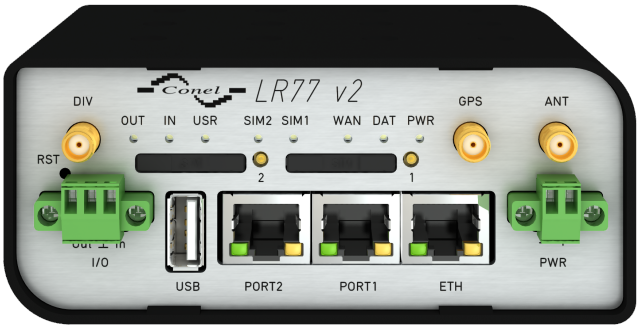
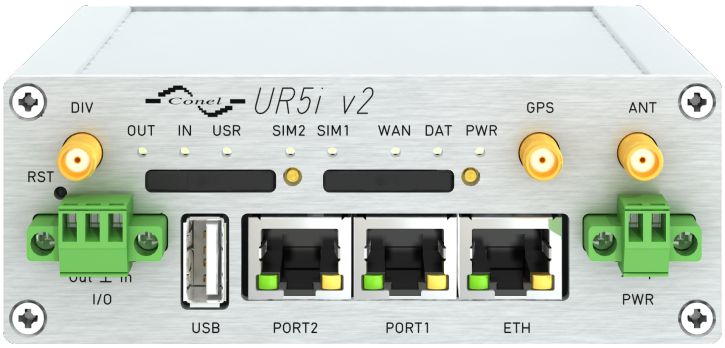
Bezdrátové průmyslové

v2 Routery

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.

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

1 Konfigurace přes web **2**

1.1 Zabezpečený přístup do webové konfigurace . . . 3

2 Status **5**

2.1 General Status . . . 5
2.1.1 Mobile Connection . . . 5
2.1.2 Primary LAN, Secondary LAN, WiFi . . . 5
2.1.3 Peripheral Ports . . . 6
2.1.4 System Information . . . 6
2.2 Mobile WAN Status . . . 7
2.3 WiFi . . . 10
2.4 WiFi Scan . . . 11
2.5 Network Status (Síťové informace) . . . 13
2.6 DHCP Status . . . 15
2.7 IPsec Status . . . 16
2.8 DynDNS Status . . . 17
2.9 Systémový log . . . 18

3 Konfigurace **20**

3.1 LAN Configuration . . . 20
3.2 VRRP Configuration . . . 29
3.3 Mobile WAN . . . 32
3.3.1 Konfigurace připojení do mobilní sítě . . . 32
3.3.2 Konfigurace DNS adres . . . 34
3.3.3 Konfigurace kontroly spojení s mobilní sítí . . . 34
3.3.4 Konfigurace datového limitu . . . 35
3.3.5 Konfigurace přepínání mezi SIM kartami . . . 35
3.3.6 Konfigurace Dial-In přístupu . . . 38
3.3.7 Konfigurace PPPoE bridge mode . . . 38
3.4 Konfigurace PPPoE . . . 41
3.5 WiFi konfigurace . . . 42
3.6 Konfigurace WLAN . . . 49
3.7 Backup Routes . . . 51
3.8 Konfigurace firewallu . . . 54
3.9 NAT Configuration . . . 58
3.10 Konfigurace OpenVPN tunelu . . . 63
3.11 Konfigurace IPsec tunelu . . . 68
3.12 Konfigurace GRE tunelu . . . 76
3.12.1 Příklad konfigurace GRE tunelu . . . 77

3.13 Konfigurace L2TP tunelu . . . 79
3.13.1 Příklad konfigurace L2TP tunelu . . . 80
3.14 Konfigurace PPTP tunelu . . . 81
3.14.1 Příklad konfigurace PPTP tunelu . . . 82
3.15 Services . . . 83
3.15.1 DynDNS . . . 83
3.15.2 FTP . . . 84
3.15.3 HTTP . . . 85
3.15.4 NTP . . . 86
3.15.5 SNMP . . . 87
3.15.6 SMTP . . . 93
3.15.7 SMS . . . 95
3.15.8 SSH . . . 103
3.15.9 Telnet . . . 104
3.16 Konfigurace volitelného portu . . . 105
3.17 Konfigurace USB portu . . . 109
3.18 Skripty (Scripts) . . . 113
3.18.1 Startup Script . . . 113
3.18.2 Up/Down Script . . . 114
3.19 Konfigurace automatické aktualizace . . . 115

4 Přizpůsobení 118

4.1 Správa uživatelských modulů . . . 118

5 Administrace 120

5.1 Uživatelé . . . 120
5.2 Změna profilu . . . 121
5.3 Změna přístupového hesla . . . 122
5.4 Nastavení vnitřních hodin . . . 122
5.5 Nastavení SMS centra . . . 123
5.6 Odemknutí SIM karty . . . 123
5.7 Odblokování SIM karty . . . 124
5.8 Poslání SMS zprávy . . . 125
5.9 Zálohování konfigurace . . . 125
5.10 Obnovení konfigurace . . . 125
5.11 Aktualizace firmware . . . 126
5.12 Reboot . . . 127

6 Konfigurace přes Telnet 128

7 Seznam pojmů a zkratek 130

8 Index 135

9 Doporučená literatura 138

Seznam obrázků

1 Webové rozhraní . . . 2
2 Mobile WAN status . . . 9
3 WiFi Status . . . 10
4 WiFi Scan . . . 12
5 Network Status . . . 14
6 DHCP Status . . . 15
7 IPsec Status . . . 16
8 DynDNS Status . . . 17
9 Systémový log . . . 18
10 Příklad spuštění programu syslogd s volbou -R . . . 19
11 Příklad 1 – Topologie sítě s dynamickým DHCP Server . . . 23
12 Příklad 1 – Konfigurace na stránce LAN . . . 24
13 Příklad 2 – Topologie sítě se statickým i dynamickým DHCP serverem . . . 25
14 Příklad 2 – Konfigurace na stránce LAN . . . 26
15 Příklad 3 – Topologie sítě . . . 27
16 Příklad 3 – Konfigurace na stránce LAN . . . 28
17 Topologie k příkladu konfigurace VRRP . . . 30
18 Příklad konfigurace VRRP – Hlavní router . . . 30
19 Příklad konfigurace VRRP – Záložní router . . . 31
20 Mobile WAN konfigurace . . . 39
21 Příklad 1 – Mobile WAN konfigurace . . . 40
22 Příklad 2 – Mobile WAN konfigurace . . . 40
23 Konfigurace PPPoE . . . 41
24 Konfigurace WiFi . . . 48
25 WLAN konfigurace . . . 50
26 Backup Routes . . . 51
27 Konfigurace firewallu . . . 56
28 Topologie příkladu nastavení firewallu . . . 57
29 Příklad nastavení firewallu . . . 57
30 Příklad 1 – Topologie konfigurace NAT . . . 59
31 Příklad 1 – NAT konfigurace . . . 60
32 Příklad 2 – Topologie konfigurace NAT . . . 61
33 Příklad 2 – NAT konfigurace . . . 61
34 Konfigurace OpenVPN tunelu . . . 66
35 Topologie příkladu konfigurace OpenVPN tunelu . . . 67
36 Konfigurace IPsec tunelu . . . 74
37 Topologie příkladu konfigurace IPsec tunelu . . . 75
38 GRE Tunnel Configuration . . . 77
39 Topologie příkladu konfigurace GRE tunelu . . . 77
40 Konfigurace L2TP tunelu . . . 79

41 Topologie příkladu konfigurace L2TP tunelu . . . 80
42 Konfigurace PPTP tunelu . . . 81
43 Topologie příkladu konfigurace PPTP tunelu . . . 82
44 Příklad nastavení DynDNS . . . 83
45 Povolení FTP serveru . . . 84
46 Konfigurace HTTP a HTTPS služeb . . . 85
47 Příklad nastavení NTP . . . 86
48 Základní struktura OID . . . 89
49 Příklad SNMP konfigurace . . . 91
50 Příklad MIB prohlížeče . . . 92
51 Příklad konfigurace SMTP klienta . . . 93
52 Příklad 1 – Konfigurace SMS . . . 99
53 Příklad 2 – Konfigurace SMS . . . 100
54 Příklad 3 – Konfigurace SMS . . . 101
55 Příklad 4 – Konfigurace SMS . . . 102
56 Konfigurace SSH služby . . . 103
57 Povolení služby Telnet . . . 104
58 Konfigurace volitelného portu . . . 107
59 Příklad nastavení komunikace z Ethernetu na sériovou linku . . . 108
60 Příklad konfigurace sériového rozhraní . . . 108
61 Konfigurace USB . . . 111
62 Příklad 1 – nastavení USB portu . . . 111
63 Příklad 2 – nastavení USB portu . . . 112
64 Příklad Startup scriptu . . . 113
65 Příklad Up/Down skriptu . . . 114
66 Příklad automatické aktualizace 1 . . . 116
67 Příklad automatické aktualizace 2 . . . 117
68 User modules . . . 118
69 Přidány uživatelské moduly . . . 118
70 Users . . . 121
71 Změna profilu . . . 121
72 Změna přístupového hesla . . . 122
73 Nastavení vnitřních hodin . . . 122
74 Nastavení SMS centra . . . 123
75 Odemknutí SIM karty . . . 123
76 Odblokování SIM karty . . . 124
77 Poslání SMS zprávy . . . 125
78 Obnovení konfigurace . . . 125
79 Aktualizace firmware . . . 126
80 Reboot . . . 127

Seznam tabulek

1 Mobile Connection . . . 5
2 Peripheral Ports . . . 6
3 System Information . . . 6
4 Mobile Network Information . . . 7
5 Popis jednotlivých období . . . 8
6 Mobile Network Statistics . . . 8
7 Traffic Statistics . . . 9
8 Stavové informace o přístupovém bodu . . . 10
9 Stavové informace o připojených klientech . . . 10
10 Informace o okolních sítích . . . 11
11 Popis rozhranní network status . . . 13
12 Popis informací Network status . . . 14
13 Popis informací DHCP status . . . 15
14 Konfigurace síťového rozhraní . . . 21
15 Konfigurace dynamického DHCP serveru . . . 22
16 Konfigurace statického DHCP serveru . . . 22
17 Konfigurace 802.1X autentikace . . . 22
18 Konfigurace VRRP . . . 29
19 Check connection . . . 29
20 Konfigurace přihlášení do mobilní sítě . . . 33
21 Konfigurace kontroly spojení s mobilní sítí . . . 34
22 Konfigurace datového limitu . . . 35
23 Konfigurace přepínání mezi SIM kartami . . . 36
24 Parametry pro přepínání SIM karet . . . 37
25 Konfigurace Dial-In přístupu . . . 38
26 Konfigurace PPPoE . . . 41
27 Konfigurace WiFi . . . 47
28 Konfigurace WLAN . . . 49
29 Konfigurace DHCP serveru . . . 50
30 Backup Routes Configuration . . . 52
31 Backup Routes . . . 52
32 Filtrování příchozích paketů . . . 54
33 Filtrování forwardingu . . . 55
34 Konfigurace překladu adres (NAT) . . . 58
35 Konfigurace jednotného přeposílání . . . 58
36 Konfigurace vzdáleného přístupu . . . 59
37 Konfigurace OpenVPN tunelu . . . 65
38 Příklad konfigurace OpenVPN tunelu . . . 67
39 Konfigurace IPsec tunelu . . . 70
40 Příklad konfigurace IPsec tunelu . . . 75

41 Konfigurace GRE tunelu . . . 76
42 Příklad konfigurace GRE tunelu . . . 78
43 Konfigurace L2TP tunelu . . . 79
44 Příklad konfigurace L2TP tunelu . . . 80
45 Konfigurace PPTP tunelu . . . 81
46 Příklad konfigurace PPTP tunelu . . . 82
47 Konfigurace DynDNS . . . 83
48 Parametry konfigurace HTTP a HTTPS služeb . . . 85
49 Konfigurace NTP . . . 86
50 Konfigurace SNMP agenta . . . 87
51 Konfigurace SNMPv3 . . . 87
52 Konfigurace SNMP – MBUS . . . 88
53 Konfigurace SNMP – R-SeeNet . . . 88
54 Vnitřní proměnné pro binární vstup a výstup . . . 89
55 Vnitřní proměnné pro CNT port . . . 90
56 Vnitřní proměnné pro M-BUS port . . . 90
57 Konfigurace SMTP klienta . . . 93
58 Konfigurace posílání SMS . . . 95
59 Ovládání pomocí SMS zpráv . . . 96
60 Význam ovládacích SMS . . . 97
61 Posílání/Příjem zpráv na sériovém portu 1 . . . 97
62 Posílání/Příjem zpráv na sériovém portu 2 . . . 97
63 Posílání/Příjem zpráv na zadaném TCP portu . . . 97
64 AT příkazy pro práci s SMS . . . 98
65 Parametry konfigurace SSH služby . . . 103
66 Konfigurace volitelného portu – sériové rozhraní . . . 105
67 Konfigurace volitelného portu – *Check TCP connection* . . . 106
68 Popis signálu CD . . . 106
69 Popis signálu DTR . . . 106
70 Konfigurace USB portu 1 . . . 109
71 Konfigurace USB portu 2 . . . 110
72 Popis signálu CD . . . 110
73 Popis signálu DTR . . . 110
74 Konfigurace automatické aktualizace . . . 115
75 Uživatelské moduly . . . 119
76 Přehled uživatelů . . . 120
77 Přidání nového uživatele . . . 120
78 Telnet příkazy . . . 129

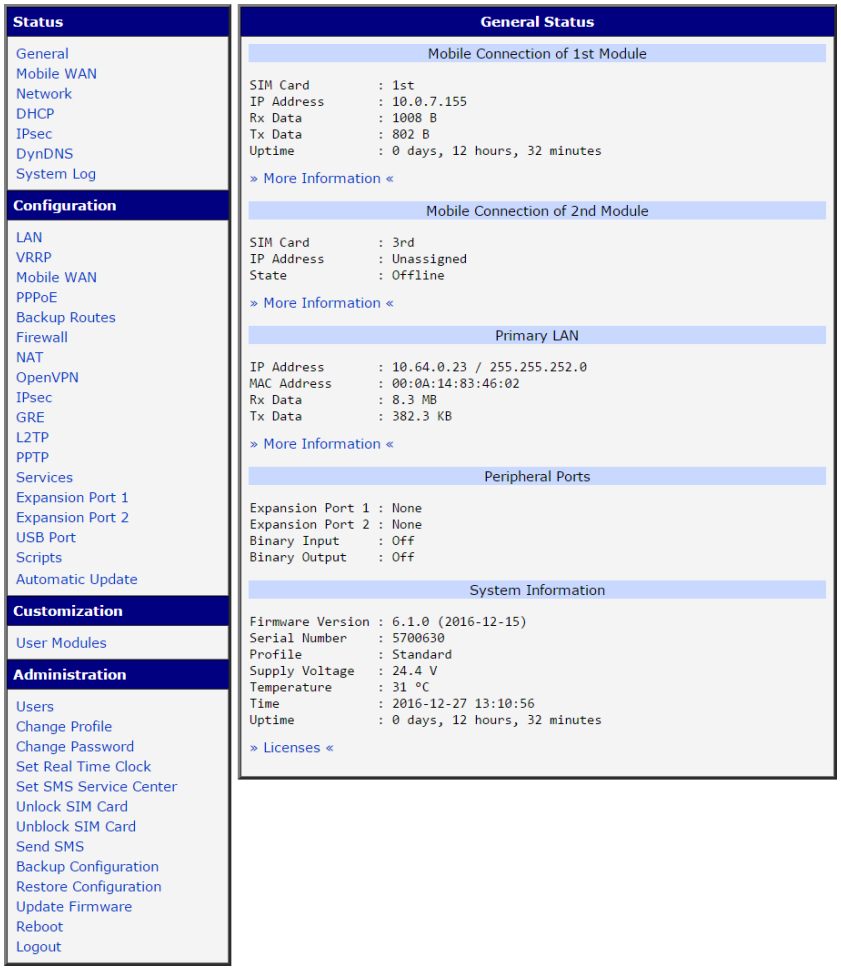
1. Konfigurace přes webový prohlížeč

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

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

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).



Obrázek 1: Webové rozhraní

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

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

1.1 Zabezpečený přístup do webové konfigurace

Do webové konfigurace lze přistoupit i pomocí zabezpečeného protokolu HTTPS.

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

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*), například 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.

2. Status

2.1 General Status

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

2.1.1 Mobile Connection

Položka	Popis
SIM Card	Identifikace SIM karty (*Primary* nebo *Secondary*)
Interface	Definuje síťové rozhraní
Flags	Příznaky daného síťového rozhraní
IP Address	IP adresa daného síťového 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
Tx Overruns	Ztracené odchozí pakety z důvodu přetížení
Uptime	Doba, po kterou je sestavené spojení na mobilní síti

Tabulka 1: Mobile Connection

2.1.2 Primary LAN, Secondary LAN, 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*, *Secondary LAN – eth1*, *WiFi – wlan0*). Zobrazené informace závisí na konfiguraci (viz 3.1 nebo 3.5).

2.1.3 Peripheral Ports

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

Tabulka 2: Peripheral Ports

2.1.4 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, licence ve stylu MIT).

Tabulka 3: System Information

2.2 Mobile WAN Status

Tato položka není dostupná pro routery XR5i v2.

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 a CDMA (Jedná se o poměr přijímaného signálu z pilotního kanálu – EC – vůči celkové úrovni spektrální hustoty, tj. vůči součtu signálů ostatních buněk – IO.) • RSRQ pro technologii LTE (Definováno jako podíl $\frac{N \times RSRP}{RSSI}$) • Pro technologii EDGE 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
ESN	ESN (Electronic Serial Number) modulu (pro CDMA routery)
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*:

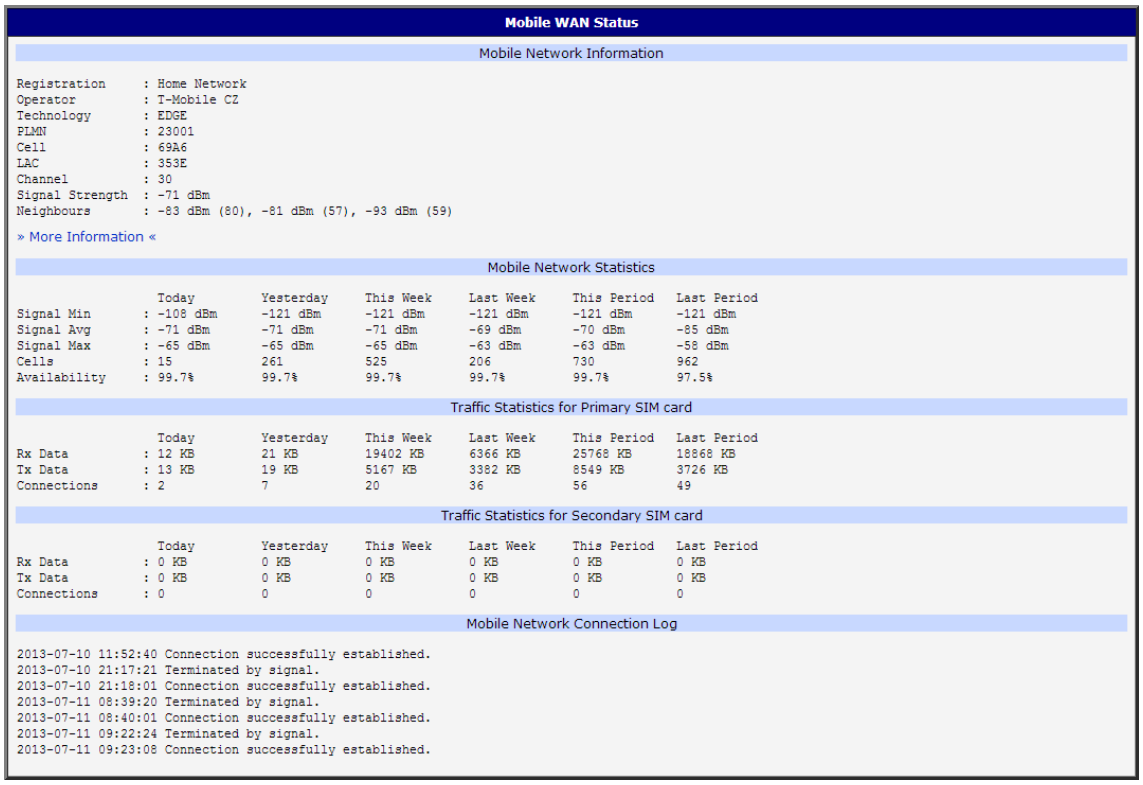
- Dostupnost spojení do mobilní sítě je údaj v procentech, který je počítán poměrem času navázaného spojení do mobilní sítě vůči času, kdy je router zapnutý.
- Po najetí kurzorem na hodnoty maximální nebo minimální síly signálu se zobrazí poslední čas, kdy této síly signálu router dosáhl.

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

2.3 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.

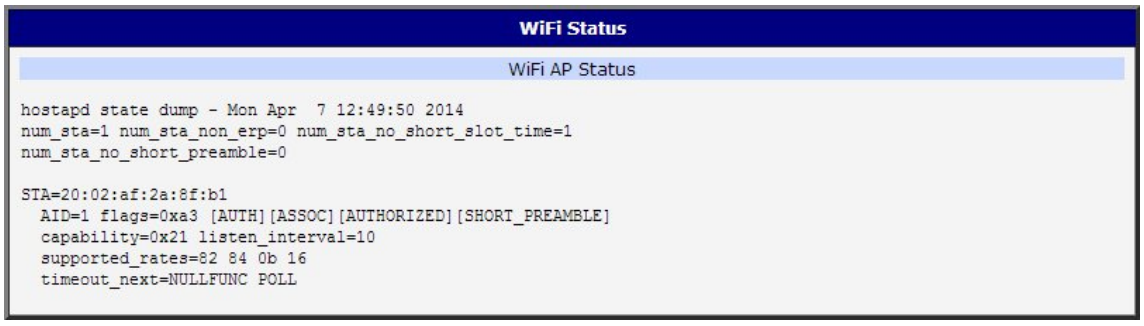
Položka	Popis
hostapd state dump	Čas, ke kterému se statistická data vztahují
num_sta	Počet připojených stanic
num_sta_non_erp	Počet stanic využívající připojení 802.11b v 802.11g BSS
num_sta_no_short_slot_time	Počet stanic nepodporující Short Slot Time
num_sta_no_short_preamble	Počet stanic nepodporující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

2.4 WiFi Scan

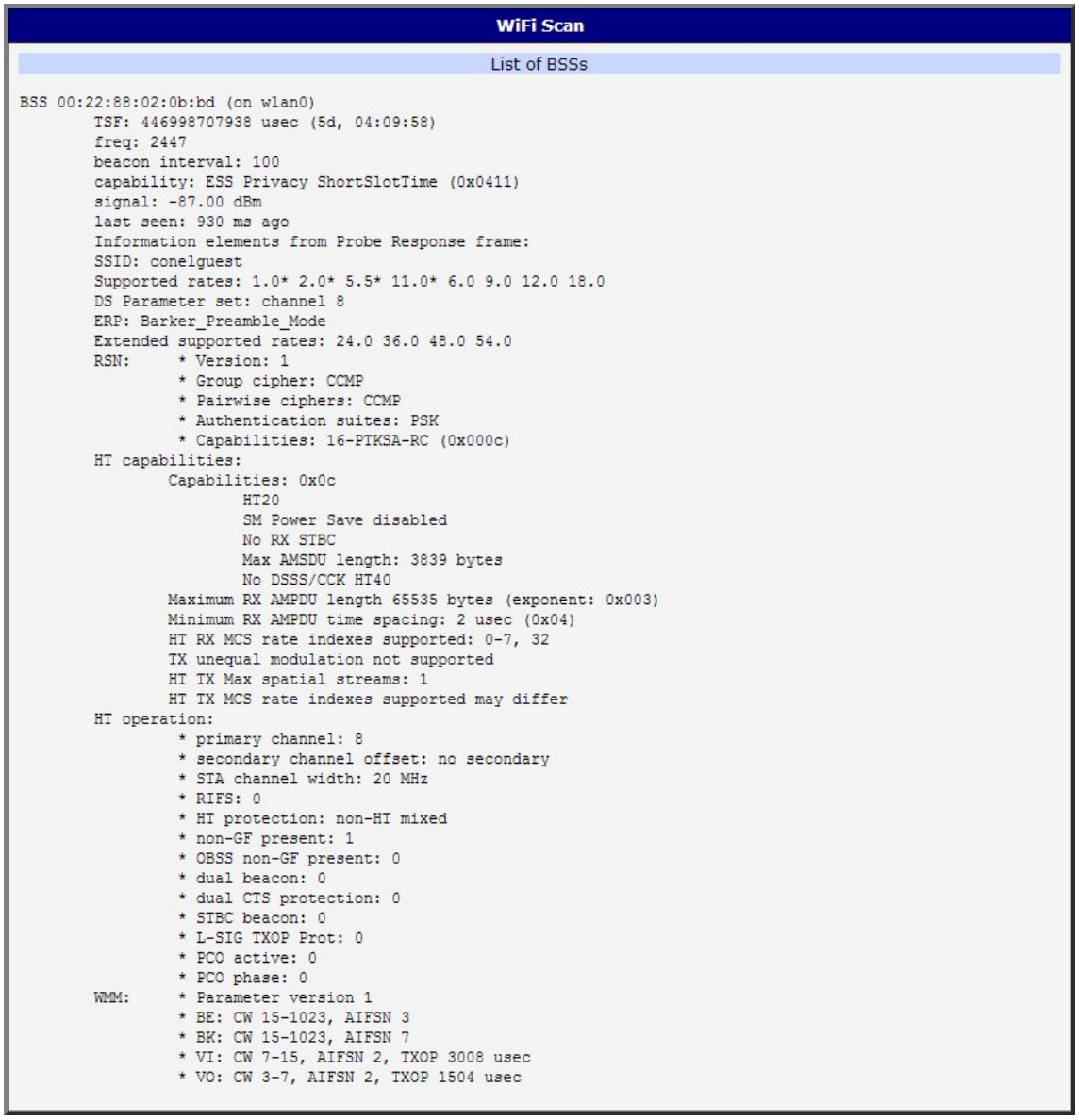
Tato položka je dostupná pouze tehdy, je-li v routeru osazen WiFi modul.

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:



Obrázek 4: WiFi Scan

2.5 Network Status (Síťové informace)

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

Rozhraní	Popis
eth0, eth1	Síťová rozhraní (připojení do ethernetu)
ppp0	Aktivní PPP připojení do mobilní sítě – bezdrátový modul je připojen přes USB rozhraní
wlan0	WiFi rozhraní
tun0	Rozhraní OpenVPN tunelu
ipsec0	Rozhraní IPsec tunelu
gre1	Rozhraní GRE tunelu
usb0	USB rozhraní

Tabulka 11: Popis rozhranní network status

U každého rozhraní jsou pak zobrazeny následující informace:

Položka	Popis
HWaddr	Hardwarová (MAC) adresa síťového rozhraní
inet	Vlastní IP adresa rozhranní
P-t-P	IP adresa druhého konce spojení
Bcast	Všesměrová adresa
Mask	Maska sítě
MTU	Maximální velikost paketu, kterou je prvek schopen přenášet
Metric	Počet směrovačů, přes které musí paket projít
RX	• **packets** – přijaté pakety • **errors** – chybné příchozí pakety • **dropped** – zahozené příchozí pakety • **overruns** – ztracené příchozí pakety z důvodu přetížení • **frame** – chybné příchozí pakety z důvodu chybné velikosti paketu

Pokračování na následující straně

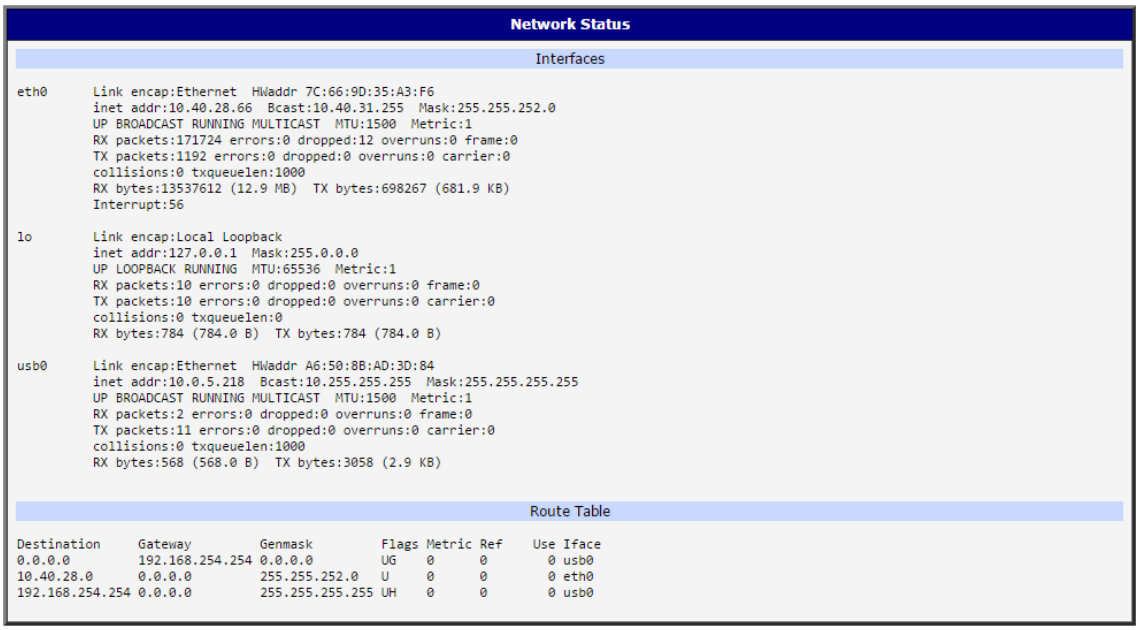
Pokračování z předchozí strany

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 je také zobrazena routovací tabulka.

Pro routery XR5i v2 platí, že rozhranní ppp0 označuje PPPoE spojení.



Obrázek 5: Network Status

2.6 DHCP Status

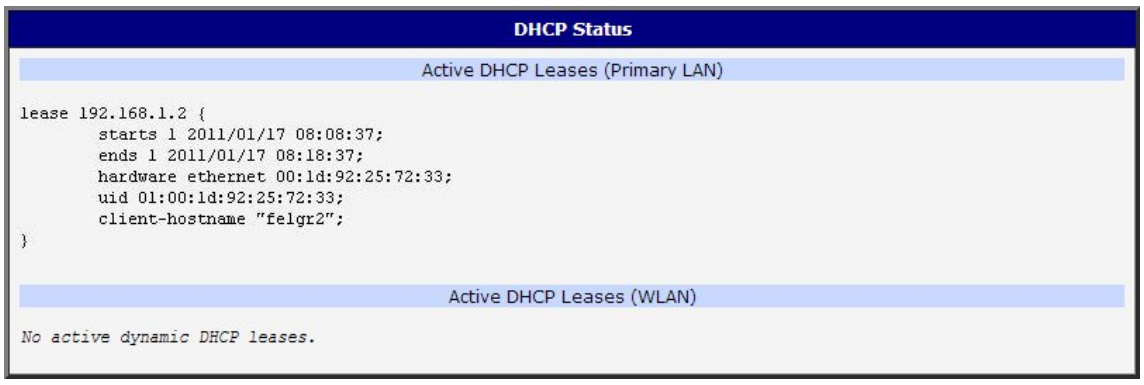
Informace o činnosti DHCP serveru lze vyvolat volbou položky *DHCP status*. DHCP server zajišťuje automatickou konfiguraci zařízení připojených do sítě spravované routerem. DHCP server přiděluje jednotlivým zařízením jejich IP adresu, masku sítě, IP adresu výchozí brány a IP adresu DNS serveru.

Pro každou konfiguraci jsou v okně *DHCP status* zobrazeny následující informace:

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

Tabulka 13: Popis informací DHCP status

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

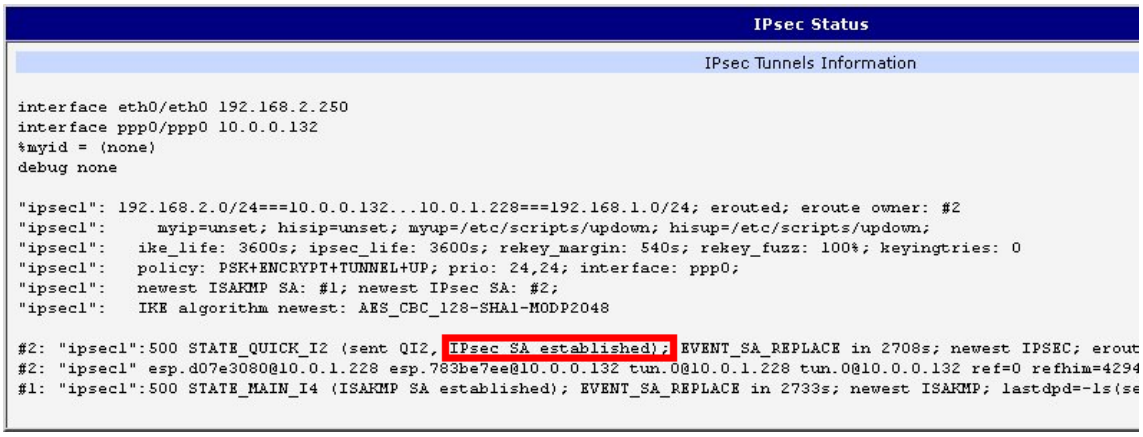


Obrázek 6: DHCP Status

Pozn.: Počínaje firmwarem 4.0.0 se záznamy v okně *DHCP status* dělí do dvou samostatných částí – *Active DHCP Leases (Primary LAN)* a *Active DHCP Leases (WLAN)*.

2.7 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

2.8 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:

- 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.

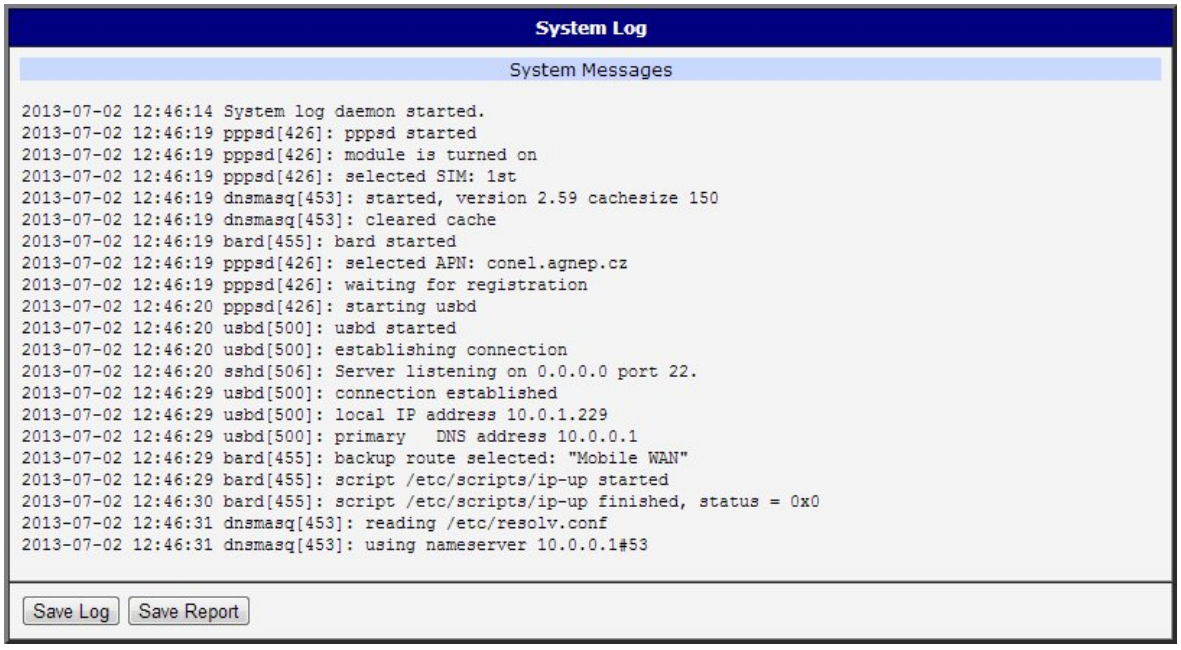
Pro správnou funkci DynDNS musí mít SIM karta routeru přiřazenou veřejnou IP adresu.

2.9 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).

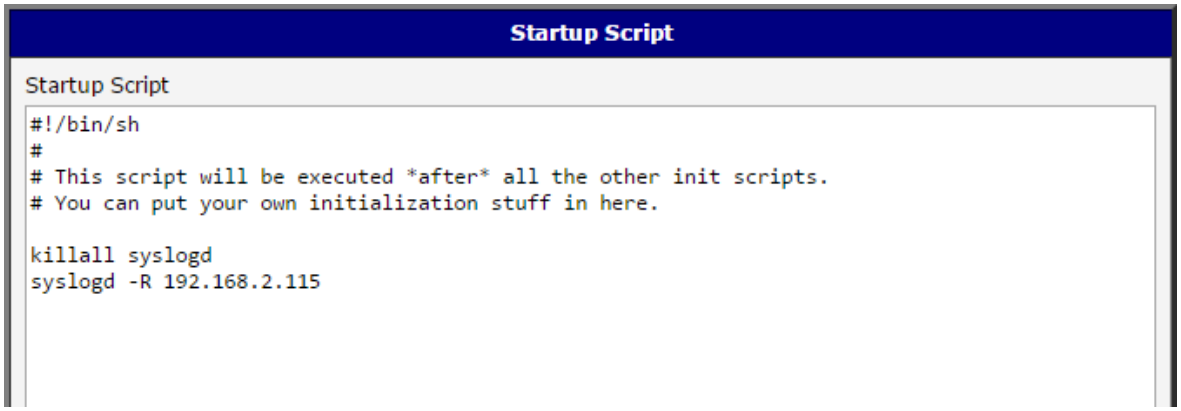
Defaultní velikost systémového logu je 1000 řádků. Po dovršení 1000 řádků se vytvoří nový soubor pro ukládání systémového logu. Po dovršení 1000 řádků v druhém souboru se maže první soubor a vytvoří se místo něho nový.

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

3. Konfigurace

3.1 LAN Configuration

Konfiguraci síťového rozhraní lze vyvolat volbou položky *LAN* v sekci *Configuration*, přičemž je rozdělena do dvou samostatných formulářů. Stránka *Primary* je určena pro konfiguraci primárního ethernetového rozhraní routeru (*ETH*). Formulář *Secondary* lze použít pouze ve verzi s volitelným ethernetovým portem.

Položka	Popis
DHCP Client	Povoluje/zakazuje funkci DHCP client. • **disabled** – Router nemá povoleno automatické přidělení IP adresy od DHCP serveru v síti LAN. • **enabled** – Router má povoleno automatické přidělení IP adresy od DHCP serveru v síti LAN.
IP address	Pevně nastavená IP adresa síťového rozhraní ETH routeru.
Subnet Mask	Specifikuje masku sítě.
Default Gateway	Výchozí brána routeru. Při zadání IP adresy výchozí brány se všechny pakety, pro které nebyl nalezen záznam ve směrovací tabulce, odesílají na tuto adresu.
DNS server	Specifikuje IP adresu DNS serveru routeru. Adresa, na kterou jsou přeposlány všechny DNS dotazy na router.
Bridged	Povoluje/zakazuje funkci bridge. • **no** – Router nemá aktivován režim bridge (výchozí hodnota) • **yes** – Router má aktivován režim bridge

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
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 14: Konfigurace síťového rozhraní

Router považuje poslední adresu v síťovém rozsahu za broadcast adresu, nezávisle na tom, jestli je jako broadcast nastavena či ne. Spojení (ping) na broadcast adresu nefunguje.

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 3.7). Od FW 5.3.0 jsou *Default Gateway* a *DNS Server* podporovány také na přemostěných rozhraních (např. eth0 + eth1).

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

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

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.
IP Pool End	Konec prostoru IP, které budou přidělovány DHCP klientům.
Lease time	Čas v sekundách, po který smí klient IP adresu používat.

Tabulka 15: Konfigurace dynamického DHCP serveru

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

Tabulka 16: Konfigurace statického DHCP serveru

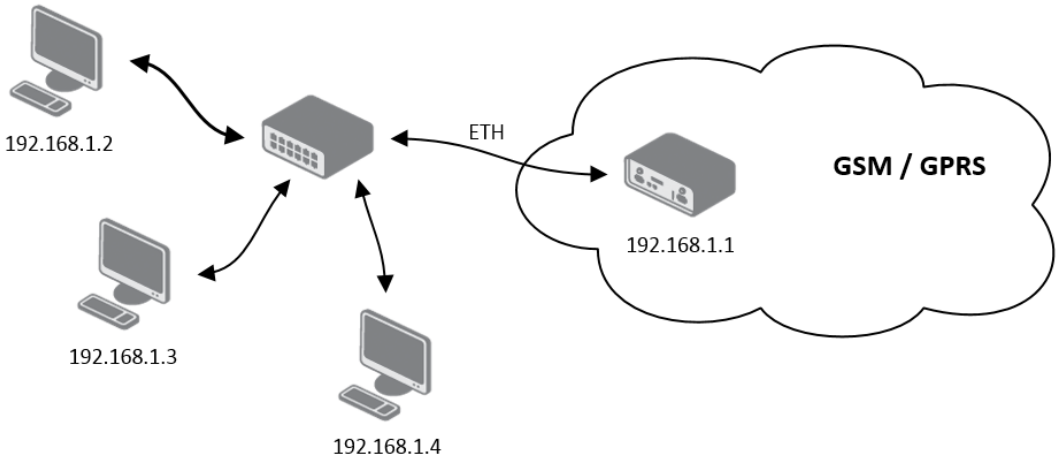
Následující část konfigurace umožňuje použít autentifikaci (802.1x) k Radius serveru. Tato funkcionalita vyžaduje nastavení identity a certifikátů, viz následující tabulka.

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.

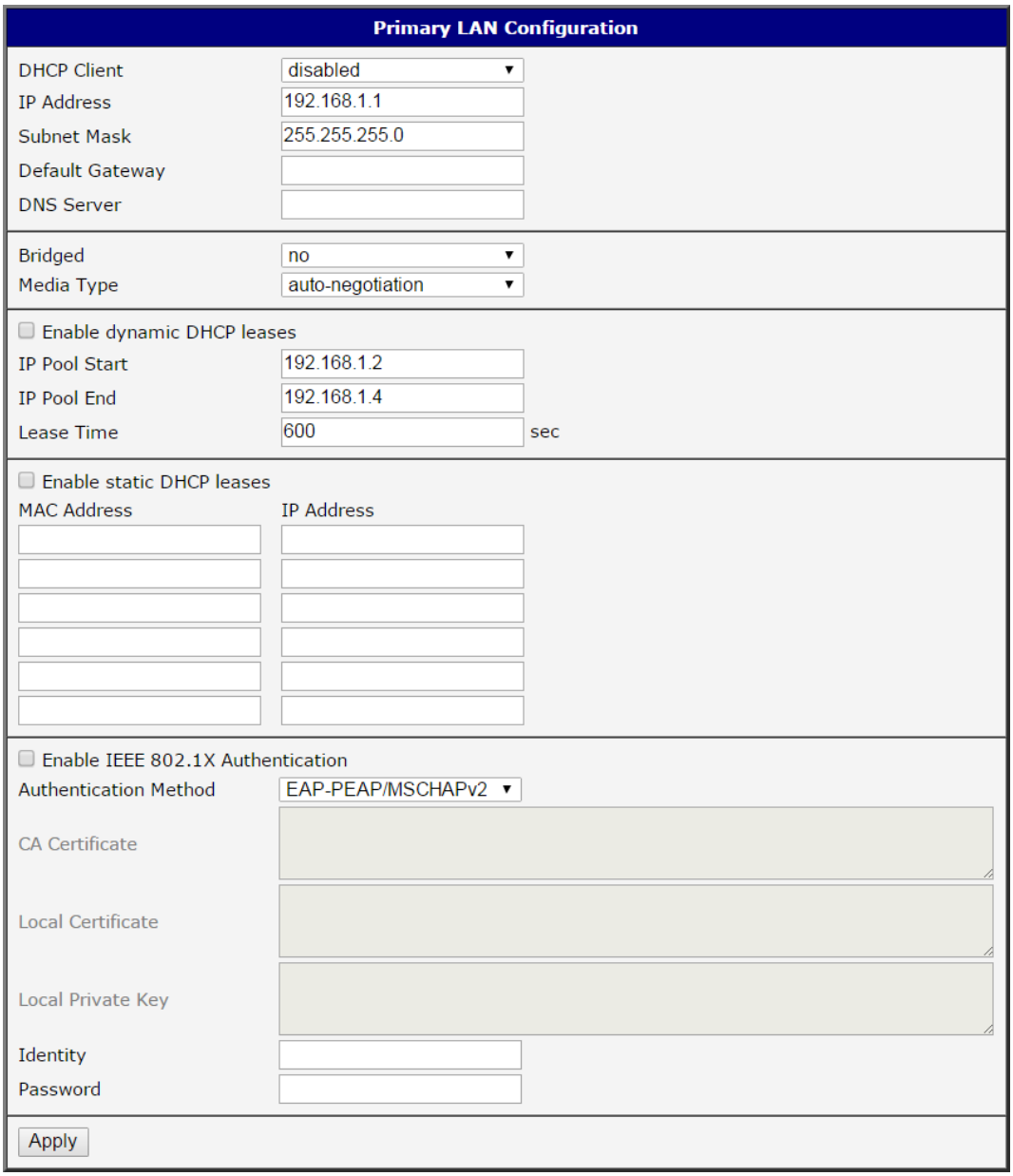
Tabulka 17: Konfigurace 802.1X autentikace

Příklad 1: Nastavení síťového rozhraní s dynamickým DHCP serverem:

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



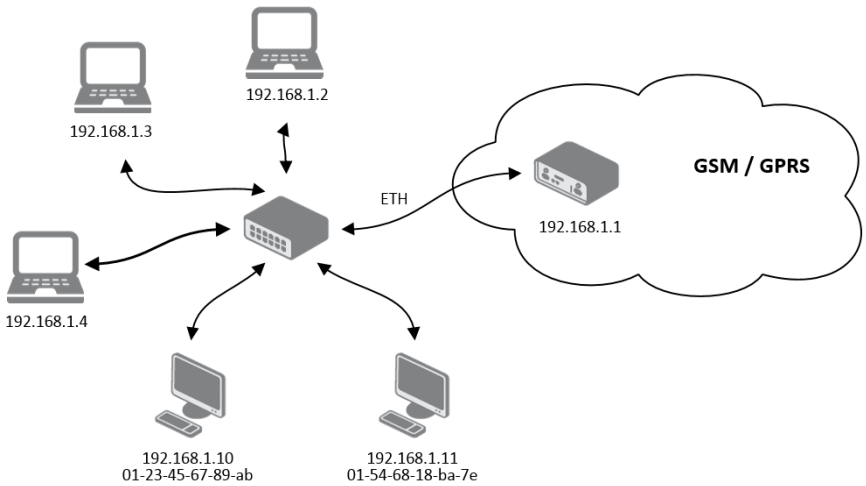
Obrázek 11: Příklad 1 – Topologie sítě s dynamickým DHCP Server



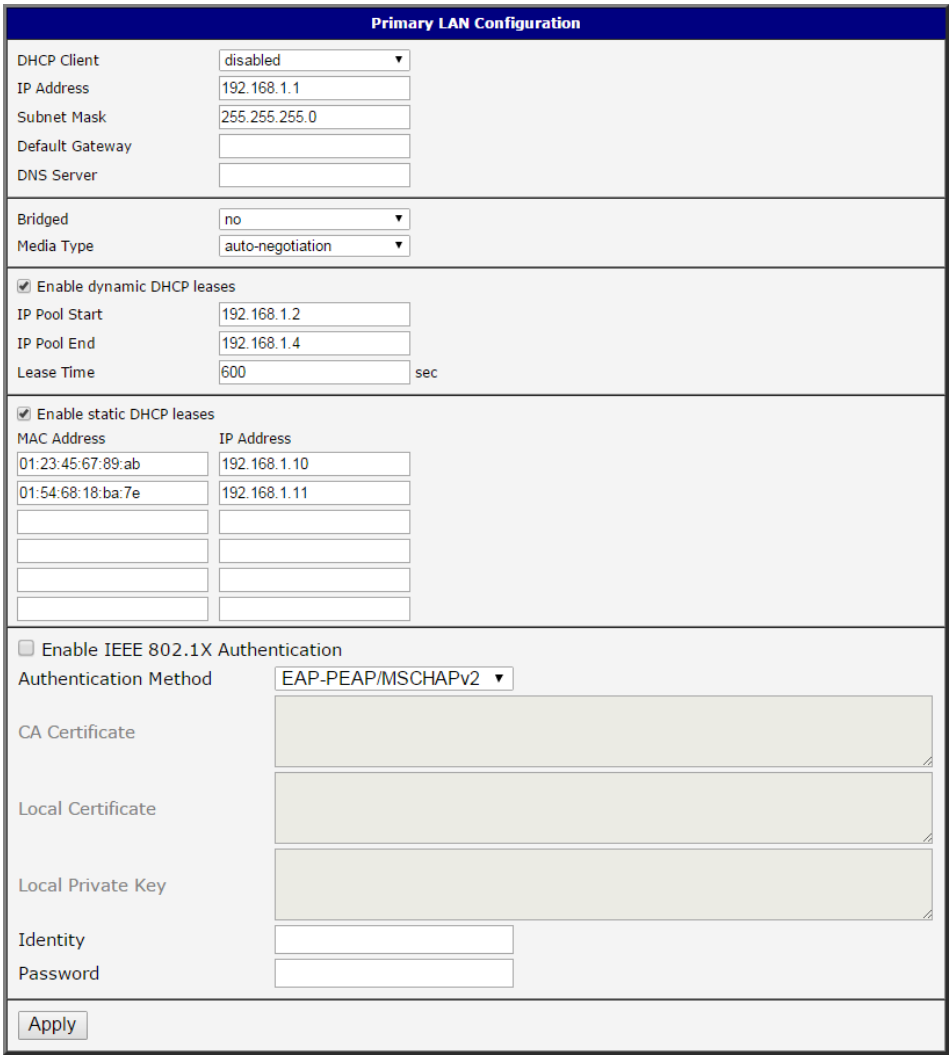
Obrázek 12: Příklad 1 – Konfigurace na stránce LAN

Příklad 2: Nastavení síťového rozhraní s dynamickým a statickým DHCP serverem:

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



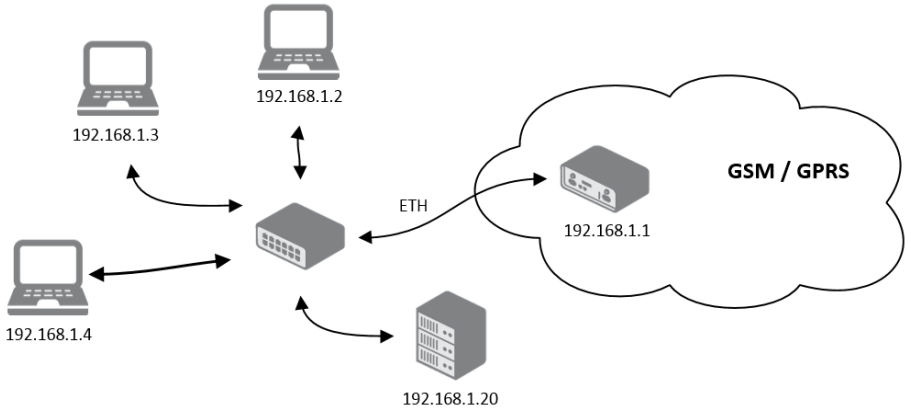
Obrázek 13: Příklad 2 – Topologie sítě se statickým i dynamickým DHCP serverem



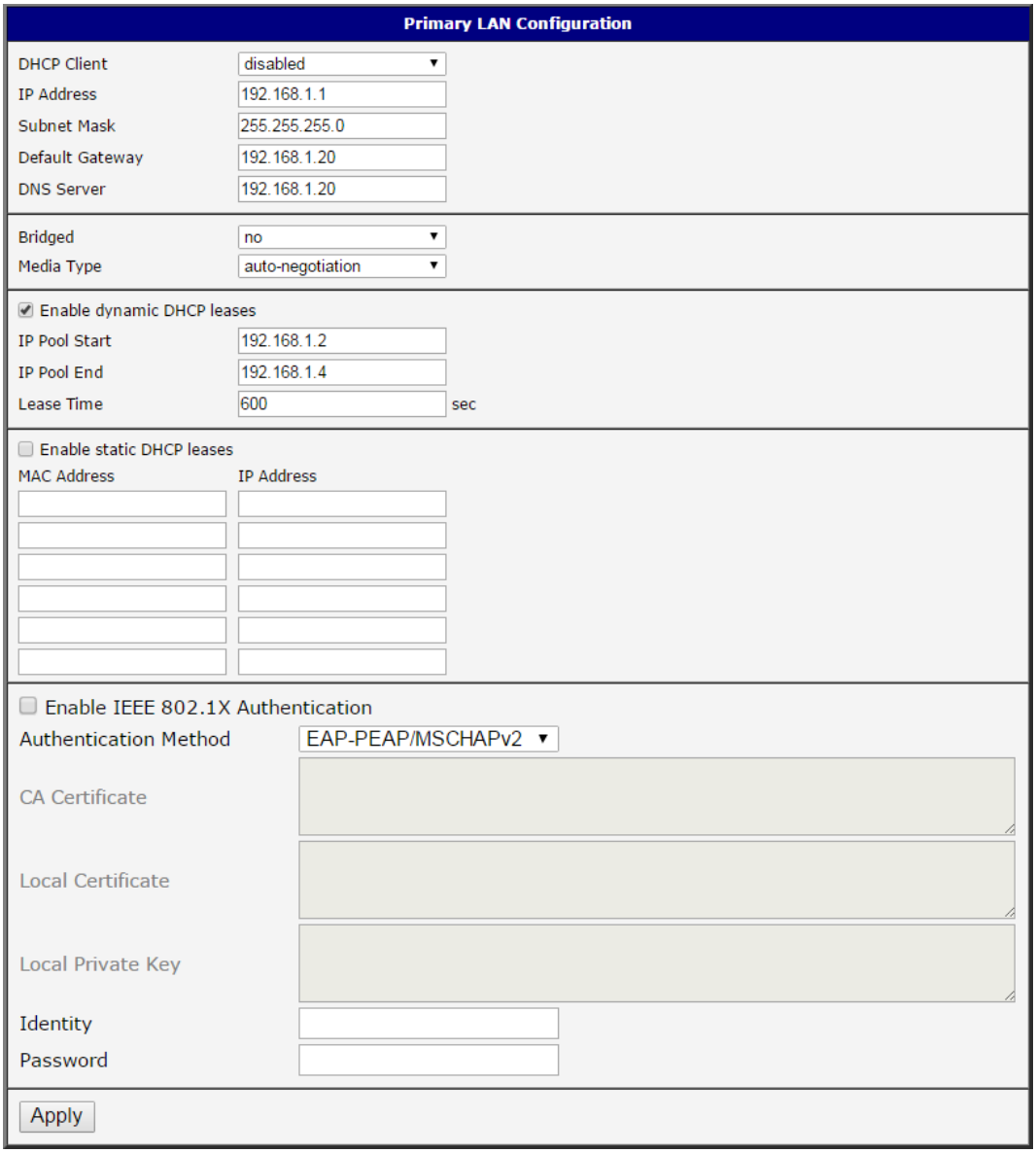
Obrázek 14: Příklad 2 – Konfigurace na stránce LAN

Příklad 3: Nastavení síťového rozhranní s výchozího bránou a DNS serverem:

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



Obrázek 15: Příklad 3 – Topologie sítě



Obrázek 16: Příklad 3 – Konfigurace na stránce LAN

3.2 VRRP Configuration

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 18: 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.

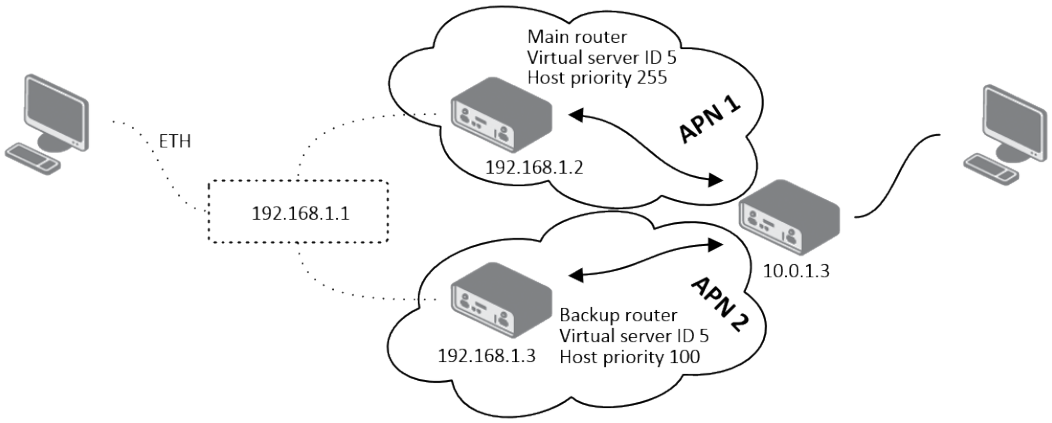
Položka	Popis
Ping IP Address	Cílová IP adresa ping dotazů (nelze zadat jako doménové jméno).
Ping Interval	Časové intervaly mezi odesílanými ping dotazy.
Ping Timeout	Doba čekání na odpověď.
Ping Probes	Počet neúspěšných ping dotazů, po kterých se trasa považuje za neprůchodnou.

Tabulka 19: Check connection

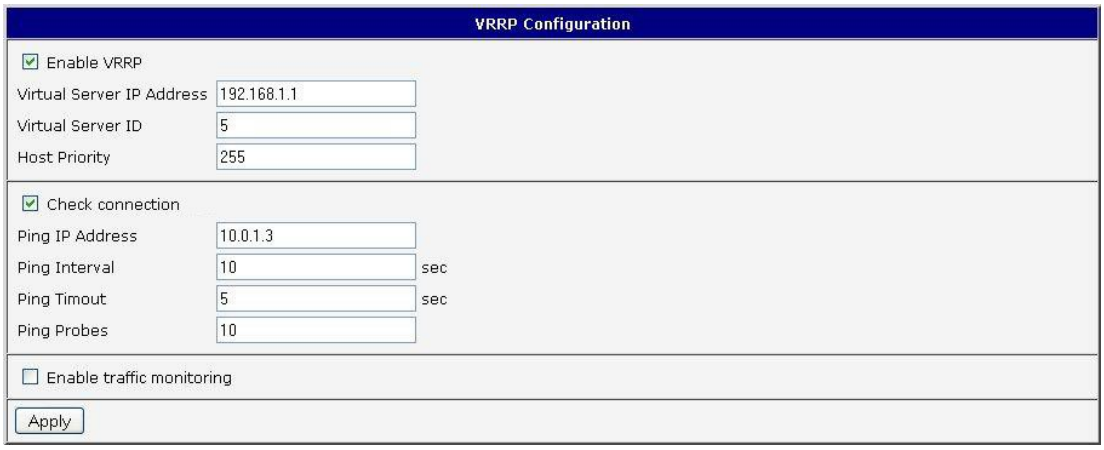
Jako ping adresu je nutné použít IP adresu, u které je jisté, že bude stále dostupná a bude na ní možné posílat ICMP dotazy (např. DNS server operátora).

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*.

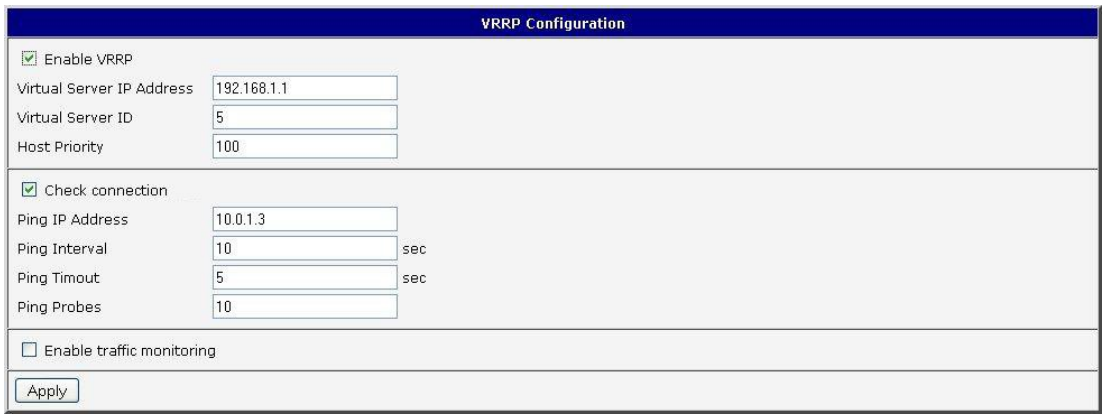
Nastavení protokolu VRRP:



Obrázek 17: Topologie k příkladu konfigurace VRRP



Obrázek 18: Příklad konfigurace VRRP – Hlavní router



Obrázek 19: Příklad konfigurace VRRP – Záložní router

3.3 Mobile WAN

Položka *Mobile WAN* není dostupná pro routery XR5i v2.

Zvolte položku *Mobile WAN* v sekci *Configuration* hlavního menu pro konfiguraci připojení do mobilní sítě.

3.3.1 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 (v případě FULL verze routeru se sloty pro 2 SIM karty) nebo jako dvě APN nastavení mezi nimiž se bude jedna SIM karta přepínat (v případě BASIC verze routeru s jedním slotem pro SIM kartu).

Položka	Popis
APN	Access point name – přístupový bod sítě.
Username	Jméno uživatele pro přihlášení do sítě.
Password	Přístupové heslo pro přihlášení do sítě.
Authentication	Protokol autentizace v GSM síti: • **PAP or CHAP** – Autentizační metodu zvolí router. • **PAP** – Router používá autentizační metodu PAP. • **CHAP** – Router používá autentizační metodu CHAP.
IP Address	IP 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. • *Další položky závisí na typu daného routeru* – Je možné vybrat konkrétní způsob přenosu dat (GPRS/EDGE, UMTS, LTE . . .).
PIN	Nutno nastavit pouze pokud to vyžaduje SIM karta routeru. Po několika špatných pokusech o zadání PIN dojde k zablokování SIM karty.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
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 je 128 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 128 B.

Tabulka 20: 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“. Je-li detekována síť AT&T, použije se „**phone**“. APN definuje mobilní operátor.
- Je-li v poli *APN* zadáno slovo *blank*, je APN routerem interpretováno jako prázdné.

UPOZORNĚNÍ:

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

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

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

3.3.2 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*).

3.3.3 Konfigurace kontroly spojení s mobilní sítí

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

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

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

Tabulka 21: Konfigurace kontroly spojení s mobilní sítí

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

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

3.3.4 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 22: 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.

3.3.5 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.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
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. Tato volba není dostupná na Libratum verzích routerů. • **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 1, tj. pod napětím. • **off** – SIM kartu je možné použít pouze pokud je stav vstupu BIN0 logická 0, tj. bez napětí.

Tabulka 23: 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 24: Parametry pro přepínání SIM karet

Příklad:

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 nebo APN 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).

3.3.6 Konfigurace Dial-In přístupu

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

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

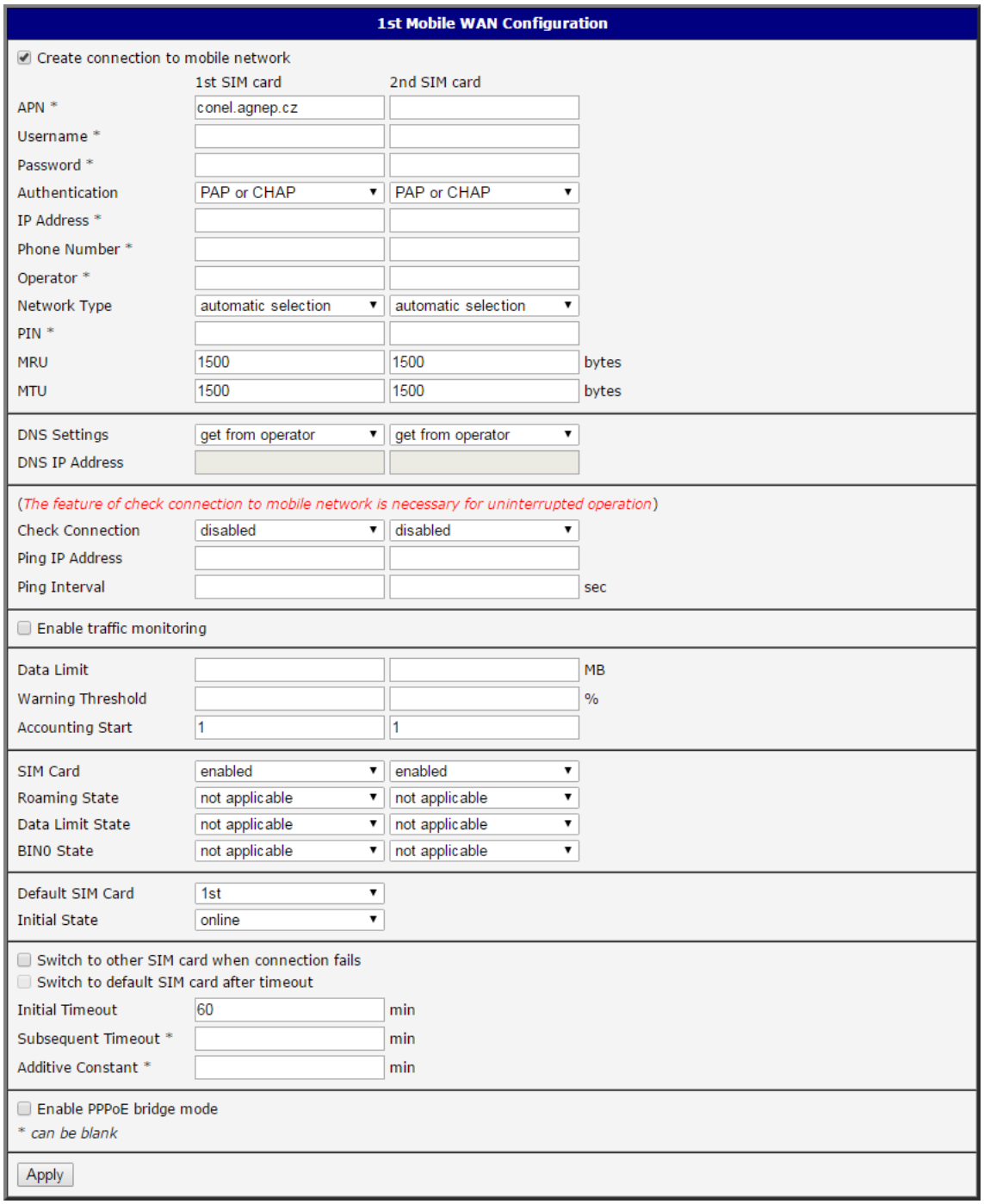
Položka	Popis
Username	Přihlašovací jméno pro zabezpečený přístup.
Password	Heslo pro zabezpečený přístup.

Tabulka 25: Konfigurace Dial-In přístupu

3.3.7 Konfigurace PPPoE bridge mode

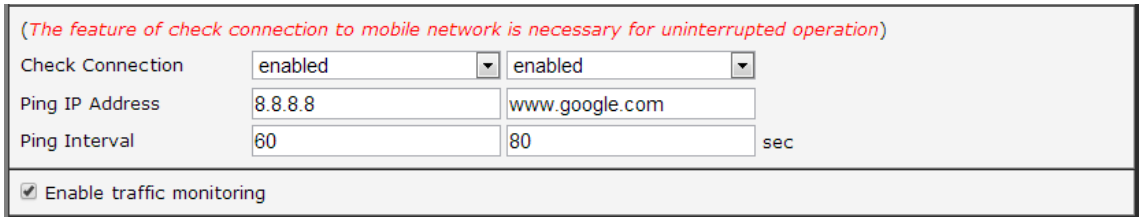
V poslední časti okna je možné zaškrtnout mód *Enable PPPoE bridge mode*, kterým aktivujete PPPoE bridge mód. PPPoE (point-to-point over ethernet) je síťový protokol zapouzdřující PPP rámce do ethernetových rámců. Umožňuje vytvoření PPPoE spojení ze zařízení za routerem. Například z PC připojeného na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

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



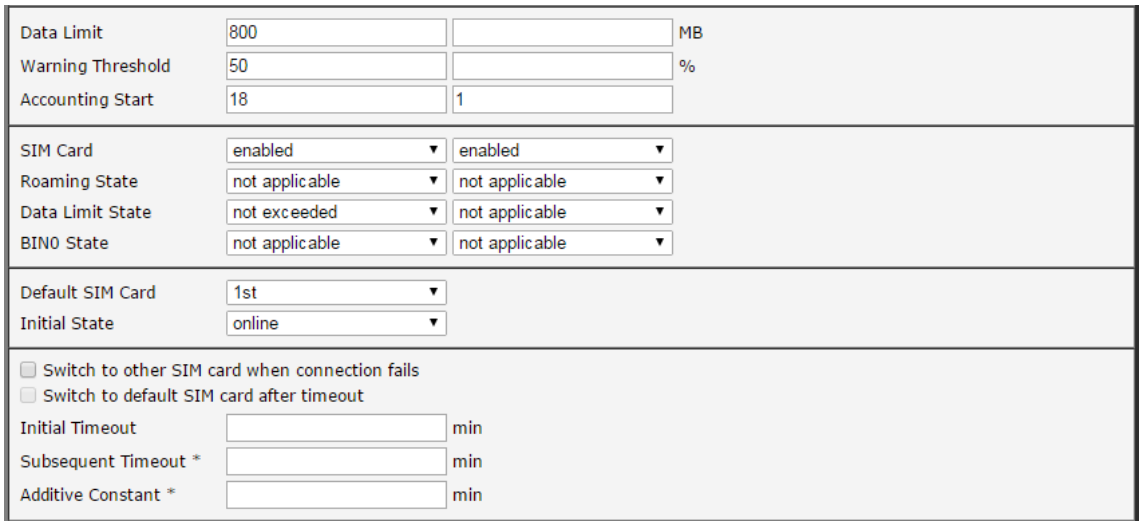
Obrázek 20: Mobile WAN konfigurace

Příklad 1: 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 21: Příklad 1 – Mobile WAN konfigurace

Příklad 2: 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:



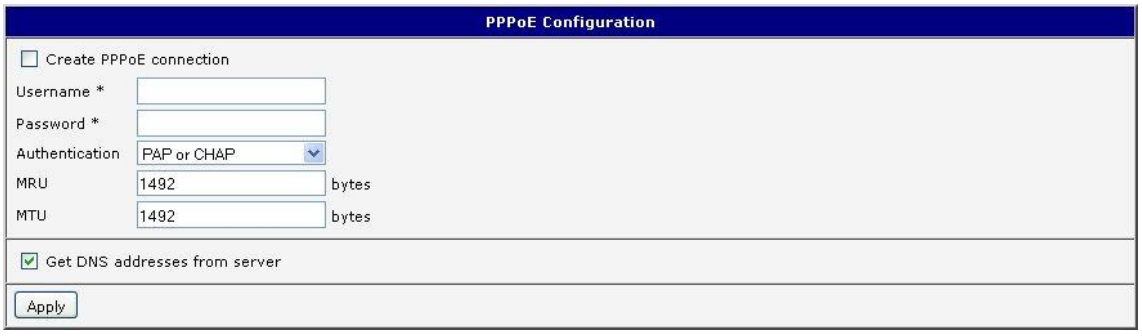
Obrázek 22: Příklad 2 – Mobile WAN konfigurace

3.4 Konfigurace PPPoE

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.

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.
MRU	Maximum Receiving Unit – Identifikuje maximální velikost paketu, kterou je prvek v daném prostředí schopen přijmout. Z výroby je nastavena velikost na 1492 bytů.
MTU	Maximum Transmission Unit – Identifikuje maximální velikost paketu, kterou je prvek v daném prostředí schopen přenášet. Z výroby je nastavena na 1492 bytů.

Tabulka 26: Konfigurace PPPoE



Obrázek 23: Konfigurace PPPoE

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

3.5 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.
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.
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	IP 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

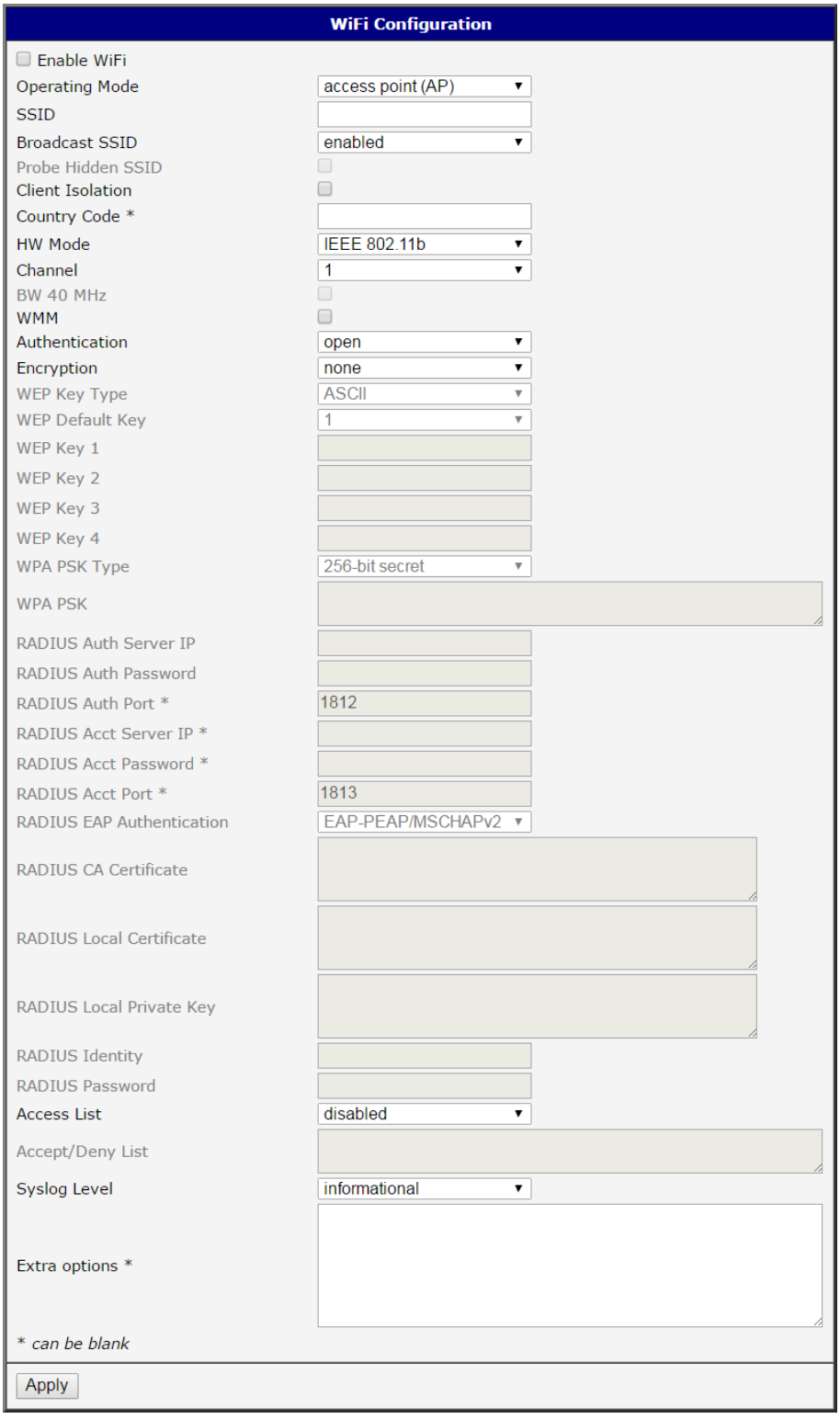
Položka	Popis
RADIUS Acct Server IP	IP adresa serveru RADIUS pro účtování (accounting). Je nutné vyplnit pouze pokud je server pro účtování odlišný od serveru pro autentizaci a autorizaci. Dostupné pouze v režimu AP a při zvolení některé z autentizačních metod RADIUS.
RADIUS Acct Password	Přístupové 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. Položka není dostupná pro autentizační protokol EAP-TLS.
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 27: Konfigurace WiFi



Obrázek 24: Konfigurace WiFi

3.6 Konfigurace WLAN

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. Dále je možné nastavit následující vlastnosti:

Item	Description
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.
DHCP Client	Aktivuje/deaktivuje DHCP klienta.
IP Address	Pevně nastavená IP adresa WiFi rozhraní routeru.
Subnet Mask	Maska sítě WiFi rozhraní routeru.
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).
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.
DNS Server	Adresa, na kterou jsou přeposlány všechny DNS dotazy.

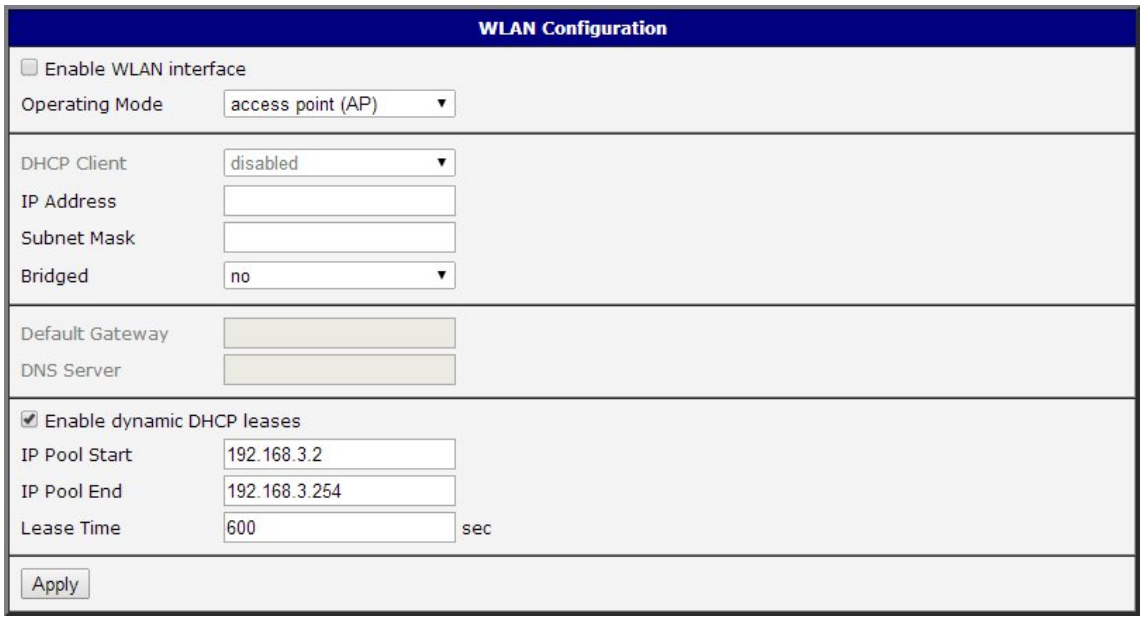
Tabulka 28: Konfigurace WLAN

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

Item	Description
IP Pool Start	Začátek rozsahu IP adres, které budou přidělovány DHCP klientům.
IP Pool End	Konec rozsahu IP adres, které budou přidělovány DHCP klientům.
Lease Time	Čas v sekundách, po který smí klient IP adresu používat.

Tabulka 29: Konfigurace DHCP serveru

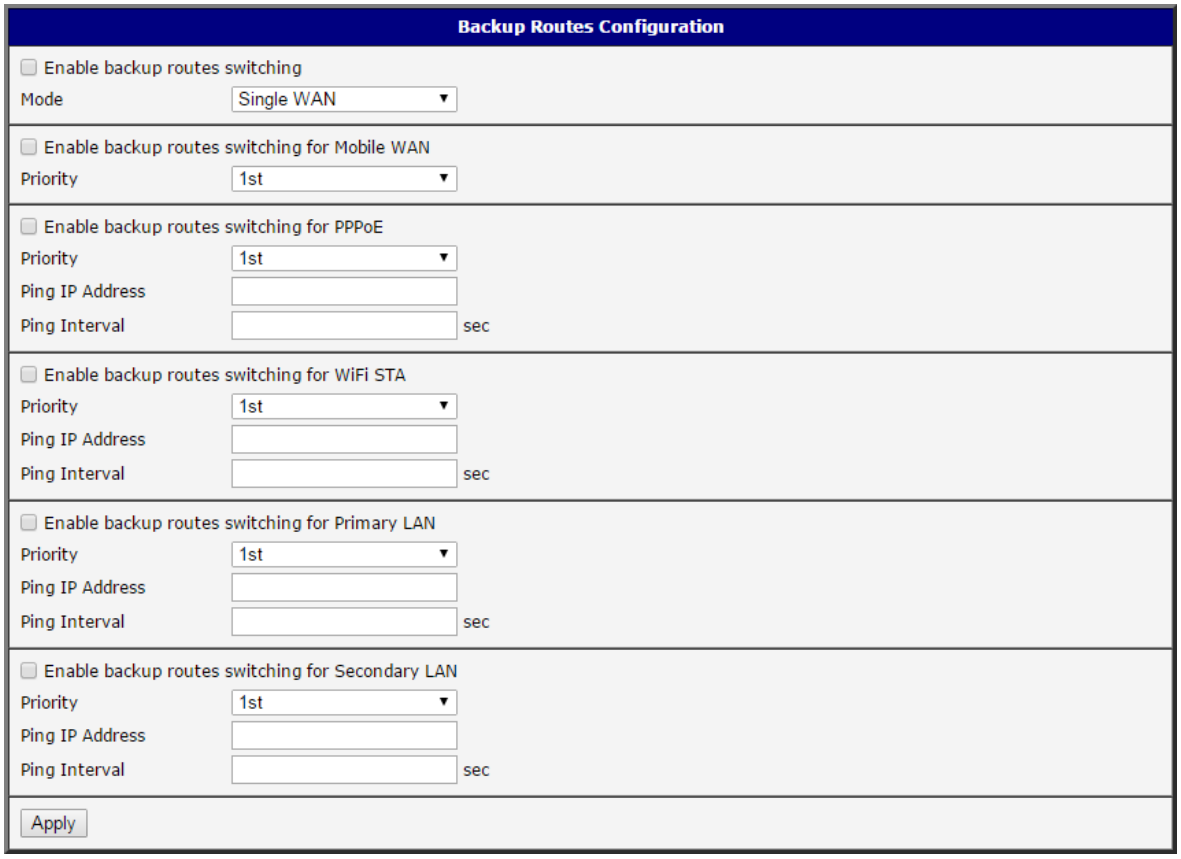
Všechny změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 25: WLAN konfigurace

3.7 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 26: Backup Routes

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 30: 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*, *Enable backup routes switching for Primary LAN* nebo *Enable backup routes switching for Secondary 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 IP adresa nebo doménové jméno ping dotazů pro kontrolu spojení.
Ping Interval	Časové intervaly mezi odesílanými ping dotazy.

Tabulka 31: Backup Routes

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. 3.3.1.

Navíc se u síťových rozhraní, příslušejících k jednotlivým záložním cestám, kontroluje příznak "RUNNING". Tato kontrola řeší např. odpojení ethernetového kabelu. Všechny změny v nastavení se projeví po stisknutí tlačítka *Apply*.

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 (pppX, usbX)
- PPPoE (ppp0)
- WiFi STA (wlan0)
- Secondary LAN (eth1)
- Primary LAN (eth0)

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

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*.

3.8 Konfigurace firewallu

Prvním bezpečnostním prvkem, na který příchozí pakety narazí, je kontrola povolených zdrojových IP adres a cílových portů. 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, ze které je povolen přístup na router.
Protocol	Protokol, kterým je povolen přístup na router: • **all** – Přístup povolen všemi protokoly. • **TCP** – Přístup povolen protokolem TCP. • **UDP** – Přístup povolen protokolem UDP. • **ICMP** – Přístup povolen protokolem ICMP.
Target Port	Číslo portu, na kterém je povolen přístup na router.
Action	Typ akce: • **allow** – Přístup povolen. • **deny** – Přístup zakázán.

Tabulka 32: 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.

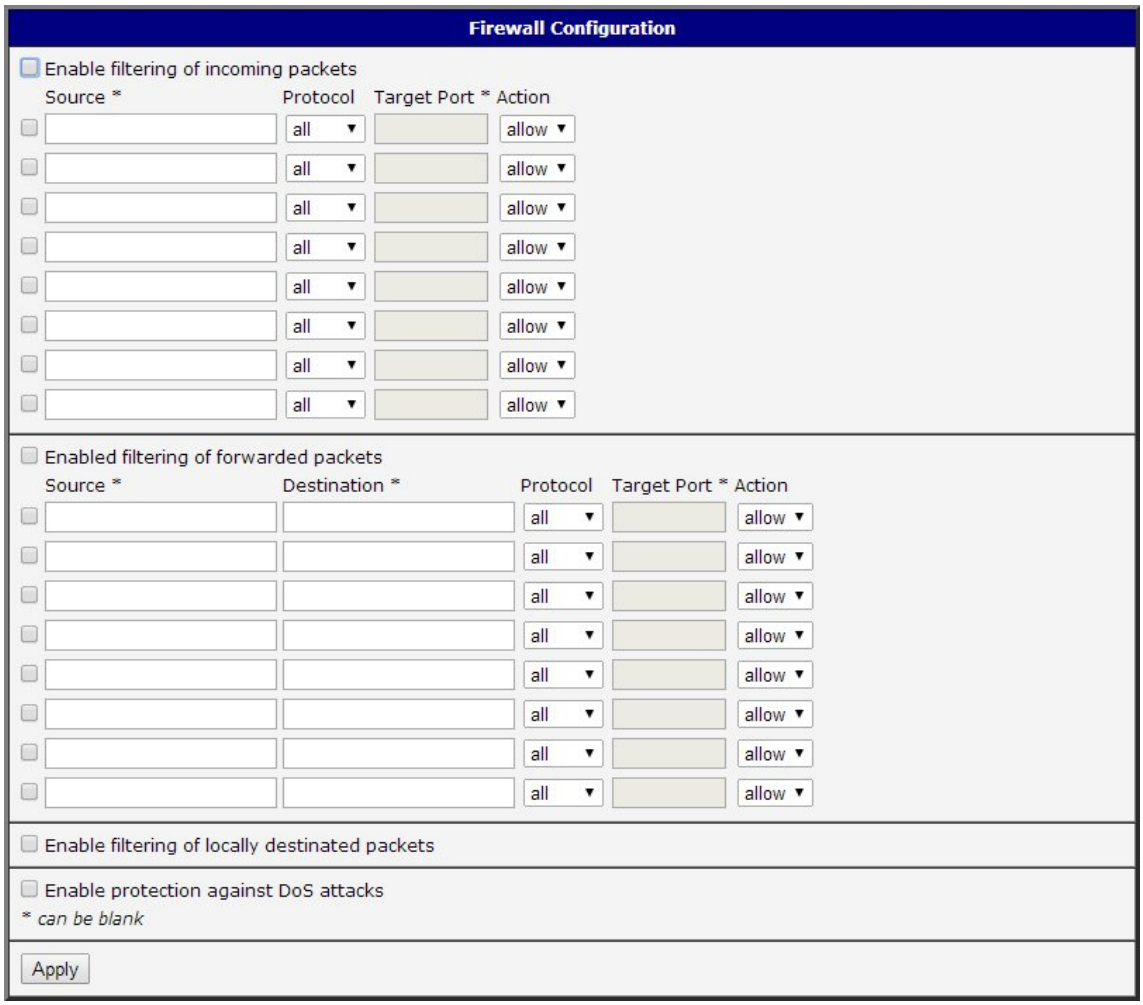
V tabulkách pro definici pravidel lze povolit také veškerý provoz v rámci zvoleného protokolu (specifikuje se pouze protokol), nebo vytvářet přísnější pravidla specifikováním položek pro zdrojové či cílové IP adresy a portu.

Položka	Popis
Source	IP adresa zdrojového zařízení.
Destination	IP adresa cílového zařízení.
Protocol	Protokol kterým je povolen přístup na router: • **all** – Přístup povolen všemi protokoly. • **TCP** – Přístup povolen protokolem TCP. • **UDP** – Přístup povolen protokolem UDP. • **ICMP** – Přístup povolen protokolem ICMP.
Target Port	Číslo portu, na kterém je povolen přístup na router.
Action	Typ akce: • **allow** – Přístup povolen. • **deny** – Přístup zakázán.

Tabulka 33: 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.

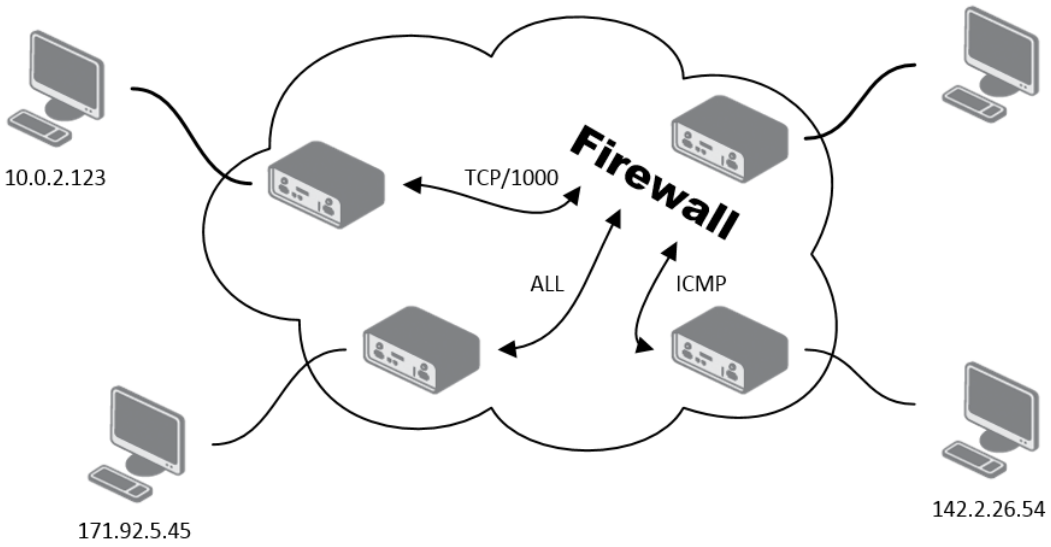


Obrázek 27: Konfigurace firewallu

Příklad nastavení firewallu:

Na router jsou povoleny následující přístupy:

- z adresy 171.92.5.45 pomocí jakéhokoli protokolu
- z adresy 10.0.2.123 pomocí protokolu TCP na portu 1000
- z adresy 142.2.26.54 pomocí protokolu ICMP



Obrázek 28: Topologie příkladu nastavení firewallu

Firewall Configuration

Enable filtering of incoming packets

	Source *	Protocol	Target Port *	Action
☑	171.92.5.45	all		allow
☑	10.0.2.123	TCP	1000	allow
☑	142.2.26.54	ICMP		allow
☐		all		allow
☐		all		allow
☐		all		allow
☐		all		allow
☐		all		allow

Obrázek 29: Příklad nastavení firewallu

3.9 NAT Configuration

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

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

Tabulka 34: Konfigurace překladu adres (NAT)

Pokud je potřeba nastavit více než šestnáct pravidel pro NAT, je možné vložit do start-up script (položka *Startup Script* v sekci *Configuration*) následující skript:

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

kde je třeba místo [PORT_PUBLIC] a [PORT_PRIVATE] vložit konkrétní čísla portů a místo [IPADDR] vložit IP adresu.

Následující položky slouží k nastavení routování veškeré příchozí komunikace z PPP na počítač s definovanou IP adresou.

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

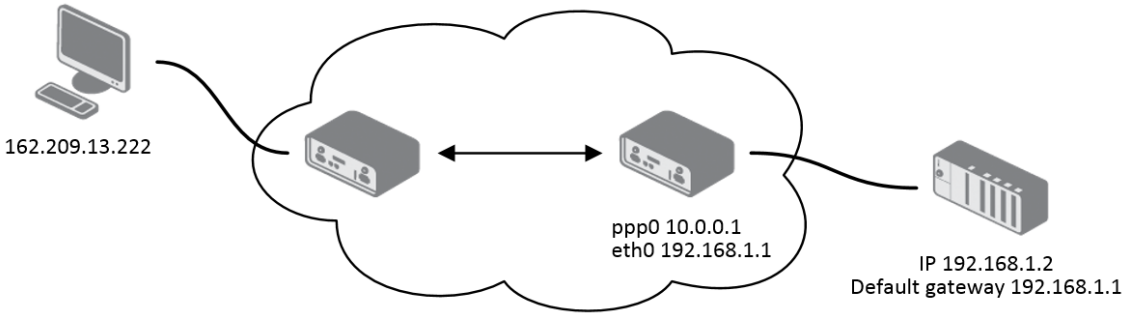
Tabulka 35: Konfigurace jednotného přeposílání

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

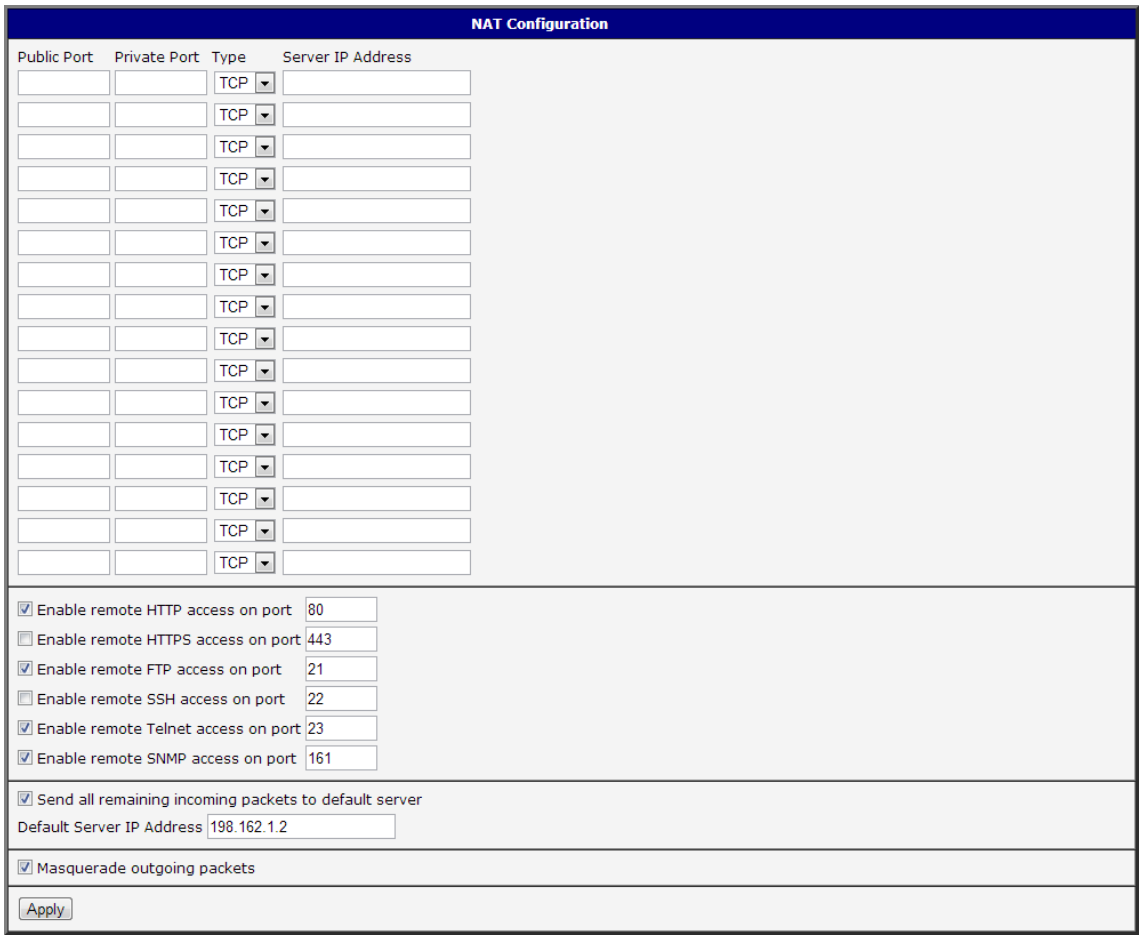
Položka	Popis
Enable remote HTTP access on port	Umožňuje konfiguraci routeru přes webové rozhraní (ve výchozí konfiguraci zakázáno).
Enable remote HTTPS access on port	Umožňuje konfiguraci routeru přes zabezpečený webový protokol *HTTPS* (ve výchozí konfiguraci zakázáno).
Enable remote FTP access on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

Tabulka 36: Konfigurace vzdáleného přístupu

Příklad 1: Konfigurace s jedním připojeným zařízením na routeru.



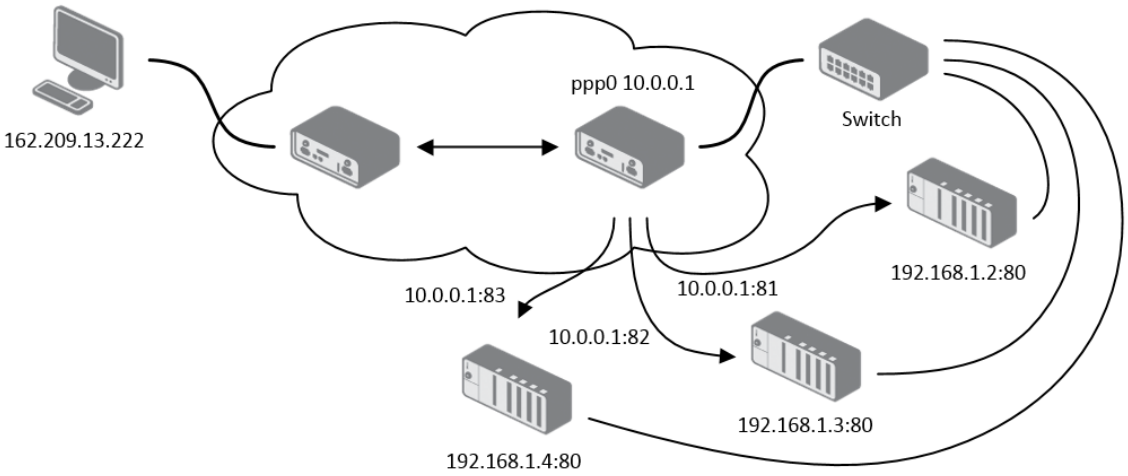
Obrázek 30: Příklad 1 – Topologie konfigurace NAT



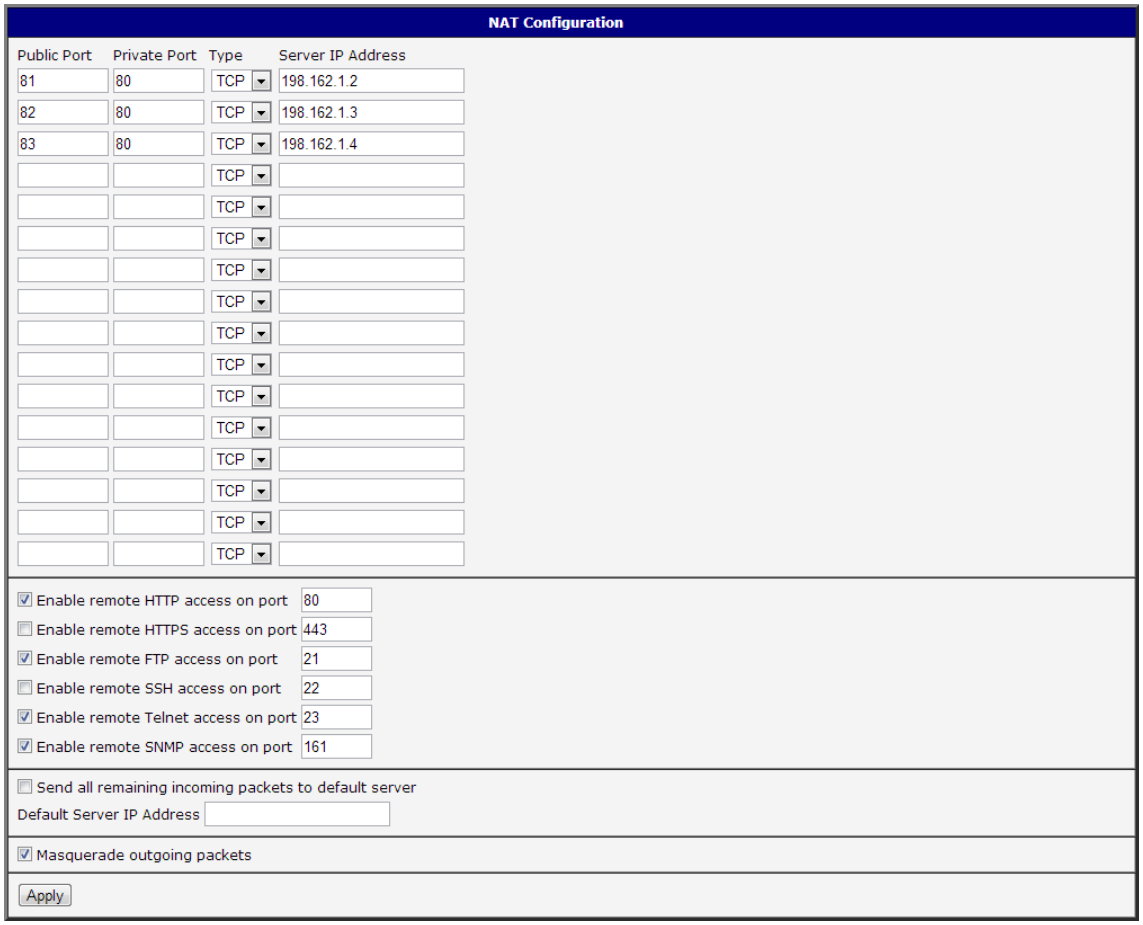
Obrázek 31: Příklad 1 – NAT konfigurace

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

Příklad 2: Konfigurace s více zařízeními na routeru.



Obrázek 32: Příklad 2 – Topologie konfigurace NAT



Obrázek 33: Příklad 2 – NAT konfigurace

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

3.10 Konfigurace OpenVPN tunelu

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*.

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.
UDP/TCP port	Port příslušného protokolu.
Remote IP Address	IP adresa protější strany tunelu. Lze použít i doménové jméno.
Remote Subnet	IP adresa sítě za protější stranou tunelu.
Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Redirect Gateway	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 IP adresu lokálního rozhraní.
Remote Interface IP Address	Definuje IP adresu rozhraní protější strany tunelu.
Ping Interval	Definuje časový interval, po kterém pošle zprávu druhé straně, pro kontrolu správné existence tunelu.
Ping Timeout	Definuje časový interval, po který router čeká na vyslanou zprávu protistranou. Aby se správně ověřoval OpenVPN tunel, musí být parametr *Ping Timeout* větší než *Ping Interval*.
Renegotiate Interval	Nastavuje periodu renegociace (reautorizace) tunelu OpenVPN. Tento parametr je možné nastavit pouze při ověřování username/password nebo při použití certifikátu X.509. Po této časové periodě router mění šifrování tunelu, aby byla zajištěna trvalá bezpečnost tunelu.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Max Fragment Size	Tímto parametrem je možné definovat maximální velikost odesílaného paketu.
Compression	Odesílané data je možné komprimovat. • **none** – Není použitá žádná komprese. • **LZO** – Je použita bezeztrátová komprese, která musí být nastavená na obou stranách tunelu.
NAT Rules	Tímto parametrem lze aplikovat NAT pravidla na OpenVPN tunel: • **not applied** – NAT pravidla nejsou aplikována na OpenVPN tunel. • **applied** – NAT pravidla jsou aplikována na OpenVPN tunel.
Authenticate Mode	Tímto parametrem je možné nastavit autentizaci: • **none** – Není nastavena žádná autentizace. • **Pre-shared secret** – Nastavuje sdílený klíč pro obě strany tunelu. • **Username/password** – Umožňuje autentizaci pomocí *CA Certificate*, *Username* a *Password*. • **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.

Pokračování na následující straně

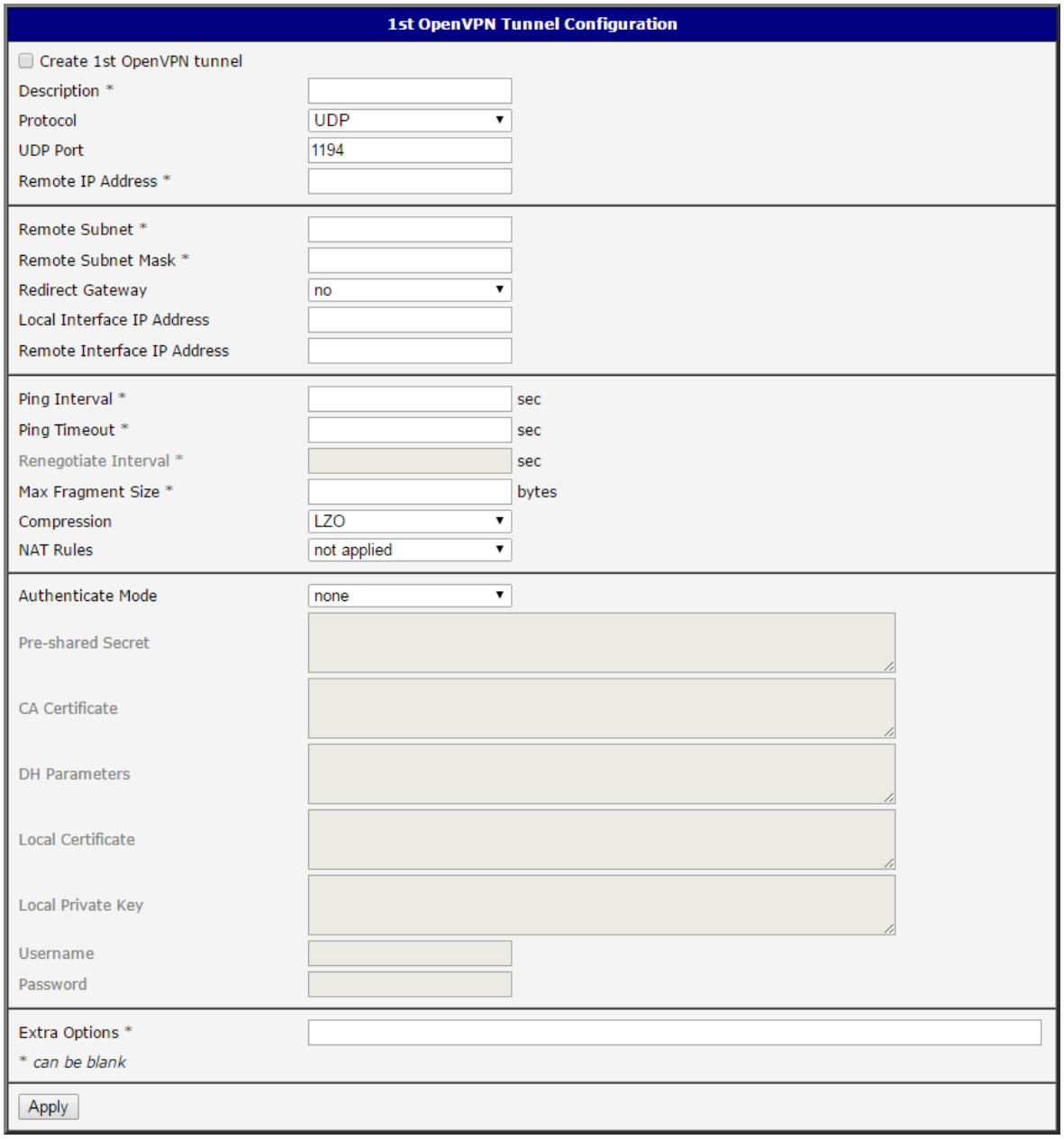
Pokračování z předchozí strany

Položka	Popis
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 37: Konfigurace OpenVPN tunelu

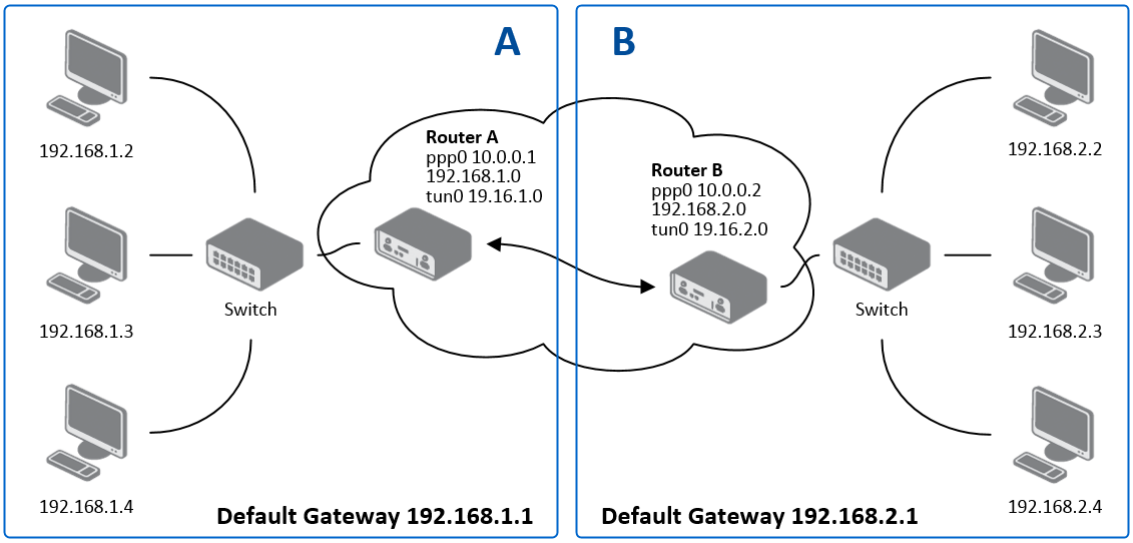
Podmínkou pro sestavení tunelu je, aby aktuálně nastavená cesta do WAN byla aktivní (v případě mobilního spojení musí dojít k jeho úspěšnému navázání) a to i v případě, že samotný tunel nevede do WAN.

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



Obrázek 34: Konfigurace OpenVPN tunelu

Příklad: Konfigurace OpenVPN tunelu.



Obrázek 35: 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 38: Příklad konfigurace OpenVPN tunelu

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

3.11 Konfigurace IPsec tunelu

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

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.
Remote IP Address	IP adresa protější strany tunelu. Lze zadat i doménové jméno.
Remote ID	Identifikátor (ID) protější strany tunelu. Skládá se ze dvou částí: *hostname* a *domain-name* (více informací pod tabulkou).
First Remote Subnet	IP adresa sítě za protější stranou tunelu.
First Remote Subnet Mask	Maska sítě za protější stranou tunelu.
Second Remote Subnet	IP adresa druhé sítě za protější stranou tunelu. Pouze pro *IKE Protocol* = IKEv2.
Second Remote Subnet Mask	Maska druhé sítě za protější stranou tunelu. Pouze pro *IKE Protocol* = IKEv2.
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	IP adresa lokální sítě.
First Local Subnet Mask	Maska lokální sítě.
Second Local Subnet	IP adresa druhé lokální sítě. Pouze pro *IKE Protocol* = IKEv2.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
Second Local Subnet Mask	Maska druhé lokální sítě. 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.
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.

Pokračování na následující straně

Pokračování z předchozí strany

Položka	Popis
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.
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).

Tabulka 39: 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=Conel,OU=TP,CN=A)
- FQDN (např. @director.conel.cz) – **před FQDN vždy musí být znak @**
- User FQDN (např. director@conel.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

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*.

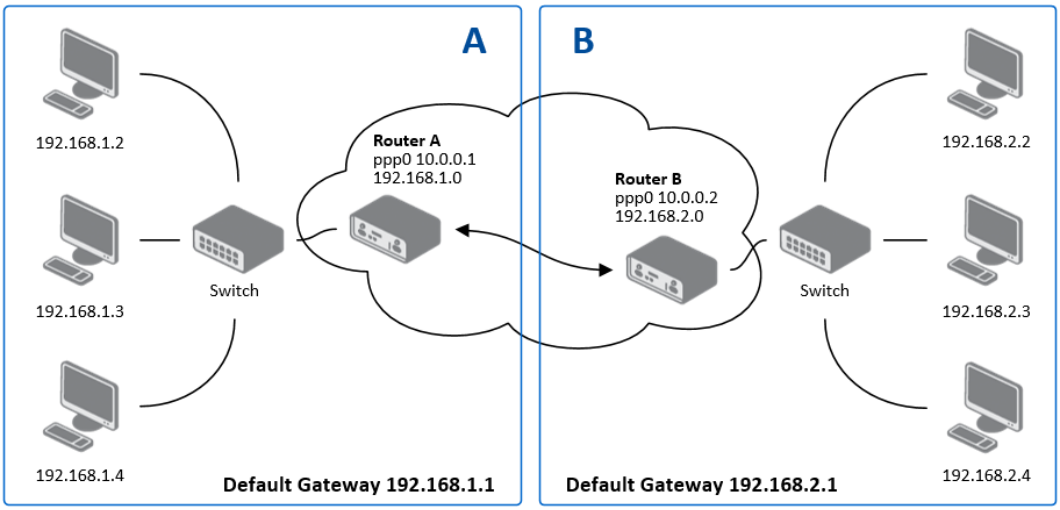
1st IPsec Tunnel Configuration

☐ 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 36: Konfigurace IPsec tunelu

Příklad: Konfigurace IPSec tunelu



Obrázek 37: Topologie příkladu konfigurace IPsec tunelu

Konfigurace IPSec tunelu:

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

Tabulka 40: Příklad konfigurace IPsec tunelu

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

3.12 Konfigurace GRE tunelu

GRE je nešifrovaný protokol.

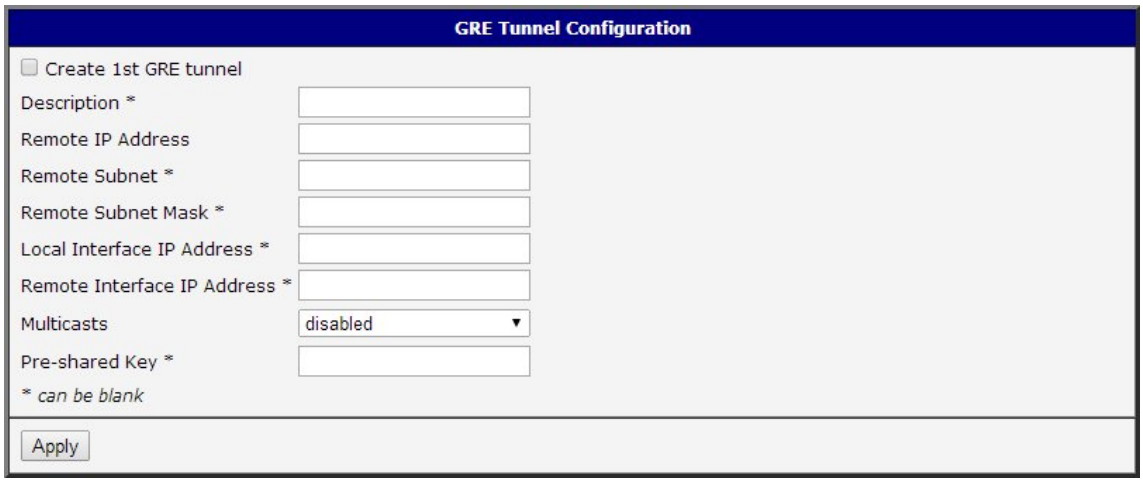
GRE tunel vytváří propojení dvou sítí LAN do jedné, která se tváří jako homogenní. Router umožňuje vytvořit až čtyři GRE tunely, jejichž konfiguraci je možné vyvolat volbou položky *GRE* v menu. V menu se pod touto položkou rozbalí čtyři další konfigurační stránky: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* 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 41: Konfigurace GRE tunelu

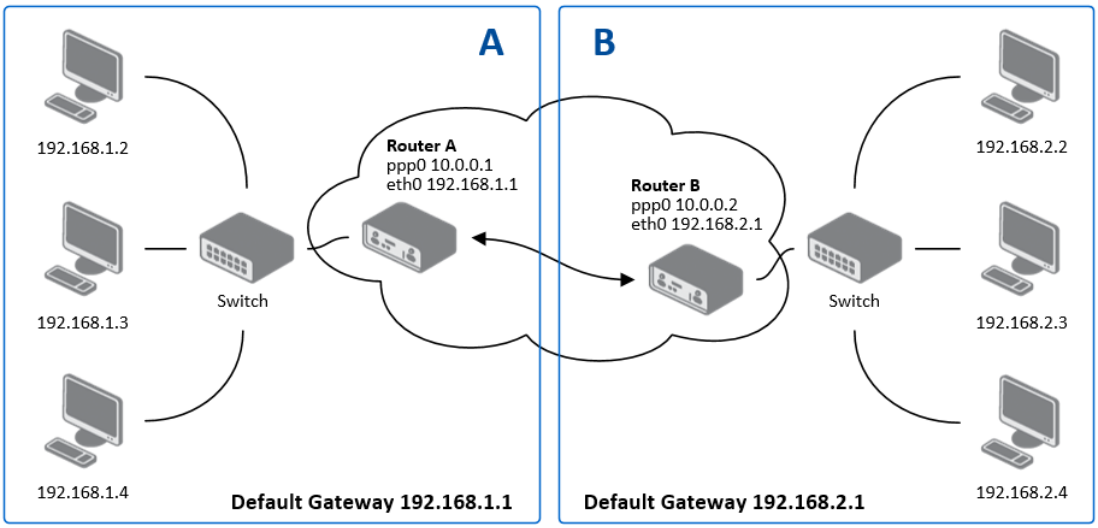
Pozor, GRE tunel neprojde přes překlad adres NAT.

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



Obrázek 38: GRE Tunnel Configuration

3.12.1 Příklad konfigurace GRE tunelu



Obrázek 39: 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 42: Příklad konfigurace GRE tunelu

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

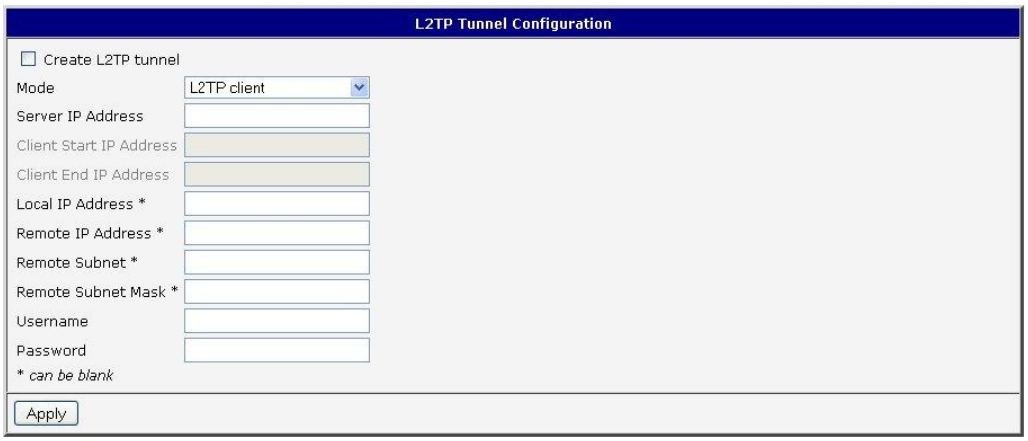
3.13 Konfigurace L2TP tunelu

L2TP je nešifrovaný protokol.

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

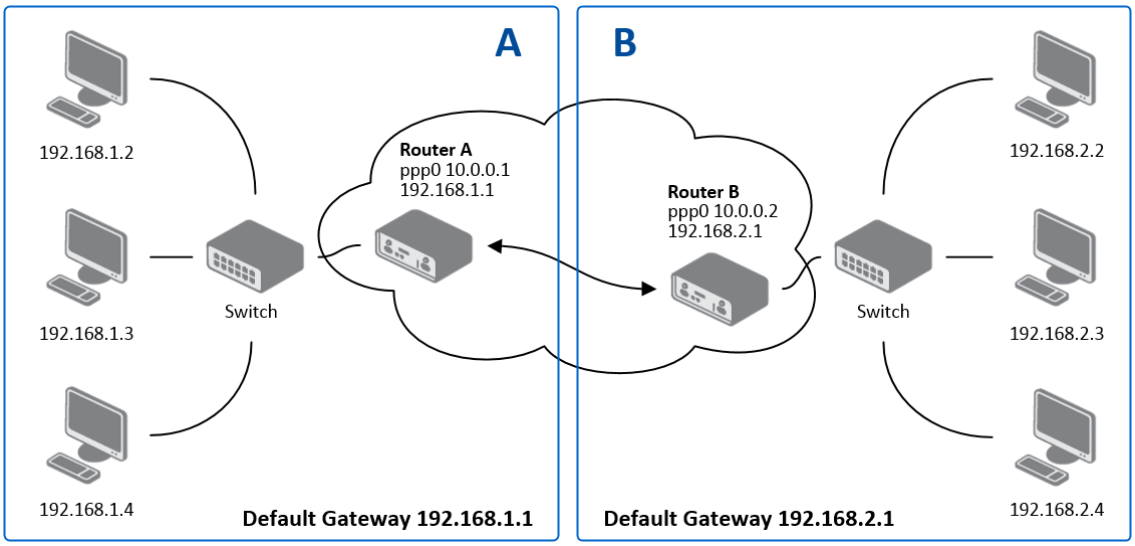
Položka	Popis
Mode	Mód L2TP tunelu na straně routeru: • **L2TP server** – Lze definovat počáteční a konečnou IP adresu rozsahu nabízenou serverem. • **L2TP client** – Lze definovat IP adresu server.
Server IP Address	Adresa serveru.
Client Start IP Address	První IP adresa v rozsahu nabízeném serverem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

Tabulka 43: Konfigurace L2TP tunelu



Obrázek 40: Konfigurace L2TP tunelu

3.13.1 Příklad konfigurace L2TP tunelu



Obrázek 41: 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 44: Příklad konfigurace L2TP tunelu

3.14 Konfigurace PPTP tunelu

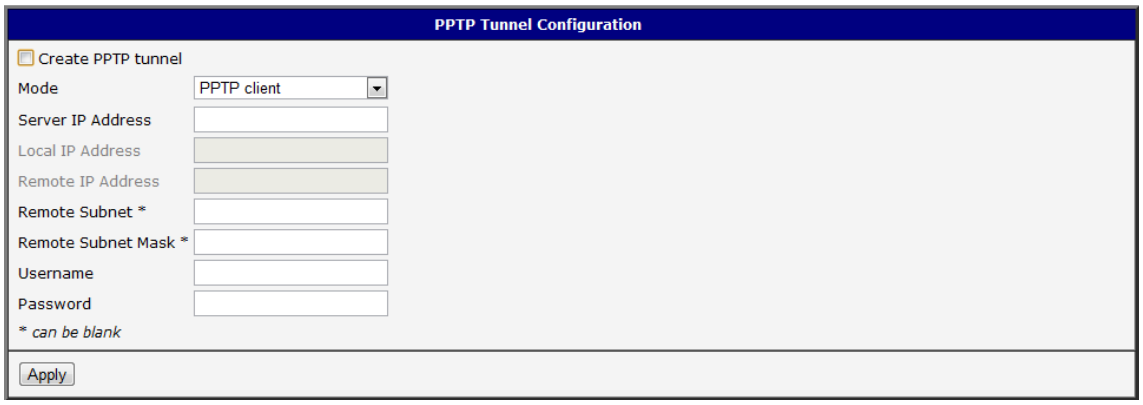
PPTP je nešifrovaný protokol.

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

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

Tabulka 45: Konfigurace PPTP tunelu

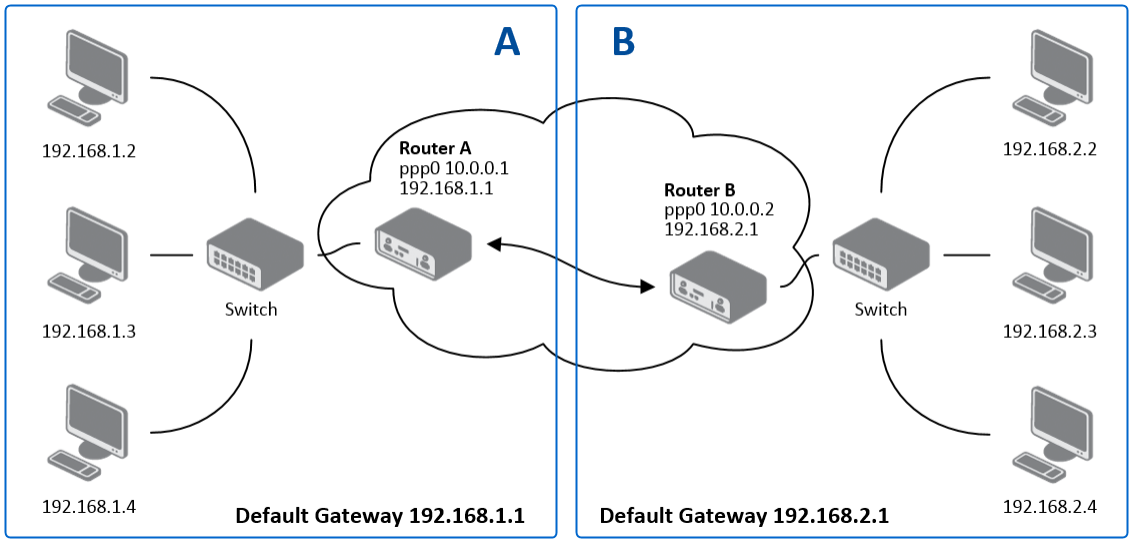
Změny v nastavení se projeví po stisknutí tlačítka *Apply*.



Obrázek 42: Konfigurace PPTP tunelu

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

3.14.1 Příklad konfigurace PPTP tunelu



Obrázek 43: 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 46: Příklad konfigurace PPTP tunelu

3.15 Services

3.15.1 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.

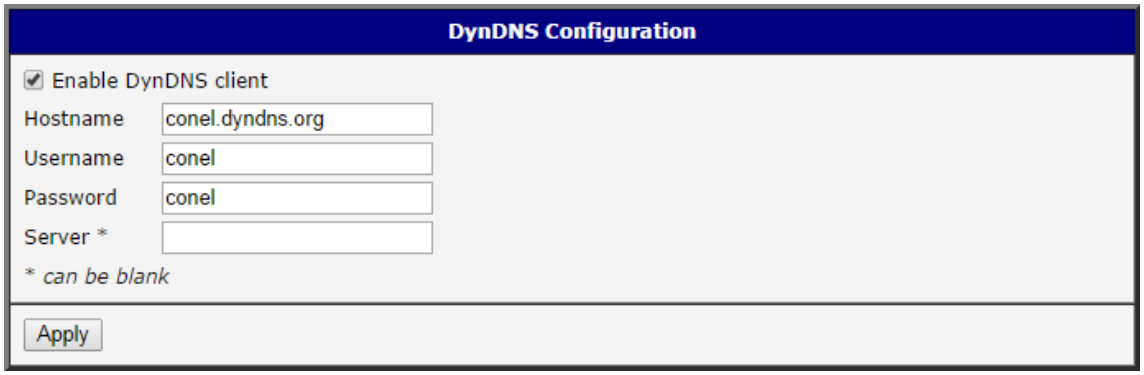
Konfiguraci DynDNS klienta lze vyvolat volbou položky *DynDNS* v menu. V okně lze definovat doménu třetího řádu registrovanou na serveru www.dyndns.org a údaje k účtu u této služby.

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.
	`www.spdns.de`
	`www.dnsdynamic.org`
	`www.noip.com`
	Pokud tato položka zůstane nevyplněna, používá se výchozí server members.dyndns.org.

Tabulka 47: Konfigurace DynDNS

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

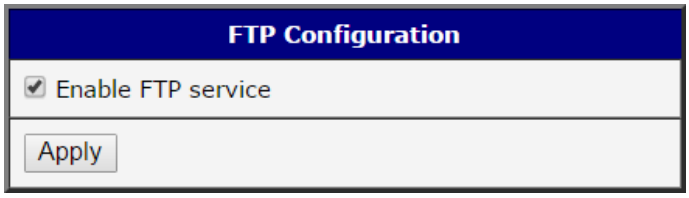


Obrázek 44: Příklad nastavení DynDNS

Pro vzdálený přístup ke konfiguraci routeru je nutné tento přístup povolit ještě v konfiguraci NAT (ve spodní části formuláře), viz kap. 3.9.

3.15.2 FTP

FTP protokol (File Transfer Protocol) umožňuje přenos souborů mezi routerem a jiným zařízením v počítačové síti. Konfigurační okno FTP serveru je možno otevřít volbou položky *FTP*, která se nachází ve složce menu *Services*. Zaškrtnutím položky *Enable FTP service* je na routeru povolena funkce FTP serveru.



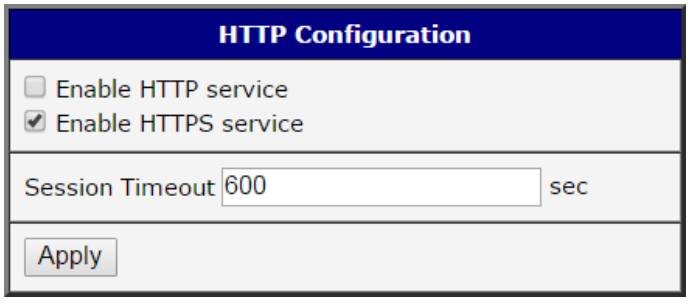
Obrázek 45: Povolení FTP serveru

3.15.3 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 48: Parametry konfigurace HTTP a HTTPS služeb



Obrázek 46: Konfigurace HTTP a HTTPS služeb

3.15.4 NTP

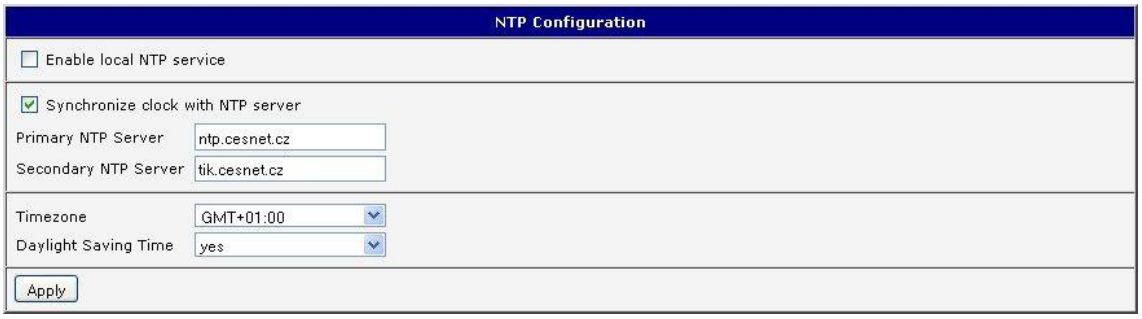
Konfiguraci NTP klienta lze vyvolat volbou položky *NTP* v menu. NTP (Network Time Protocol) umožňuje pravidelně nastavovat přesný čas do routeru ze serverů, které přesný čas na síti poskytují.

- Parametr *Enable local NTP service* nastaví router do režimu, při němž funguje jako NTP server pro ostatní zařízení v lokální síti za routerem.
- Parametr *Synchronize clock with NTP server* nastaví router do režimu NTP klienta, kdy každých 24 hodin router automaticky seřídí vnitřní hodiny.

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

Tabulka 49: 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 47: Příklad nastavení NTP

3.15.5 SNMP

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

SNMP (Simple Network Managment Protocol) poskytuje stavové informace o prvcích sítě, jakými jsou routery nebo koncové počítače. 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*.

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 50: 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 51: Konfigurace SNMPv3

Dále je možná tato konfigurace:

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

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

Tabulka 52: Konfigurace SNMP – MBUS

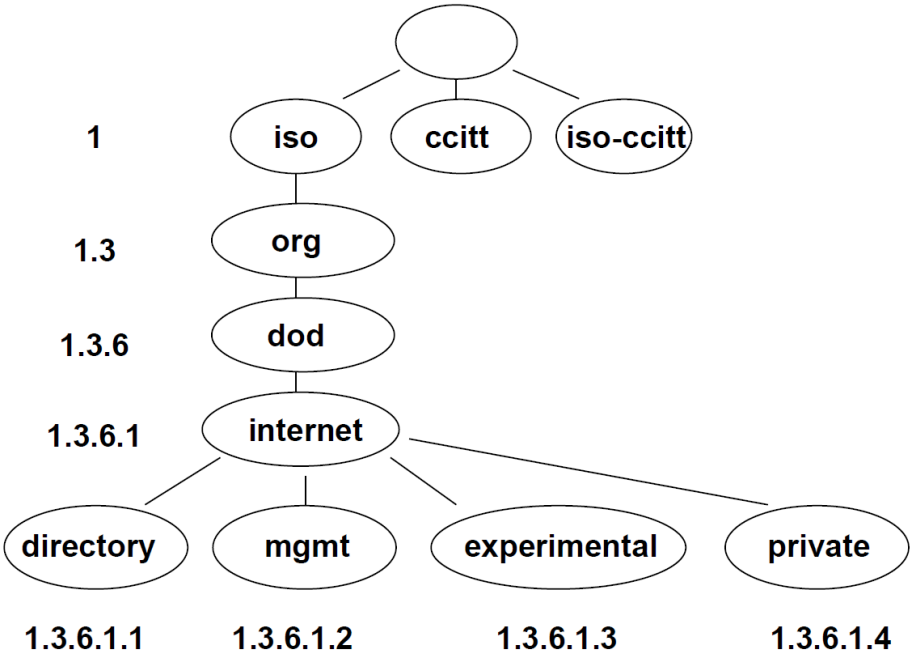
Parametry *Enable XC-CNT extension* a *Enable M-BUS extension* nemohou být zaškrtnuty **zároveň**.

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

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

Tabulka 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 48: 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 binárním vstupu a výstupu. K tomuto účelu je 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)

Tabulka 54: Vnitřní proměnné pro binární vstup a výstup

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

OID	Význam
.1.3.6.1.4.1.30140.2.1.1.0	Analogový vstup AN1 (rozsah 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogový vstup AN2 (rozsah 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Čítačový vstup CNT1 (rozsah 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Čítačový vstup CNT2 (rozsah 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binární vstup BIN1 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binární vstup BIN2 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binární vstup BIN3 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.8.0	Binární vstup BIN4 (hodnoty 0,1)
.1.3.6.1.4.1.30140.2.1.9.0	Binární výstup OUT1 (hodnoty 0,1)

Tabulka 55: Vnitřní proměnné pro CNT port

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

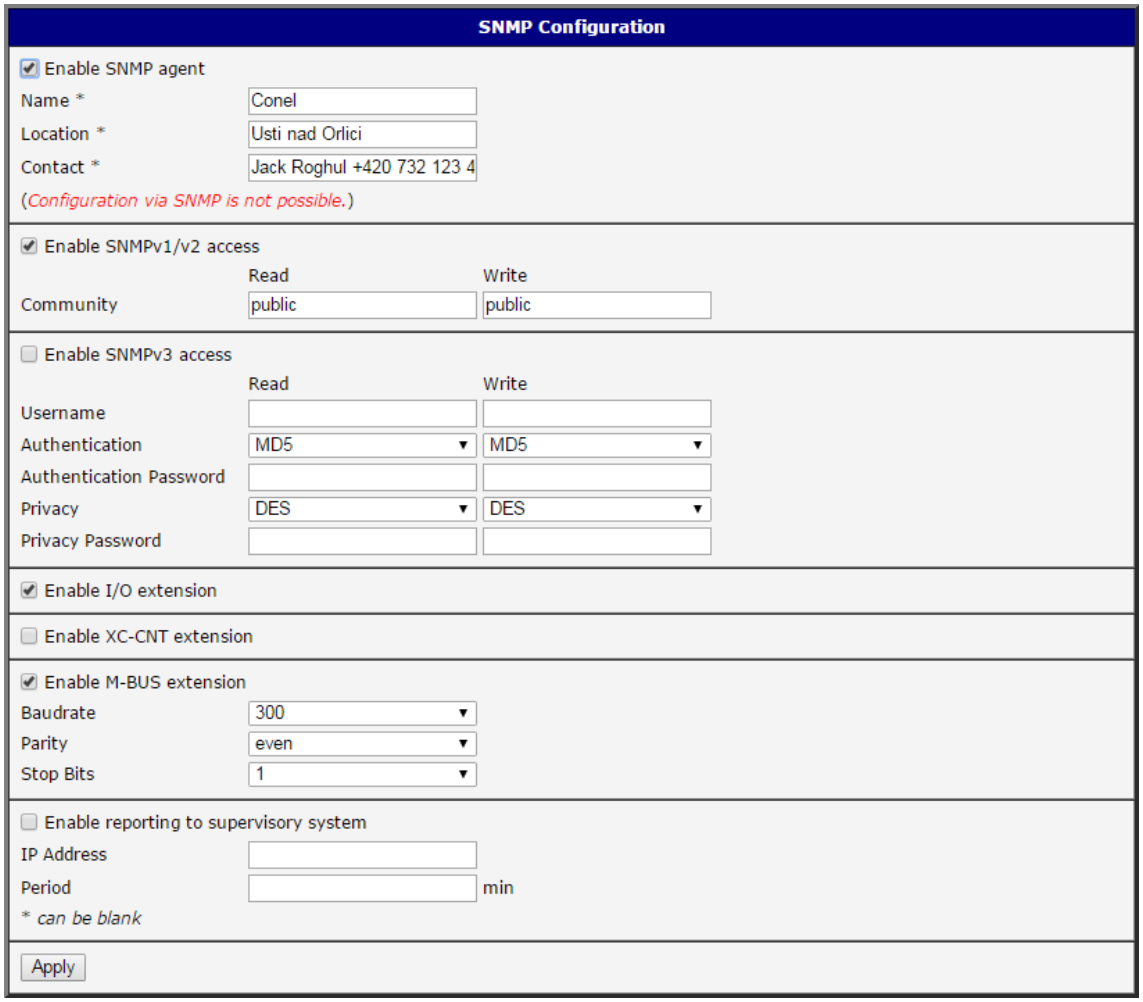
OID	Význam
.1.3.6.1.4.1.30140.2.2.<address>.1.0	IdNumber – číslo měřiče
.1.3.6.1.4.1.30140.2.2.<address>.2.0	Manufacturer – výrobce
.1.3.6.1.4.1.30140.2.2.<address>.3.0	Version – specifikuje verzi měřiče
.1.3.6.1.4.1.30140.2.2.<address>.4.0	Medium – typ měřeného média
.1.3.6.1.4.1.30140.2.2.<address>.5.0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

Tabulka 56: Vnitřní proměnné pro M-BUS port

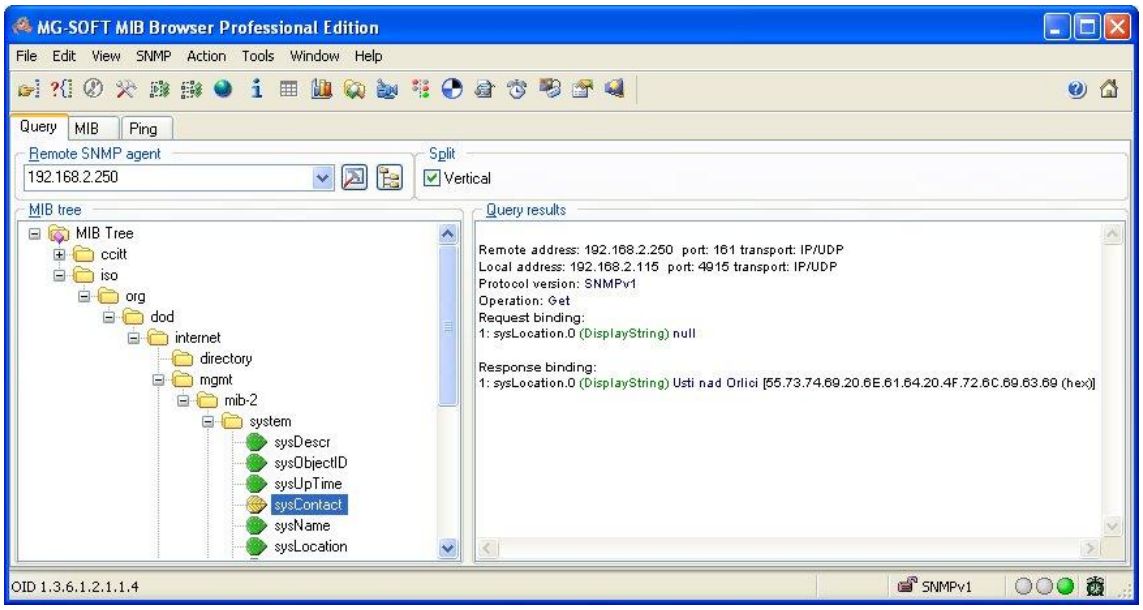
Adresa měřiče může být z rozsahu 0..254, přičemž 254 je broadcast.

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

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



Obrázek 49: Příklad SNMP konfigurace



Obrázek 50: 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

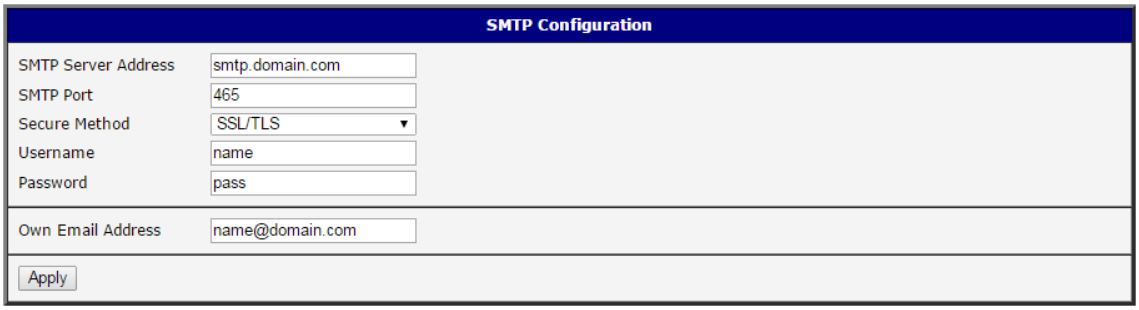
3.15.6 SMTP

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

Položka	Popis
SMTP Server Address	Doménová nebo IP adresa 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 57: Konfigurace SMTP klienta

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



Obrázek 51: Příklad konfigurace SMTP klienta

Samotné emaily lze posílat ze Startup skriptu (položka *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 name@domain.com –s "subject" –m "message" –a c:\directory\abc.doc –r 5

Tento příkaz odešle e-mail na adresu name@domain.com s předmětem zprávy *"subject"*, tělem zprávy *"message"* a přílohou *"abc.doc"* z adresáře c:\directory\. Router má k dispozici pět pokusů o odeslání.

3.15.7 SMS

Konfigurační formulář *SMS Configuration* není dostupný pro routery XR5i v2.

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.
Send SMS when binary input on expansion port (BIN1 – BIN4) is active	Automatické poslání SMS při aktivním binárním výstupu na volitelné CNT desce, jejíž text je určen parametrem *BIN1 – SMS* až *BIN4 – SMS*.
Add timestamp to SMS	Přidává časovou značku (razítko) do poslaných SMS. Tato značka má fixní formát YYYY-MM-DD hh:mm:ss.
Phone Number 1	Telefonní číslo pro odesílání automaticky generovaných SMS.
Phone Number 2	Telefonní číslo pro odesílání automaticky generovaných SMS.
Phone Number 3	Telefonní číslo pro odesílání automaticky generovaných SMS.
Unit ID	Pojmenování routeru, které bude zasláno v SMS.
BIN0 – SMS	Text SMS při aktivaci prvního bin. vstupu na routeru.
BIN1 – SMS	Text SMS při aktivaci bin. vstupu 1 na CNT desce.
BIN2 – SMS	Text SMS při aktivaci bin. vstupu 2 na CNT desce.
BIN3 – SMS	Text SMS při aktivaci bin. vstupu 3 na CNT desce.
BIN4 – SMS	Text SMS při aktivaci bin. vstupu 4 na CNT desce.

Tabulka 58: 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 59: 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 (APN1)
go online sim 2	Přepnutí na druhou SIM kartu (APN2)
go online	Přepne router do online režimu
go offline	Ukončení spojení
set out0=0	Nastaví výstup I/O konektoru na 0
set out0=1	Nastaví výstup I/O konektoru na 1
set out1=0	Nastaví výstup volitelného portu CNT na 0
set out1=1	Nastaví výstup volitelného portu CNT na 1
set profile std	Nastavení standardního profilu

Pokračování na následující straně

Pokračování z předchozí strany

SMS	Význam
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 60: Význam ovládacích SMS

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

SMS	Význam
Baudrate	Komunikační rychlost na volitelném portu 1.

Tabulka 61: Posílání/Příjem zpráv na sériovém portu 1

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

SMS	Význam
Baudrate	Komunikační rychlost na volitelném portu 2.

Tabulka 62: Posílání/Příjem zpráv na sériovém portu 2

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

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

Tabulka 63: 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 Conel. Na ostatní příkazy je vždy posílána odpověď *OK*. Není podporováno zpracování složených AT příkazu (oddělených středníkem), tudíž na ně router posílá odpověď *ERROR*.

AT příkaz	Popis
AT+CGMI	Identifikuje výrobce daného zařízení
AT+CGMM	Vypisuje identifikační označení zařízení
AT+CGMR	Vypisuje informaci o verzi systému
AT+CGPADDR	Vrací IP adresu rozhraní ppp0
AT+CGSN	Zobrazí sériové číslo zařízení
AT+CIMI	Vrací hodnotu čísla označovaného jako IMSI (unikátní číslo pro SIM kartu)
AT+CMGD	Mazání SMS zprávy podle jejího indexu
AT+CMGF	Nastavuje režim psaní SMS zpráv
AT+CMGL	Vypisuje seznam uložených SMS zpráv
AT+CMGR	Čtení určité SMS zprávy (všechny SMS mají svůj index)
AT+CMGS	Posílá SMS na uvedené telefonní číslo
AT+CMGW	Ukládá zprávu do paměti
AT+CMSS	Odesílá zprávu z paměti (na základě zadané pozice zprávy)
AT+COPS?	Identifikuje aktuálně dostupné mobilní sítě
AT+CPIN	Dotazování a zadávání PIN kódu
AT+CPMS	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 64: AT příkazy pro práci s SMS

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

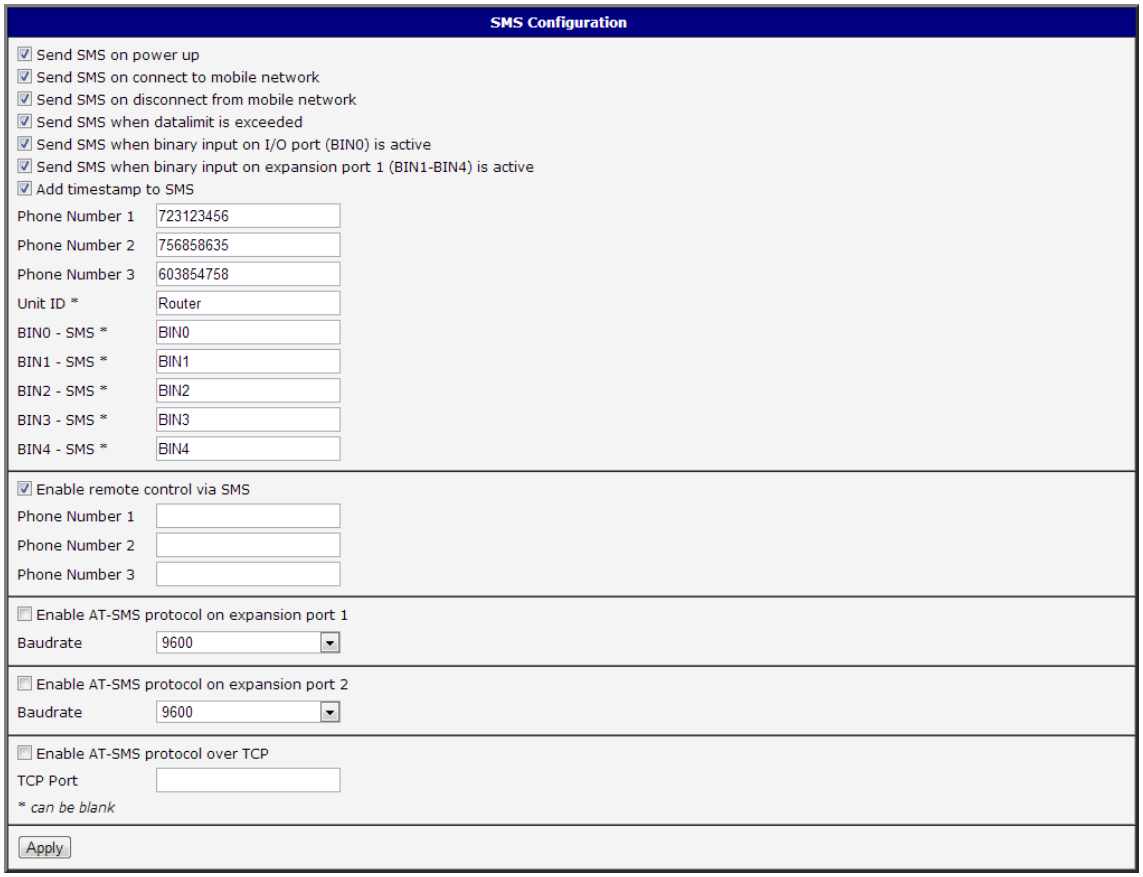
Příklady SMS konfigurace

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.

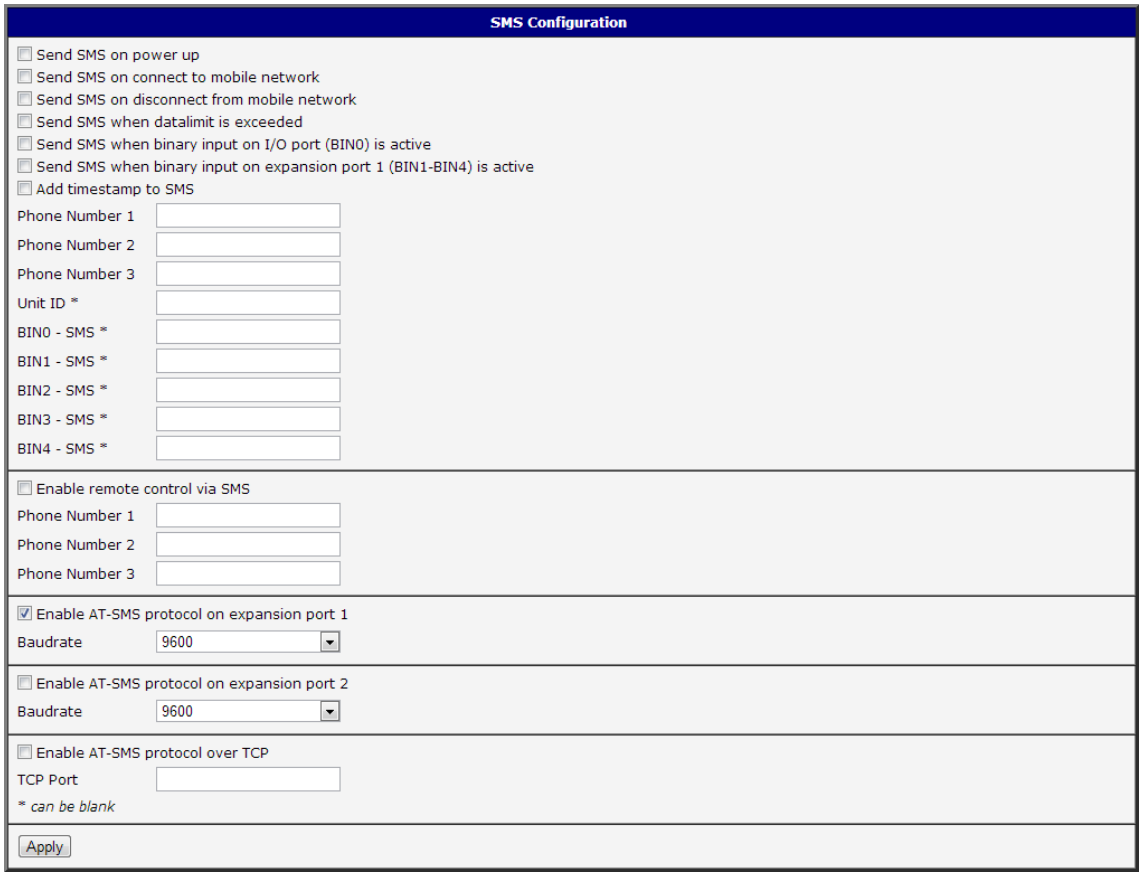
Při sestavení spojení přijde na uvedené telefonní číslo SMS ve tvaru:
Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

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



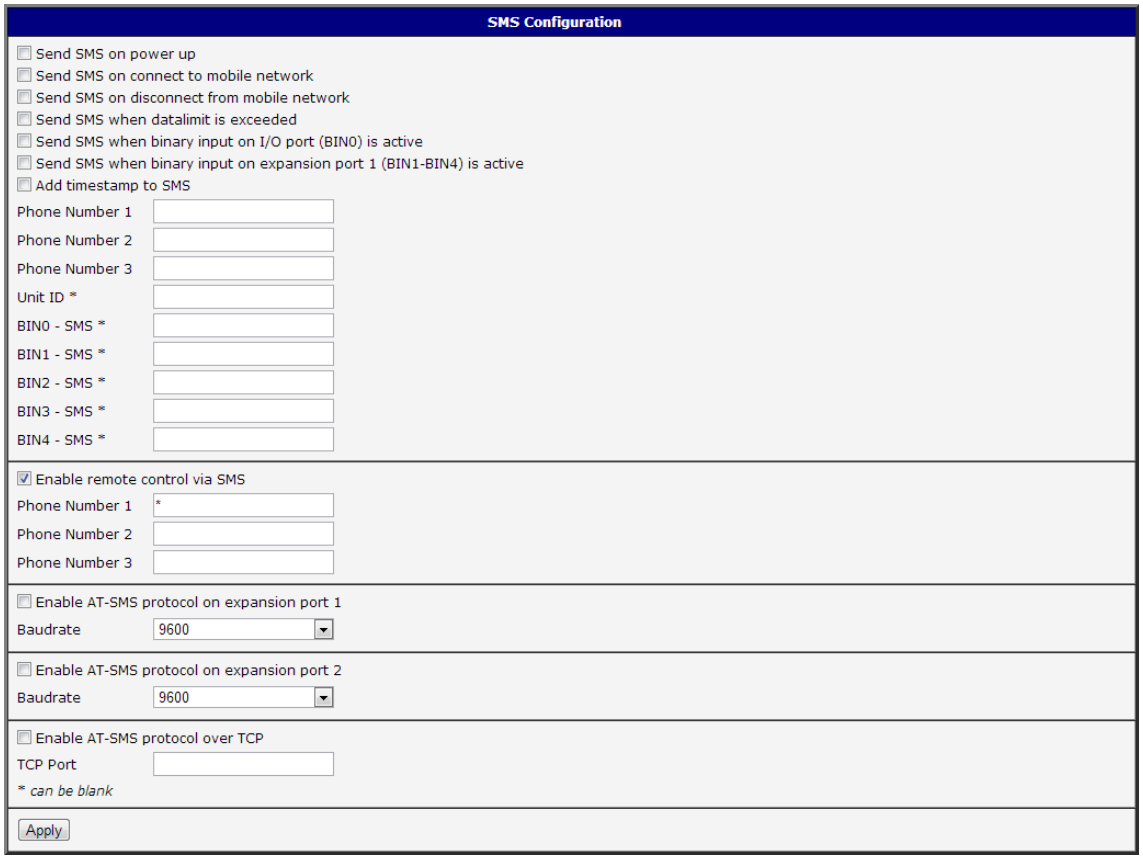
Obrázek 52: Příklad 1 – Konfigurace SMS

Příklad 2: Nastavení routeru pro posílání SMS zpráv přes sériové rozhraní portu 1.



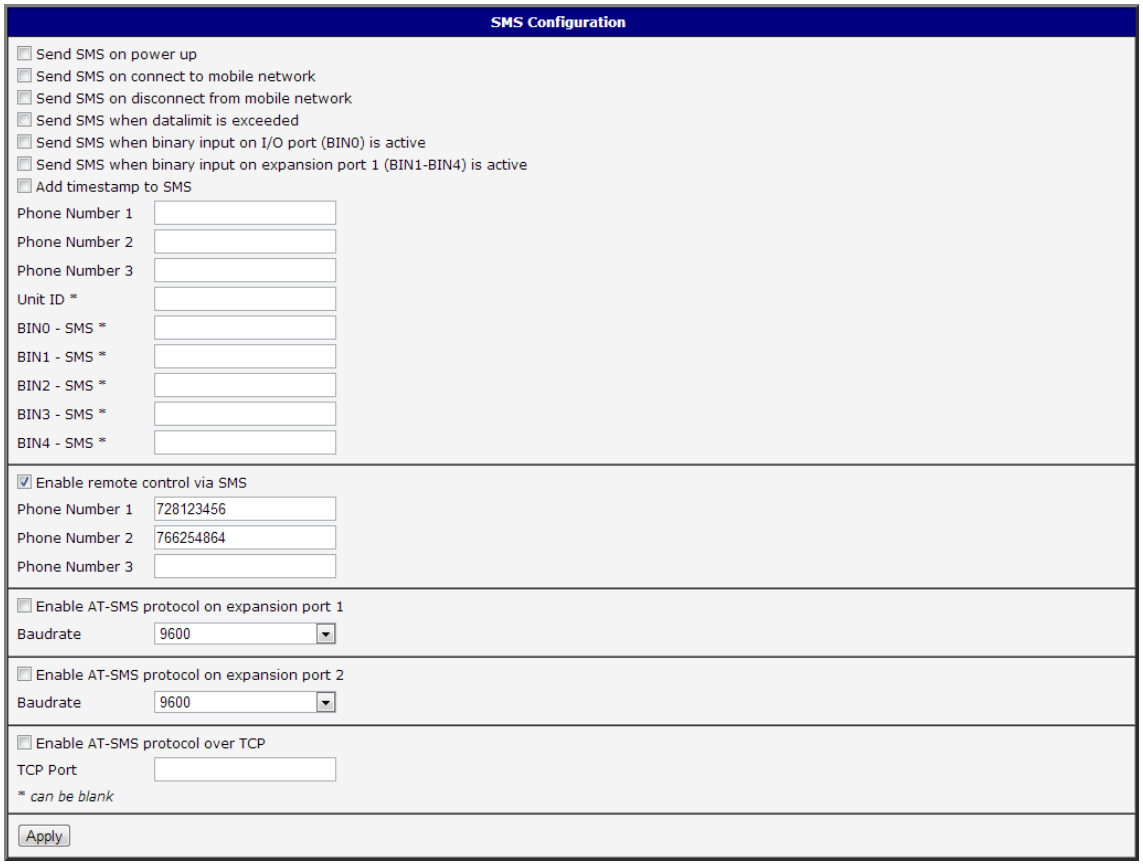
Obrázek 53: Příklad 2 – Konfigurace SMS

Příklad 3: Nastavení routeru pro ovládání pomocí SMS zpráv z libovolného tel. čísla.



Obrázek 54: Příklad 3 – Konfigurace SMS

Příklad 4: Nastavení routeru pro ovládání pomocí SMS zpráv ze dvou tel. čísel.



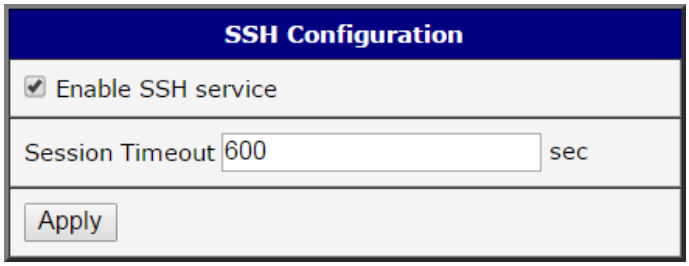
Obrázek 55: Příklad 4 – Konfigurace SMS

3.15.8 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.

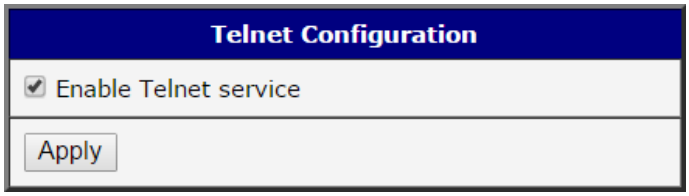
Tabulka 65: Parametry konfigurace SSH služby



Obrázek 56: Konfigurace SSH služby

3.15.9 Telnet

Telnet je protokol využívaný k vytvoření oboustranné textově orientované interaktívní komunikace s routerem. Konfiguraci Telnet serveru lze vyvolat volbou položky *Telnet* ve složce *Services*. Zaškrtnutím položky *Enable Telnet service* dojde k povolení Telnet serveru na routeru.



Obrázek 57: Povolení služby Telnet

3.16 Konfigurace volitelného portu

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

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.

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.
TCP Port	TCP/UDP port na kterém probíhá komunikace.
Inactivity Timeout	Časový úsek, po kterém se přeruší TCP/UDP spojení v případě neaktivity.

Tabulka 66: Konfigurace volitelného portu – sériové rozhraní

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 67: 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

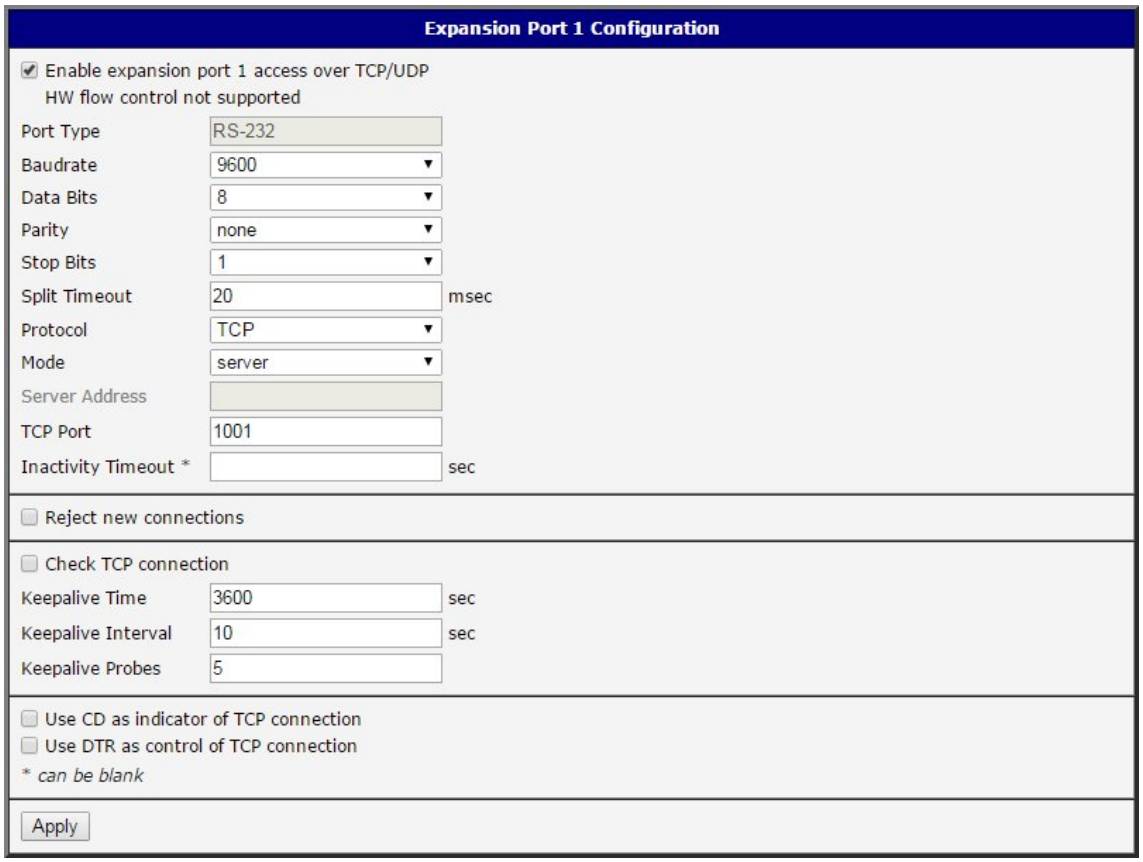
Tabulka 68: Popis signálu CD

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

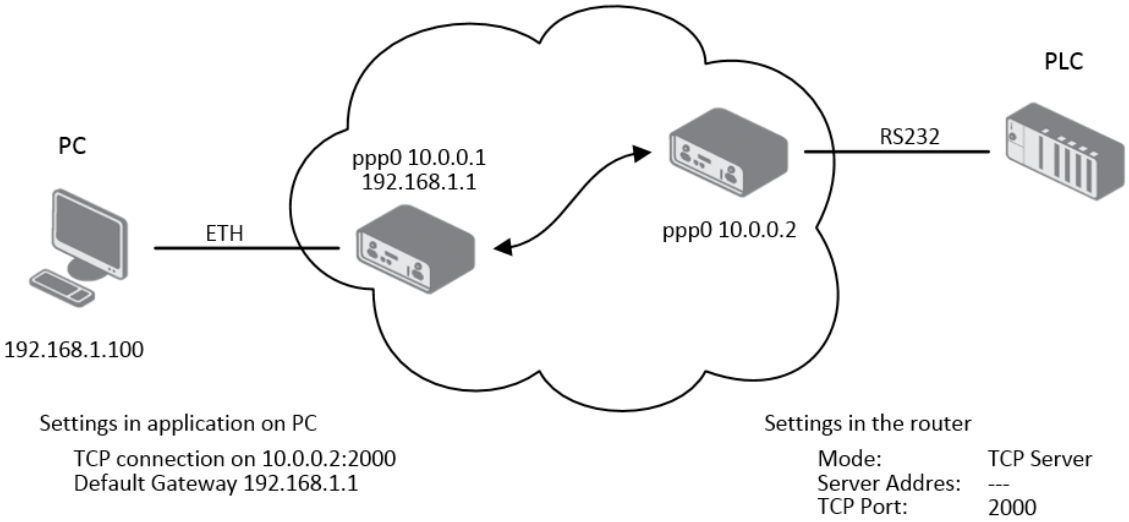
Tabulka 69: Popis signálu DTR

Počínaje firmwarem verze 3.0.9 je k dispozici program zvaný *getty*, který umožňuje připojení uživatele do routeru přes sériovou linku (router musí mít osazen volitelný port RS232!). Getty zobrazí přihlašovací prompt a po zadání přihlašovacího jména ho předá programu login, který se zeptá na heslo, ověří jej a spustí shell. Po přihlášení je tedy možné systém spravovat stejně jako by byl uživatel připojený přes telnet.

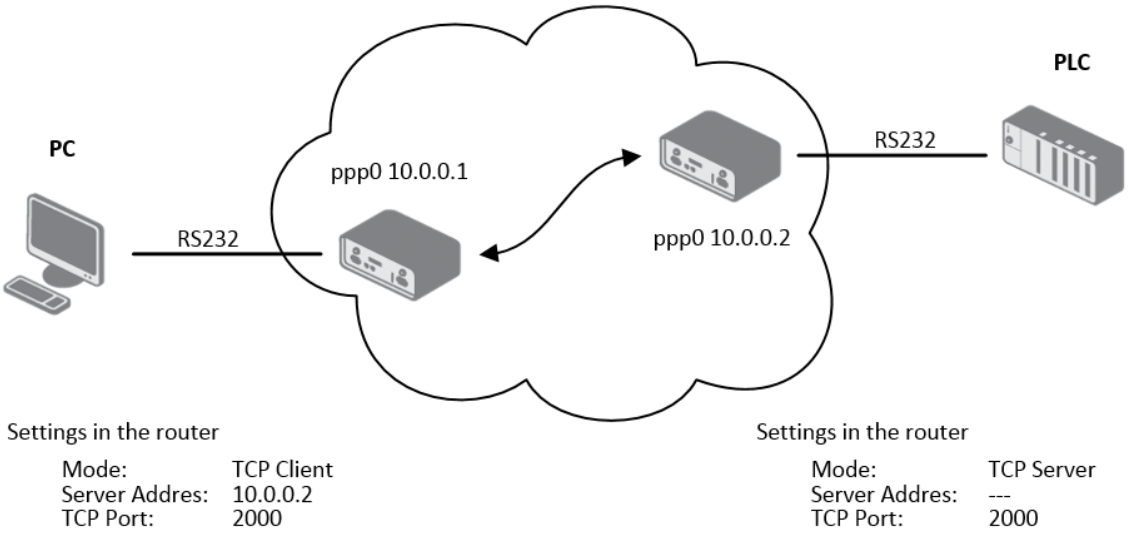


Obrázek 58: Konfigurace volitelného portu

Příklady konfigurace volitelného portu:



Obrázek 59: Příklad nastavení komunikace z Ethernetu na sériovou linku



Obrázek 60: Příklad konfigurace sériového rozhraní

3.17 Konfigurace USB portu

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

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

Tabulka 70: Konfigurace USB portu 1

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 71: Konfigurace USB portu 2

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

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

Tabulka 72: 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).

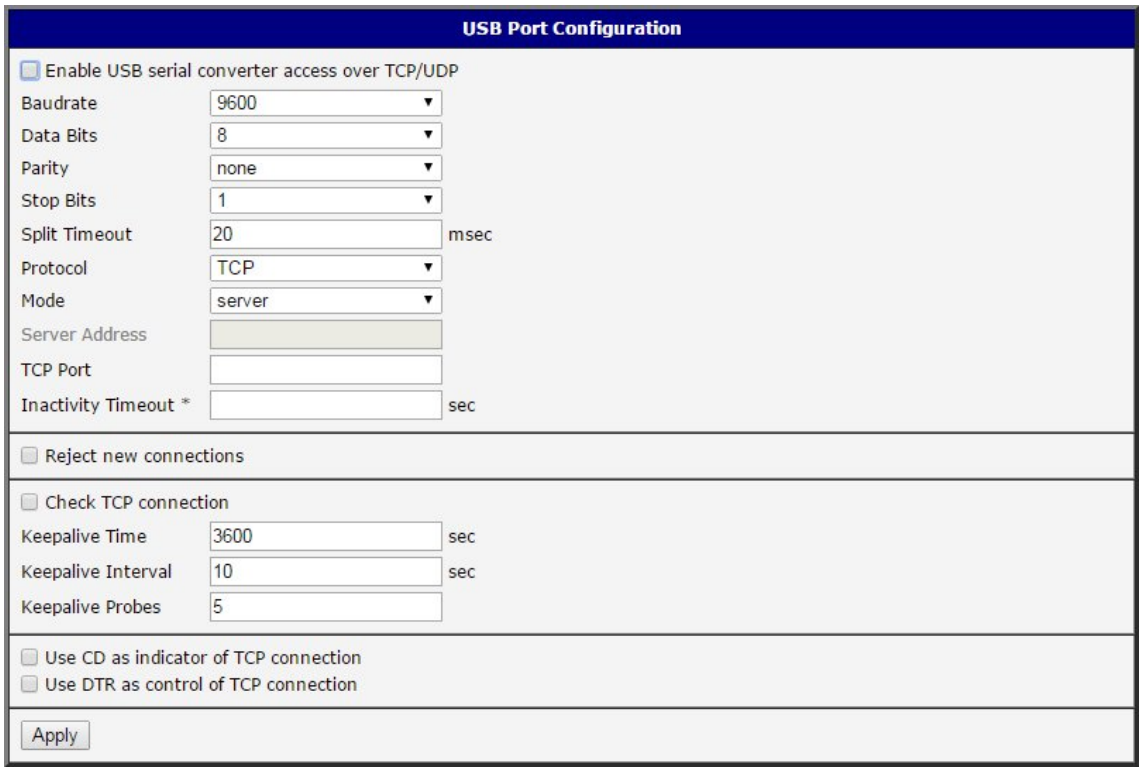
DTR	Popis chování serveru	Popis chování klienta
Active	Router povolí sestavení TCP spojení	Router sestaví TCP spojení
Nonactive	Router nepovolí sestavení TCP spojení	Router rozpojí TCP spojení

Tabulka 73: Popis signálu DTR

Podporované USB/RS232 převodníky:

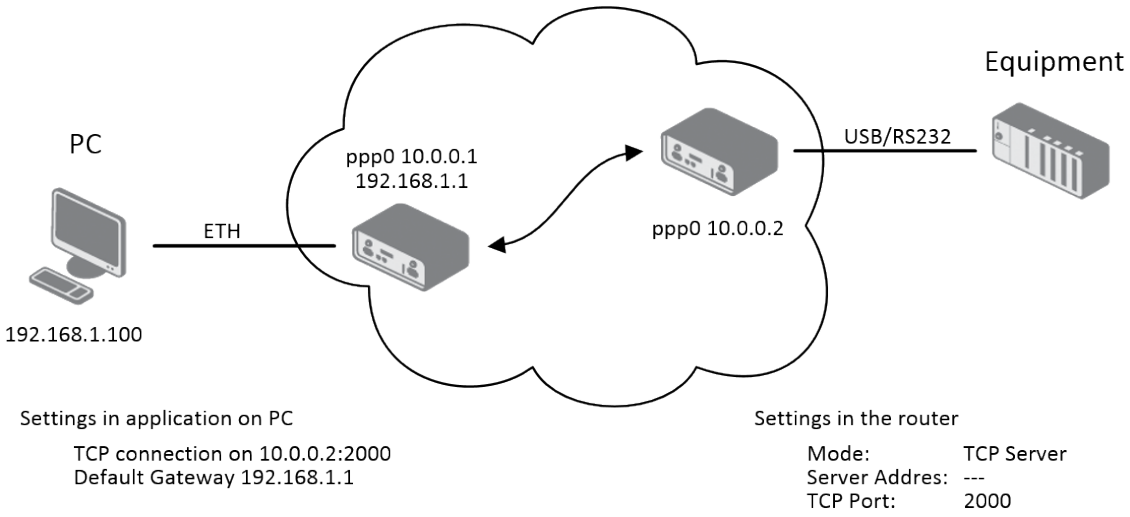
- FTDI
- Prolific PL2303
- Silicon Laboratories CP210×

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

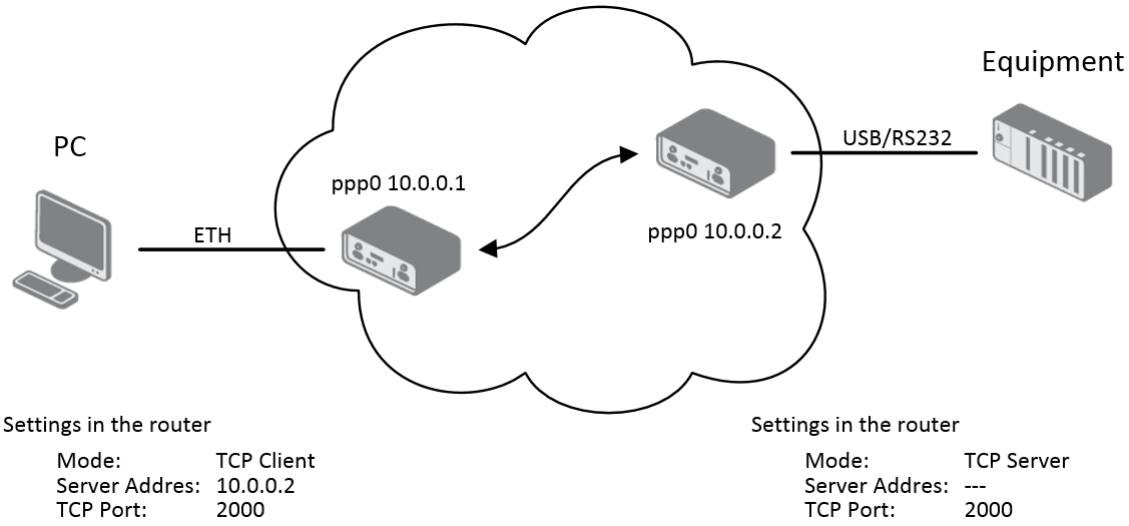


Obrázek 61: Konfigurace USB

Příklady konfigurace USB portu:



Obrázek 62: Příklad 1 – nastavení USB portu



Settings in the router

Mode:	TCP Client
Server Addres:	10.0.0.2
TCP Port:	2000

Settings in the router

Mode:	TCP Server
Server Addres:	---
TCP Port:	2000

Obrázek 63: Příklad 2 – nastavení USB portu

3.18 Skripty (Scripts)

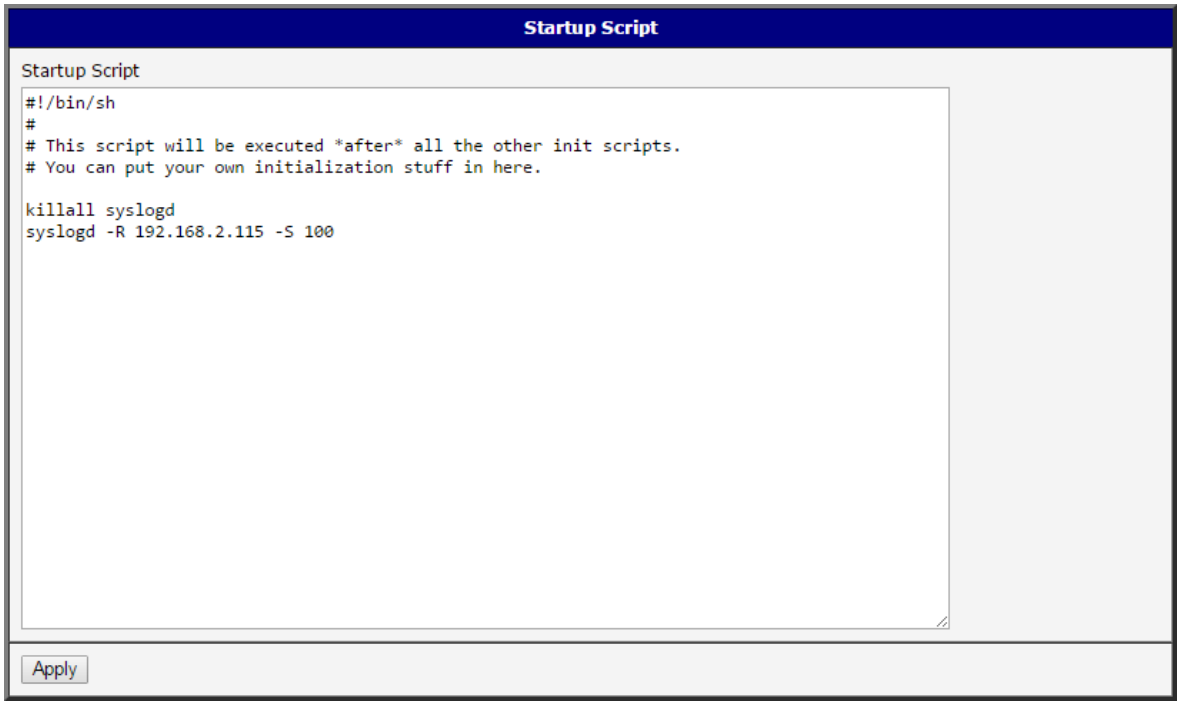
Na stránce *Scripts* v sekci *Configuration* lze definovat vlastní shellové skripty, které jsou spoštěny ve specifických situacích. Položka *Scripts* v menu se po kliknutí rozvine a objeví se možnosti *Startup Script* a *Up/Down*, které je možno definovat. Pro více příkladů skriptů a seznam možných příkazů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

3.18.1 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.

Příklad Startup skriptu: 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.



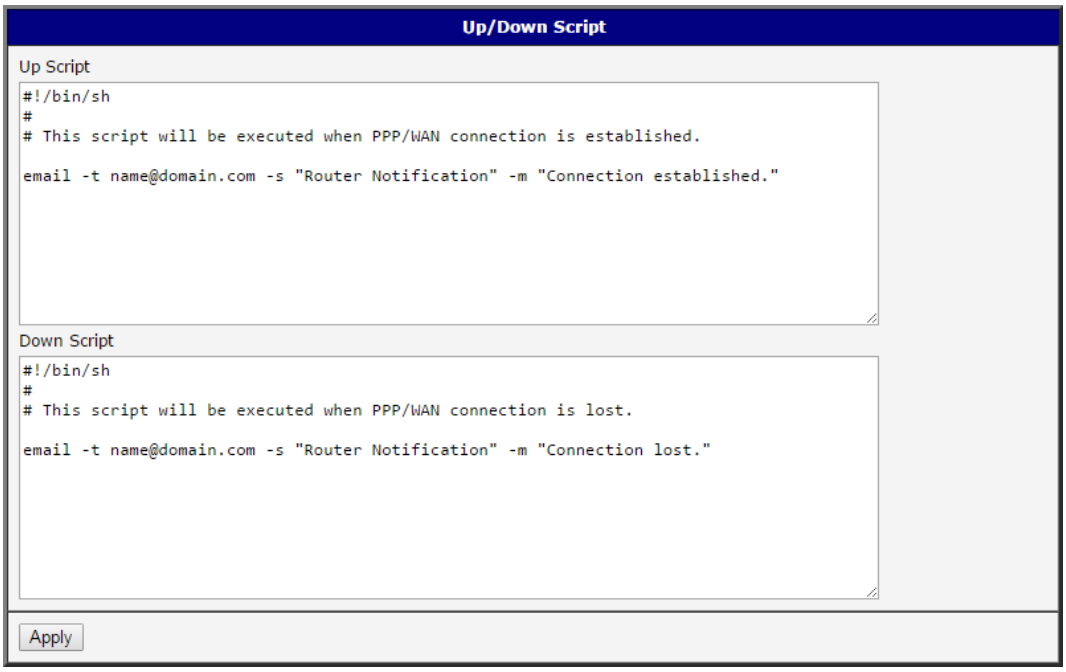
Obrázek 64: Příklad Startup scriptu

3.18.2 Up/Down Script

Na stránce *Up/Down* je možné vytvářet vlastní skripty, které jsou spouštěny když dojde k (mobilnímu) připojení nebo odpojení od internetu. *Up/Down Script* se spouští pouze při připojení či odpojení internetu. 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.

Příklad 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*.



Obrázek 65: Příklad Up/Down skriptu

3.19 Konfigurace automatické aktualizace

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

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

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

Položka	Popis
Source	Nastavuje, odkud bude router aktuální firmware stahovat: • **HTTP(S)/FTP(S) server** – Aktualizace se stahují z adresy zadané v položce *Base URL*, kterou je specifikován protokol, který se má použít: HTTP, HTTPS, FTP nebo FTPS. • **USB flash drive** – Router hledá aktuální firmware v kořenovém adresáři zařízení připojeného do USB portu. • **Both** – Router hledá aktuální firmware z obou zdrojů.
Base URL	Umožňuje zadat základní část doménového jména nebo IP adresy serveru, ze které se bude firmware nebo konfigurace routeru stahovat. 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 74: 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*.

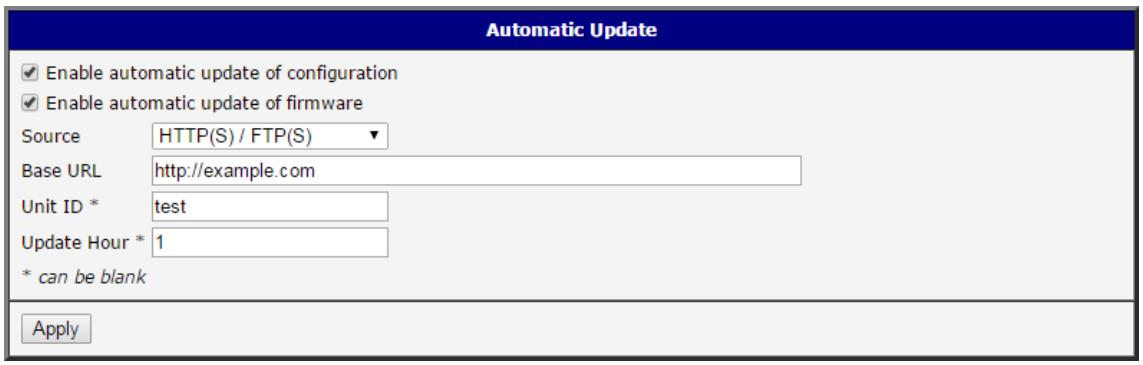
Název stahovaného firmware se skládá z parametru *Base URL*, typu routeru a přípony *bin*. Správné jméno souboru firmware je vypsáno na stránce *Update Firmware* v sekci *Administration*. Viz kapitola 5.11.

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.

Následující příklady zjišťují, jestli je k dispozici nový firmware nebo konfigurace a případně provádí aktualizaci každý den v 1:00 ráno. Příklad je uveden pro router LR77 v2.

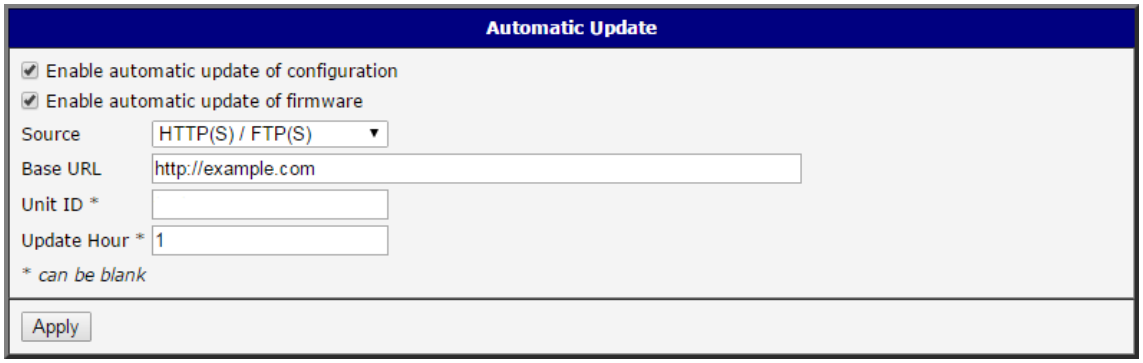
- Firmware: http://example.com/LR77-v2.bin
- Konfigurační soubor: http://example.com/test.cfg



Obrázek 66: Příklad automatické aktualizace 1

Následující příklady zjišťují, jestli je k dispozici nový firmware nebo konfigurace a případně provádí aktualizaci každý den v 1:00 ráno. Příklad je uveden pro router LR77 v2 s MAC adresou 00:11:22:33:44:55.

- Firmware: http://example.com/LR77-v2.bin
- Konfigurační soubor: http://example.com/00.11.22.33.44.55.cfg

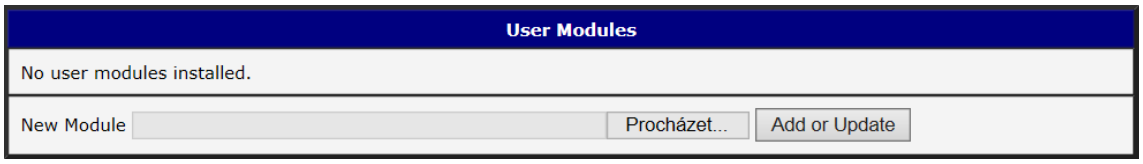


Obrázek 67: Příklad automatické aktualizace 2

4. Přizpůsobení

4.1 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*.

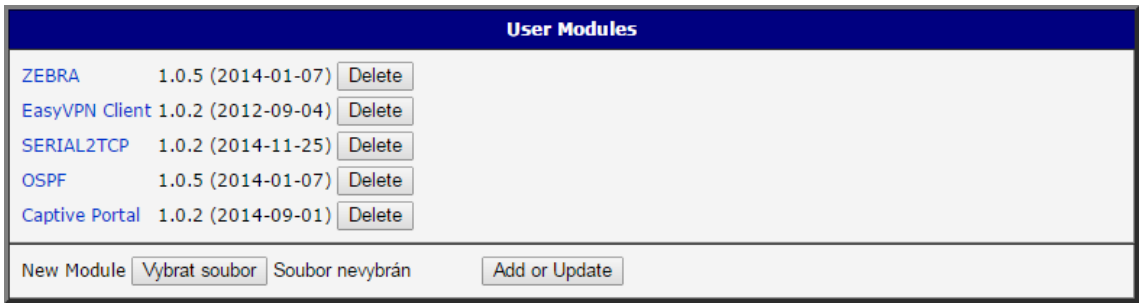


Obrázek 68: User modules

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 69: 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 75: 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.

5. Administrace

5.1 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 76: Přehled uživatelů

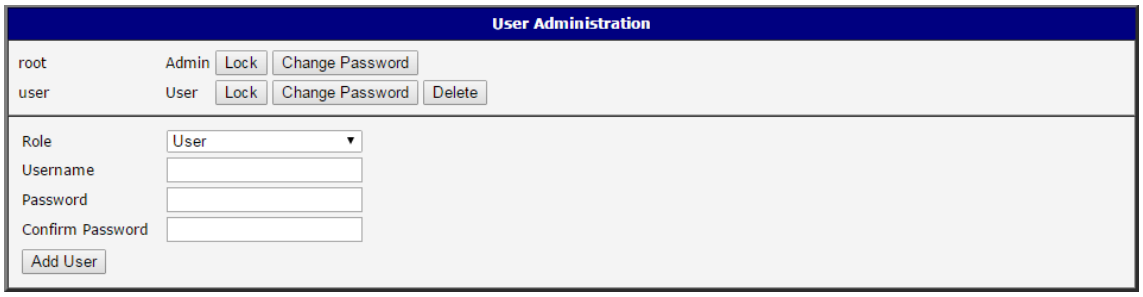
Pozor! Pokud uzamknete účet všem uživatelům s oprávněním *Admin*, nebude již možné tyto účty odemknout! To rovněž znamená, že stránka *Users* bude všem uživatelům nedostupná, protože uživatelé s oprávnění admin budou mít zamknuté účty a uživatelé users nemají dostatečné oprávnění.

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 77: Přidání nového uživatele

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

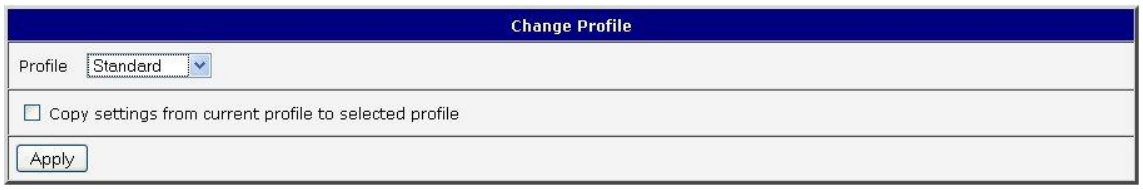


Obrázek 70: Users

5.2 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.

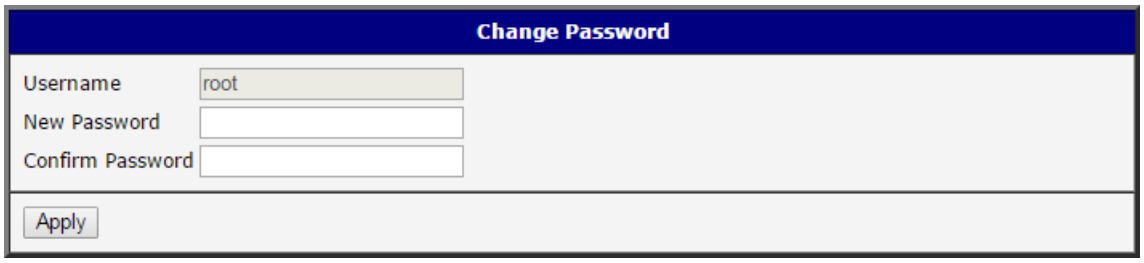


Obrázek 71: Změna profilu

5.3 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*.

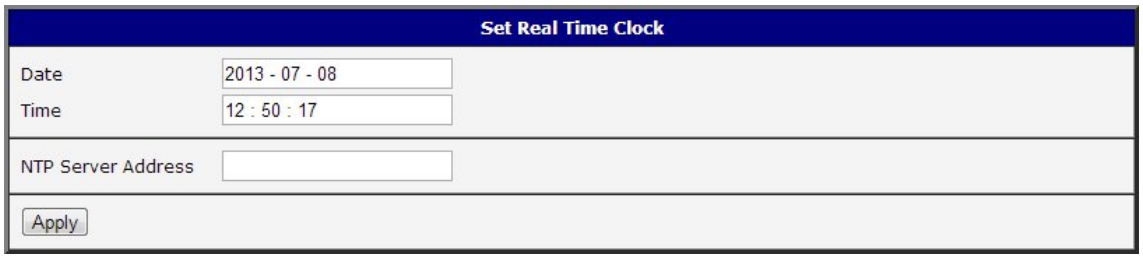
V základním nastavení routeru je heslo nastaveno defaultně na *root*. **Pro zajištění bezpečnosti sítě spravované routerem je nutné standardní heslo změnit.**



Obrázek 72: Změna přístupového hesla

5.4 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*.

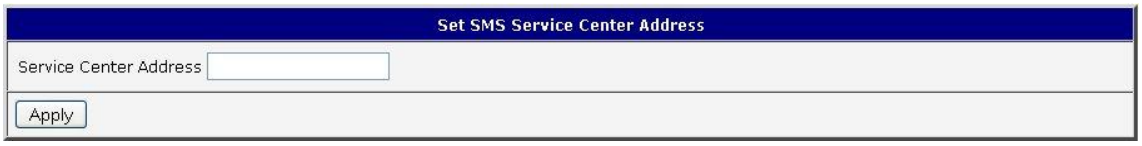


Obrázek 73: Nastavení vnitřních hodin

5.5 Nastavení SMS centra

Pro routery XR5i v2 není položka *Set SMS Service Center Address* dostupná.

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



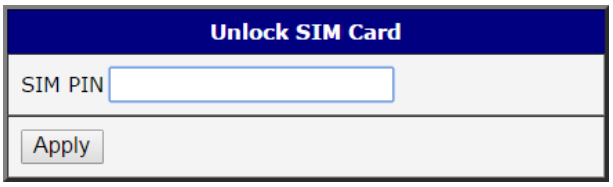
Obrázek 74: Nastavení SMS centra

5.6 Odemknutí SIM karty

Pro routery XR5i v2 není položka *Unlock SIM Card* dostupná.

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.



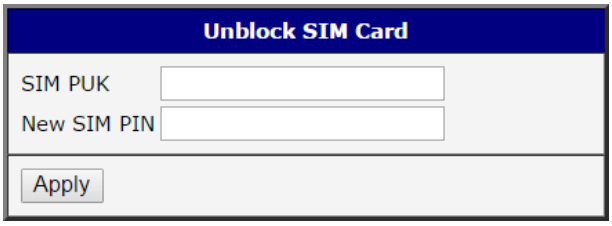
Obrázek 75: Odemknutí SIM karty

5.7 Odblokování SIM karty

Pro routery XR5i v2 není položka *Unblock SIM Card* dostupná.

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.

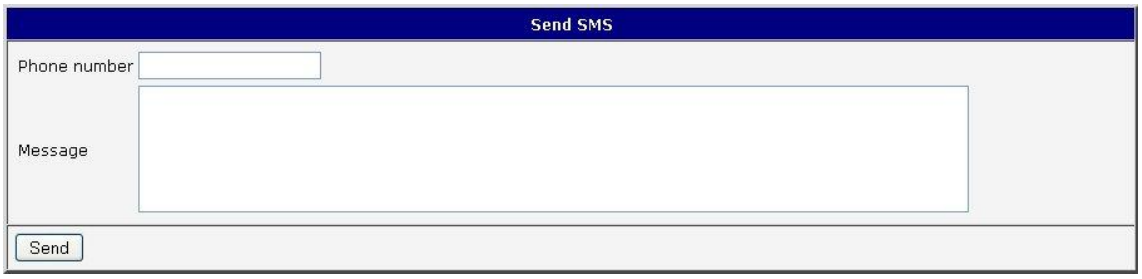


Obrázek 76: Odblokování SIM karty

5.8 Poslání SMS zprávy

Pro routery XR5i v2 není položka *Send SMS* dostupná.

Poslání SMS zprávy je možné v okně *Send SMS*. Po vložení telefonního čísla příjemce (*Phone number*) a textu SMS zprávy (*Message*) se zpráva odešle pomocí tlačítka *Send*. Lze posílat pouze zprávy standartní délky 160 znaků. (Pro posílání dlouhých SMS lze využít např. uživatelský modul pduSMS).



Obrázek 77: 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].

5.9 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.

5.10 Obnovení konfigurace

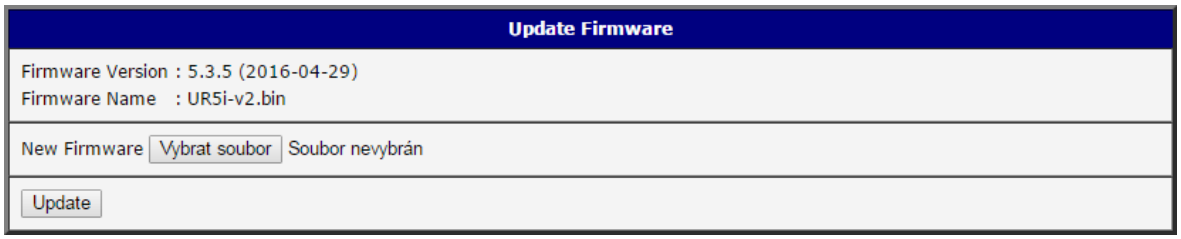
Pokud je potřeba obnovit konfiguraci routeru, je možné v položce *Restore Configuration* vybrat z vašeho počítače konfigurační soubor pomocí tlačítka *Procházet*.

Obrázek 78: Obnovení konfigurace

5.11 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 79: Aktualizace firmware

Během aktualizace firmwaru se vypíše následující výpis, který informuje o aktuálním průběhu. Progres programování FLASH paměti je znázorněn přibývajícími tečkami ('.').

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

Reboot in progress

Continue here after reboot.

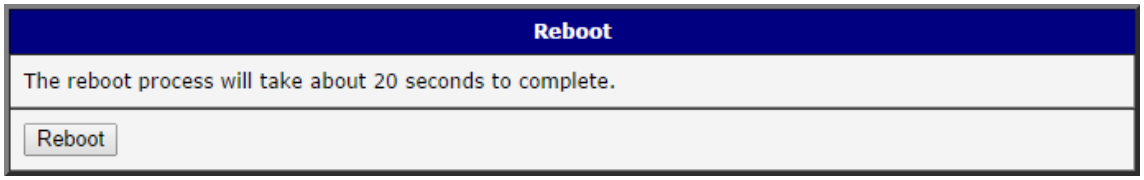
Po dokončení aktualizace firmware je router automaticky restartován.

Nahráním firmware jiného přístroje by mohlo dojít k poškození routeru!

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.

5.12 Reboot

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



Obrázek 80: Reboot

6. Konfigurace přes Telnet

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

Pro Telnet existují následující příkazy:

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

Pokračování na následující straně

Pokračování z předchozí strany

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

Tabulka 78: Telnet příkazy

7. 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 dává 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 potřeby 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.

8. Index

A

Access Point
- Informace ... 10

Add User ... 120
Aktualizace firmware ... 115, 126
Aktualizace konfigurace ... 115
APN ... 32
AT příkazy ... 97
Automatická aktualizace ... 115

B

Backup Routes ... 51
Bridge ... 20

D

Data limit ... 35
Default Gateway ... 20
Default SIM card ... 37
DHCP ... 20, 130
- Dynamic ... 21
- Static ... 21

DNS ... 130
DNS server ... 20, 34
Domain Name System ... *viz* DNS
DoS útoky ... 55
DynDNS ... 83

F

Firewall ... 54
- Filtrování forwardingu ... 54
- Filtrování příchozích paketů ... 54
- Ochrana proti DoS útokům ... 55

Firmware update ... 126
FTP ... 84

G

GRE ... 76, 130

H

Heslo ... 122
HTTP ... 85, 130
HTTPS ... 131

I

IPsec ... 68, 131
- Authenticate Mode ... 70
- Encapsulation Mode ... 69
- IKE Mode ... 69

IPv4 ... 131
IPv6 ... 131

L

L2TP ... 79, 131
LAN ... 131
- Primary LAN ... 20
- Secondary LAN ... 20

M

Mobilní síť ... 32
Multiple WANs ... 51, 52

N

Nastavení vnitřních hodin ... 122
NAT ... 58, 131
NTP ... 86, 132
NTP server ... 122

O

Object Identifier ... 89
Obnovení konfigurace ... 125
Odblokování SIM karty ... 124
Odemknutí SIM karty ... 123
OID ... 89
Okolní WiFi sítě ... 11
OpenVPN ... 63, 132
Ovládací SMS zprávy ... 96

P

Přístup k webové konfiguraci ... 2
Překlad síťových adres ... *viz* NAT
Přepínání mezi SIM kartami ... 35
PAT ... 58
PIN ... 123
Poslání SMS zprávy ... 125
PPPoE ... 41
PPPoE Bridge Mode ... 38
PPTP ... 81, 132
Profily ... 121
PUK ... 124

R

RADIUS ... 45
Reboot ... 127
Router
    Přístup ... 2

S

Sériová linka
    RS232 ... 105
    RS422 ... 105
    RS485 ... 105
Save Log ... 18
Save Report ... 18
Seřízení vnitřních hodin ... 86
SMS ... 95
SMS centrum ... 123
SMTP ... 93, 132
SMTPS ... 132
SNMP ... 87, 133
SSH ... 103, 133
Startup Script ... 113
System Log ... 18

T

TCP ... 133
Telnet ... 104, 128
Transmission Control Protocol ... *viz* TCP

U

Uživatelé ... 120
Uživatelský modul ... 118
UDP ... 133
Uniform resource locator ... *viz* URL
Up/Down Script ... 114
URL ... 133
USB
    USB/RS232 převodníky ... 110
USB Port ... 109
User Datagram Protocol ... *viz* UDP
Users ... 120

V

Výchozí heslo ... 2
Výchozí IP adresa ... 2
Výchozí uživatel ... 2
Virtual private network ... *viz* VPN
Volitelný Port
    CNT ... 105
    MBUS ... 105
    RS232 ... 105
    RS485/422 ... 105
VPN ... 133
VRRP ... 29, 134
Vzdálený přístup ... 59

W

WAN 134
WiFi 42
Autentizace 44
HW mód 43
Operační mód 42
WLAN 49
Operační mód 49

Z

Zálohování konfigurace 125
Zálohované připojení 51
Změna hesla 122
Změna profilu 121

9. 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