. Nejrozšířenějšími technologiemi v dnešních LAN sítích jsou Ethernet a WiFi (nebo také WLAN).

NAT Network Address Translation (NAT) upravuje síťový provoz přes router přepisem zdrojové nebo cílové IP adresy, případně i hlaviček protokolů vyšší vrstvy. NAT je důsledkem omezeného počtu veřejných IP adres. Jelikož adresu z vnějšího rozsahu nemůže mít každý, byl vymyšlen princip, který dovoluje za jednu adresu „skrýt“ celou vnitřní síť, nehledě na její rozsah.
Klient vyšle požadavek na bránu vnitřní sítě. Router pakety zachytí, změní jejich IP adresu na svou vnější a označí je tak, že je odešle z náhodného TCP portu. Poté si do tabulky zapíše,

který port zvolil a který klient k němu patří. Při přijetí odpovědi provede router reverzní akci a pakety vrátí klientovi. Pro klienta je tedy celý proces transparentní a komunikaci nijak neovlivňuje. Servery „na druhé straně“ také o ničem neví a bez potíží odpovídají samotnému překladači.

NAT-T NAT traversal (NAT-T) je obdobou překladu adres (NAT), jež přidává UDP hlavičku, která obaluje ESP hlavičku (tzn. vkládá se mezi ESP hlavičku a vnější IP hlavičku). Toto dáva stroji provozujícím NAT-T UDP hlavičku obsahující UDP porty, které se použijí pro adresaci klienta.

NTP Network Time Protocol (NTP) je protokol pro synchronizaci vnitřních hodin po paketové síti s proměnným zpožděním. Tento protokol zajišťuje, aby všechna zařízení v síti měla stejný a přesný čas. Byl obzvláště navržen tak, aby odolával následku proměnlivého zpoždění v doručování paketů.

OpenVPN OpenVPN vytváří šifrovaný VPN tunel mezi hostitelskými stanicemi. Umožňuje ověřit navazované spojení pomocí sdíleného klíče (anglicky pre-shared key), digitálního certifikátu nebo uživatelského jména a hesla. V nastavení multiklient-server je vydán serverem pro klienty autentizační certifikát, který používá elektronický podpis a certifikační autoritu. S routery Advantech B+B SmartWorx je možné vytvořit až čtyři různé tunely.

PAT Port and Address Translation (PAT) je podmnožina NAT a těsně souvisí s konceptem překladu síťových adres. Více viz NAT.

Port Síťový port je speciální číslo (1 až 65535), které slouží v počítačových sítích při komunikaci pomocí protokolů TCP a UDP k rozlišení aplikace v rámci počítače.

PPTP Point-to-Point Tunneling Protocol (PPTP) je způsob realizace Virtuální privátní sítě (VPN), který pracuje na základě vytváření běžné PPP relace s GRE (Generic Routing Encapsulation) zapouzdřením. Druhá relace na TCP portu 1723 je používána pro zahájení a řízení GRE relace. Obvyklými náhradami jsou L2TP či IPsec.

RADIUS RADIUS (Remote Authentication Dial In User Service, česky Uživatelská vytáčená služba pro vzdálenou autentizaci) je AAA protokol (authentication, authorization and accounting, česky autentizace, autorizace a účtování) používaný pro přístup k síti nebo pro IP mobilitu.

Router Router (směrovač) je aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI (síťová vrstva) a je využíváno v lokálních sítích LAN i na Internetu, kde jsou dnes směrovány zejména IP datagramy. Síťová infrastruktura mezi odesílatelem a adresátem paketu může být velmi složitá, a proto se směrování zpravidla nezabývá celou cestou paketu, ale řeší vždy jen jeden krok, tj. komu datagram předat jako dalšímu.

SFTP Zkratka SFTP znamená SSH File Transfer Protocol nebo Secure FTP. Protokol byl navržený jako rozšíření SSH pro přenos souborů, dokáže ale pracovat i nad protokolem jiným, který se kromě šifrování musí postarat také o autorizaci.

SMTP Simple Mail Transfer Protocol (SMTP) je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem. SMTP funguje nad protokolem TCP a běžně používá port TCP/25.

SMTPS Simple Mail Transfer Protocol Secure (SMTPS) je zabezpečená varianta SMTP, jež využívá protokol SSL/TLS. Umožňuje provést autentizaci jak odesílatele, tak příjemce a zároveň zajišťuje zachování integrity a důvěrnosti přenášených zpráv.

SNMP Simple Network Management Protocol (SNMP) umožňuje průběžný sběr dat pro po-

třeby správy sítě a jejich následné vyhodnocování. Protokol se vyvíjel postupně ve třech verzích: první verze (SNMPv1) zajišťuje základní funkcionalitu SNMP, druhá (SNMPv2) obsahuje navíc autentizaci a třetí (SNMPv3) šifrování (zabezpečení). Protokol SNMP rozlišuje mezi stranou monitorovanou (hlídaný systém) a monitorovací (sběrna dat). Tyto strany mohou běžet buď odděleně na různých fyzických strojích, nebo v rámci jednoho stroje. Na monitorované straně je spuštěn agent a na straně monitorovací manager. Na straně monitorované jsou operativně shromažďovány informace o stavu zařízení. Manager vznáší požadavky agentovi, zpravidla na zaslání požadovaných informací. Agent zajišťuje realizaci reakcí na požadavky managera. Získaný obsah zpráv se na straně monitorovací může dále různým způsobem zpracovávat (tabulky, grafy, . . .).

SSH Secure Shell (SSH) umožňuje bezpečnou komunikaci mezi dvěma zařízeními, která se využívá pro zprostředkování přístupu k příkazovému řádku, kopírování souborů a též jakýkoliv obecný přenos dat (s využitím síťového tunelování). Zabezpečuje autentizaci obou účastníků komunikace, transparentní šifrování přenášených dat, zajištění jejich integrity a volitelnou bezeztrátovou kompresi. Server standardně naslouchá na portu TCP/22.

TCP Transmission Control Protocol (TCP) je nejpoužívanějším protokolem transportní vrstvy v sadě protokolů TCP/IP používaných v síti Internet. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou obousměrně přenášet data. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí. TCP také umožňuje rozlišovat a rozdělovat data pro více aplikací (například webový server a emailový server) běžících na stejném počítači. TCP využívá mnoho populárních aplikačních protokolů a aplikací na internetu, včetně WWW, e-mailu a SSH.

UDP User Datagram Protocol (UDP) je jeden ze sady protokolů internetu. Na rozdíl od protokolu TCP nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů, nebo zda některý datagram nebude doručen vícekrát. Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LAN). Jeho bezstavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a není vhodné, aby se ztrácel čas novým odesíláním (starých) nedoručených zpráv.

URL Uniform Resource Locator (URL) je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací (ve smyslu dokument nebo služba) na Internetu. URL definuje doménovou adresu serveru, umístění zdroje na serveru a protokol, kterým je možné ke zdroji přistupovat. Příkladem typické URL může být `http://www.example.com/index.html`, kde je indikován protokol (http), hostname (www.example.com) a jméno souboru (index.html).

VPN Virtual private network (VPN) slouží k propojení několika zařízení prostřednictvím (veřejné) nedůvěryhodné sítě. Lze tak snadno dosáhnout stavu, kdy spojená zařízení budou mezi sebou moci komunikovat, jako kdyby byla propojena v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné.
Tímto způsobem se lze např. připojit odkudkoliv z Internetu do firemního intranetu. Ve firemní síti se nejprve zprovozní VPN server, zajistí se připojení k Internetu, ke kterému se pak připojují VPN klienti z jakéhokoliv místa, které je také k Internetu připojeno. VPN server plní funkci síťové brány, která zprostředkovává připojení, zajišťuje zabezpečení a šifrování veškeré komunikace.

VPN server Více viz VPN.

VPN tunnel Více viz VPN.

VRRP Virtual Router Redundancy Protocol (VRRP) je technika, pomocí které lze přenést povinnosti routování z jednoho routeru na jiný (záložní), v případě, že první router vypoví službu.

WAN Wide Area Network (WAN) je počítačová síť, která pokrývá rozlehlé geografické území. Sítě WAN jsou využívány pro spojení lokálních sítí (LAN) nebo dalších typů sítí, takže uživatelé z jednoho místa mohou komunikovat s uživateli a počítači na místě jiném. Tyto sítě bývají budovány na pronajatých linkách (leased lines). Častěji se však sítě WAN budují na metodách přepojování okruhů (circuit switching) nebo přepojování paketů (packet switching). Síťové služby používají pro přenos a adresaci protokol TCP/IP.

X.509 V kryptografii je X.509 standard pro systémy založené na veřejném klíči (PKI, public key infrastructure) pro jednoduché podepisování. X.509 specifikuje mezi jiným formát certifikátů, seznamy odvolaných certifikátů (CRL, certificate revocation list), parametry certifikátů a metody kontroly platností certifikátů.

9. Index

M

N

O

P

R

S

T

U

V

W

Z

10. Doporučená literatura

[1]	Advantech B+B SmartWorx:	**Commands and Scripts for v2 and v3 Routers**, Application Note
[2]	Advantech B+B SmartWorx:	**SmartCluster**, Application Note
[3]	Advantech B+B SmartWorx:	**R-SeeNet**, Aplikační příručka
[4]	Advantech B+B SmartWorx:	**R-SeeNet Admin**, Aplikační příručka
[5]	Advantech B+B SmartWorx:	**OpenVPN tunel**, Aplikační příručka
[6]	Advantech B+B SmartWorx:	**IPsec tunel**, Aplikační příručka
[7]	Advantech B+B SmartWorx:	**GRE tunel**, Aplikační příručka
[8]	Advantech B+B SmartWorx:	**SNMP Object Identifier**, Aplikační příručka
[9]	Advantech B+B SmartWorx:	**AT příkazy**, Aplikační příručka
[10]	Advantech B+B SmartWorx:	**Programming of User Modules**, Application Note