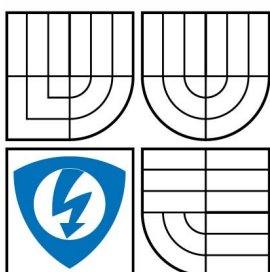


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNologiÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

HOTSPOTOVÝ SYSTÉM PRO VÍCE OPERÁTORŮ

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

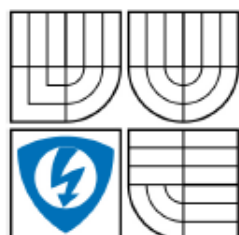
AUTOR PRÁCE
AUTHOR

Bc. ROMAN STRMISKA

VEDOUCÍ PRÁCE
SUPERVISOR

doc. Ing. KAREL BURDA, CSc.

BRNO 2009



VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Roman Strmiska
Ročník: 2

ID: 89857
Akademický rok: 2008/2009

NÁZEV TÉMATU:

Hotspotový systém pro více operátorů

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a popište problematiku přístupových bodů bezdrátových sítí (hotspotů) podle standardů řady IEEE 802.11. Popište i základní postup pro jejich plánování a také legislativu, která s jejich provozováním souvisí. Na tomto základě navrhnete koncepci hotspotového systému, který by přes společné rádiové rozhraní umožnil klientům využívat služby různých poskytovatelů internetového připojení (operátorů). Možnost připojení do systému musí mít pouze oprávnění klienti, přenosová rychlost pro klienty musí být nastavitelná a přenesená data musí být účtovatelná. Navržený systém prakticky vybudujte a otestujte. Výsledky testů zhodnotte.

DOPORUČENÁ LITERATURA:

- [1] Zandl, P.: Bezdrátové sítě WiFi - Praktický průvodce. Computer Press, Brno 2003.
- [2] Barken, L.: Jak zabezpečit bezdrátovou síť Wi-Fi. Computer Press, Brno 2004.

Termín zadání: 9.2.2009

Termín odevzdání: 26.5.2009

Vedoucí práce: doc. Ing. Karel Burda, CSc.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

ABSTRAKT DIPLOMOVÉ PRÁCE

Vysoké učení technické v Brně

Fakulta elektrotechniky a komunikačních technologií

ÚSTAV TELEKOMUNIKACÍ

Hotspotový systém pro více operátorů

Téma

Specializace: Telekomunikační a informační technika

Student: Bc. Roman Strmiska

Vedoucí práce: doc. Ing. Karel Burda, CSc.

Abstrakt :

Diplomová práce se zabývá návrhem a realizací hotspotového systému pro více operátorů, řeší problematiku QoS, účtování přenesených dat a distribuci služeb společným bezdrátovým rozhraním. Teoretická část práce je zaměřena na výběr vhodné technologie a objasnění legislativy, která s provozováním hotspotové sítě souvisí. Praktická část řeší volbu hardwaru, vlastní návrh a realizaci experimentální sítě. Na závěr jsou testovány přenosové parametry a funkčnost sítě.

Klíčová slova : hotspot, společné bezdrátové rozhraní, QoS, účtování přenesených dat

ABSTRACT OF MASTER'S THESES

Brno University of Technology

Faculty of Electrical Engineering and Communication

Department of Telecommunications

**Hotspot system for more Operators
Thesis**

Specialisation of study: Telecommunication, informatics
Student: Bc. Roman Strmiska
Supervisor: doc. Ing. Karel Burda, CSc.

Abstract :

Master's thesis deals with the design and realization of a hotspot system for more Operators, it solves problems of QoS, billing of transferred data and distribution of services via a common wireless interface. The theoretic part is oriented to the selection of a suitable technology and explanation of a legislation, which relates to an activity of the hotspot's network. The practical part solves the choice of hardware, design and realization of the experimental network. In conclusion are tested transit parameters of the network and its functionality.

Key words: hotspot, common wireless interface, QoS, billing of transferred data

Bibliografická citace

STRMISKA, R. *Hotspotový systém pro více operátorů*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 80 s. Vedoucí diplomové práce doc. Ing. Karel Burda, CSc.

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma **HOTSPOTOVÝ SYSTÉM PRO VÍCE OPERÁTORŮ** jsem vypracoval samostatně pod vedením vedoucího semestrálního projektu a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením tohoto projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne

.....
podpis autora

Obsah

1. ÚVOD	10
2. PLÁNOVÁNÍ HOTSPOTOVÉ SÍTĚ	11
2.1 Volba lokality.....	11
2.2 Velikost hotspotových buněk.....	11
2.3 Umístění hotspotu.....	12
2.4 Volba kmitočtového pásma.....	12
2.5 Standardy IEEE 802.11 v pásmu 2,4 GHz.....	14
2.5.1 Spektrum Wi-Fi signálu.....	15
2.5.2 Zabezpečení Wi-Fi.....	16
2.6 Parametry ovlivňující kvalitu radiového spoje	17
3. LEGISLATIVA PROVOZOVÁNÍ HOTSPOTOVÉ SÍTĚ.....	19
3.1 Provozování hotspotu bez nároku na zisk.....	19
3.2 Provozování hotspotu za účelem zisku.....	19
4. NÁVRH KONCEPCE HOTSPOTOVÉHO SYSTÉMU	22
4.1 Fyzická topologie systému.....	22
4.2 Logická topologie a adresace systému	24
4.3 Přístup uživatele do systému (první fáze).....	26
4.4 Přístup uživatele do systému (druhá fáze)	28
4.5 Přiřazení šířky pásma.....	28
4.6 Účtování přenesených dat	29
5. HARDWAROVÉ A SOFTWAREOVÉ VYBAVENÍ SÍTĚ	30
5.1 Centrální propojovací bod (CCP).....	30
5.2 Přístupový řídicí server (ACS).....	30
5.3 Hotspotový směrovač (HSR)	31
5.3.1 Operační systém.....	31
5.3.2 Základová deska a procesor	31
5.3.3 Bezdrátové karty a příslušenství	34
6. REALIZACE EXPERIMENTÁLNÍ SÍTĚ	36
6.1 Konfigurace hotspotového směrovače (HSR).....	38
6.1.1 Bezdrátový síťový adaptér.....	38

6.1.2 Konfigurace VLAN.....	41
6.1.3 Přemostění	42
6.1.4 IP adresace rozhraní	42
6.1.5 DHCP server.....	43
6.1.6 DNS	43
6.1.7 Směrovací tabulky a NAT	44
6.1.8 Firewall.....	45
6.1.9 Značkování paketů (Mangle).....	47
6.1.10 Virtuální hotspot.....	48
6.1.11 Radius klient.....	48
6.1.12 SNMP server	49
6.1.13 Kontrola šířky pásma a kvalita služeb (QoS).....	49
6.1.14 Ostatní služby	51
6.2 Konfigurace centrálního propoj. bodu (CCP).....	51
6.3 Konfigurace přístupového řídicího serveru (ACS)	52
6.3.1 Ethernetové síťové karty.....	52
6.3.2 Vzdálený přístup	53
6.3.3 Role doménového kontroleru.....	54
6.3.4 Mail server	54
6.3.5 Aplikační server (IIS).....	55
6.3.6 Autentizační servis (IAS)	56
6.3.7 Monitorování sítě HSR.....	59
6.3.7.1 Návrh topologie	59
6.3.7.2 Sledované služby	60
6.3.7.3 Notifikace	61
6.3.7.4 Syslog	62
6.3.8 Účtování přenesených dat – aplikace Cacti.....	62
6.3.8.1 Instalace Cacti.....	62
6.3.8.2 Princip funkce Cacti.....	64
6.3.8.3 Provozování Cacti.....	65
7. TESTOVÁNÍ EXPERIMENTÁLNÍ SÍTĚ	69
7.1 Ověření základních funkcí systému.....	69
7.2 Přenosové možnosti hotspotového směrovače.....	73
7.3 Kvalita služeb (QoS)	76

8. ZÁVĚR.....	77
9. SEZNAM POUŽITÝCH ZDROJŮ.....	79
10. SEZNAM POUŽITÝCH ZKRATEK	80

Seznam tabulek a obrázků

<i>Tabulka 1: Kriterium pro volbu kmitočtového pásma.....</i>	<i>13</i>
<i>Tabulka 2: Maximální počet kanálů pro Wi-Fi zařízení</i>	<i>14</i>
<i>Tabulka 3: Vlastnosti některých standardů.....</i>	<i>15</i>
<i>Obrázek 1: Fresnelova zóna</i>	<i>18</i>
<i>Obrázek 2: Fyzická topologie systému.....</i>	<i>23</i>
<i>Obrázek 3: Logická topologie systému + adresace</i>	<i>25</i>
<i>Obrázek 4: Místní přihlášení</i>	<i>26</i>
<i>Obrázek 5: Vzdálené přihlášení.....</i>	<i>27</i>
<i>Obrázek 6: Přihlášení se nezdařilo.....</i>	<i>27</i>
<i>Tabulka 4: Teoretická přenosová rychlost RB-433AH</i>	<i>32</i>
<i>Tabulka 5: Přehled parametrů RB-433AH</i>	<i>32</i>
<i>Obrázek 7: Rozložení komponent RB-433AH</i>	<i>33</i>
<i>Tabulka 6: Specifikace bezdrátové karty CM-11 HP.....</i>	<i>35</i>
<i>Obrázek 8: CM-11HP + pigtail MMCX-M, RSMA-M.....</i>	<i>35</i>
<i>Obrázek 9: Schema zapojení – laboratorní prostředí.....</i>	<i>36</i>
<i>Obrázek 10: Schema zapojení konektoru RJ45 – přímý kabel</i>	<i>38</i>
<i>Tabulka 7: Konfigurace portu RS232C.....</i>	<i>38</i>
<i>Obrázek 11: Prozkoumávání radiového okolí.....</i>	<i>39</i>
<i>Obrázek 12: Vytížení jednotlivých radiových kanálů.....</i>	<i>40</i>
<i>Tabulka 9: Měření parametrů bezdrátové karty přístrojem PSV monitor DM2G4</i>	<i>41</i>
<i>Obrázek 13: QoS.....</i>	<i>50</i>
<i>Obrázek 14: Konfigurace portů CCP</i>	<i>51</i>
<i>Obrázek 15: Konfigurace vzdáleného přístupu.....</i>	<i>53</i>
<i>Obrázek 16: Struktura Active Directory</i>	<i>54</i>
<i>Obrázek 17: Vytvoření emailové schránky uživateli“ helpdesk“</i>	<i>55</i>
<i>Obrázek 18: Přehled webových stránek které spravuje IIS.....</i>	<i>55</i>
<i>Obrázek 19: Politika koncových uživatelů.....</i>	<i>56</i>
<i>Obrázek 20: Politika Radius Klientů</i>	<i>57</i>
<i>Obrázek 21: Úspěšná autentizace s IAS.....</i>	<i>58</i>
<i>Obrázek 22: Neúspěšná autentizace s IAS.....</i>	<i>58</i>
<i>Obrázek 23: Monitorovaná typologie sítě</i>	<i>60</i>
<i>Obrázek 24: Sledované služby</i>	<i>61</i>
<i>Obrázek 25: Emailová notifikace.....</i>	<i>61</i>
<i>Obrázek 26: Syslog</i>	<i>62</i>
<i>Obrázek 27: Automatizované spuštění pooleru.....</i>	<i>64</i>
<i>Obrázek 28: Konfigurace komponent – Cacti.....</i>	<i>65</i>
<i>Obrázek 29: Výběr zdroje dat - Cacti</i>	<i>66</i>
<i>Obrázek 30: Objektový identifikátor (OID) uživatele Ondra - Cacti.....</i>	<i>67</i>
<i>Obrázek 31: Grafický výstup - Cacti.....</i>	<i>68</i>

<i>Obrázek 32: Prohledání radiového okolí</i>	69
<i>Obrázek 33: Přiřazení IP adresy koncovému uživateli</i>	70
<i>Obrázek 34: Vstupní portál hotspotu</i>	70
<i>Obrázek 35: Informace o uživatelské relaci</i>	71
<i>Obrázek 36: Úspěšná autentizace podle MAC</i>	71
<i>Obrázek 37: Neúspěšná autentizace podle MAC</i>	72
<i>Obrázek 38: Informační portál</i>	72
<i>Obrázek 39: Měřící bod 1</i>	73
<i>Obrázek 40: Přenosové rychlosti a vytížení CPU – Měřící bod 1</i>	74
<i>Obrázek 41: Měřící bod 2</i>	75
<i>Obrázek 42: Přenosové rychlosti a vytížení CPU – Měřící bod 2</i>	75
<i>Obrázek 43: Test funkčnosti QoS</i>	76

1. ÚVOD

Hotspot lze popsat jako místo či oblast s možností bezdrátového připojení k síťovým prostředkům nebo internetu. V dnešní době je systém hojně využíván v sektoru privátním i veřejném. Běžně se s hotspoty můžeme setkat na letištích, benzinových pumpách, kavárnách či hotelích. Zprostředkovává přístup koncovým uživatelům do sítě a jeho služby mohou být poskytovány zdarma či zpoplatněny. Princip činnosti hotspotu je založen na standardu technologie WLAN (Wireless Local Area Network) a musí být v souladu s předpisy Českého telekomunikačního úřadu (ČTÚ).

Cílem práce je vyřešit a experimentálně ověřit následující problematiku:

- plánování hotspotové sítě,
- volba vhodného standardu IEEE 802.11 a kmitočtového pásma,
- legislativa hotspotové sítě,
- návrh koncepce hotspotového systému,
- hardwarové a softwarové vybavení prvků sítě,
- realizace experimentálního pracoviště,
- testování experimentálního pracoviště.

2. PLÁNOVÁNÍ HOTSPOTOVÉ SÍTĚ

Zřízení a následné provozování hotspotové sítě přináší řadu úskalí a rozhodnutí, které je nutno provést s rozvahou. Nevhodná volba některého z dále popisovaných parametrů může zapříčinit nadbytečné finanční náklady, malou přenosovou rychlost, případně celkový nezájem o služby. Je nutné se především zaměřit na následující parametry: volba lokality, velikost hotspotových buněk, umístění hotspotu, volba kmitočtového pásma, volba technologie a parametry ovlivňující kvalitu radiového spoje.

2.1 Volba lokality

Volba lokality hraje důležitou roli v případě, že se chystáme služby hotspotu zpoplatnit. Pokud chceme provozovat hotspotové služby pouze jako bezplatný doplněk či reklamu k některé z našich činností, nejspíš bude lokalitou naše provozovna. Chceme-li však provozovat hotspotový systém za účelem zisku, bude prvním krokem právě volba vhodné lokality. Jde o průzkum blízkého i vzdáleného okolí, **snahou je najít co největší počet potenciálních zákazníků na nejmenší ploše**. Dobrý předpoklad mají středně velká města, kde se ještě nenachází ve velké míře konkurence. Není to ale pravidlem. Paradoxně mohou být zajímavou lokalitou také obce, případně jiné obytné zóny. V těchto lokalitách nemusí být ještě žádná kvalitní infrastruktura a hotspotový systém by mohl být jedinou možností širokopásmového internetu, případně jiných služeb.

2.2 Velikost hotspotových buněk

Velikost hotspotových buněk velmi úzce souvisí s výběrem lokality. Snahou je pokrýt signálem co největší počet potenciálních zákazníků. Pokud budou zákazníci koncentrováni blízko sebe, bude stačit rozměrově menší buňka. Na druhou stranu, pokud se zákazníci budou nacházet v různých vzdálenostech od hotspotu, bude potřeba buňky větší. Velikost buňky nelze zvyšovat do nekonečna. Limitem je zisk antény a vysílací výkon hotspotu. Oba tyto parametry podléhají regulačnímu zákonu ČTÚ. Předpoklad je takový, že k hotspotovému systému se budou připojovat většinou mobilní uživatelé bez externí anténní soustavy. S ohledem na to lze stanovit dva typy buněk včetně jejich parametrů:

- **mikro buňka** – signál je distribuován v rámci jednoho objektu, dosah desítky metrů, provozováno se základní dipólovou anténou,
- **makro buňka** – signál je distribuován do vzdálenosti cca. stovek metrů, nutno použít externí anténu s vyšším ziskem.

2.3 Umístění hotspotu

Pravidla pro umístění hotspotu jsou pro mikrobuňky i makrobuňky podobná. Snahou je umístit hotspot uprostřed lokality, v jejímž okolí je nejvyšší koncentrace koncových uživatelů. Ideální příklad je konstantní vzdálenost všech koncových uživatelů od hotspotu a zajištění přímé viditelnosti mezi těmito body.

2.4 Volba kmitočtového pásma

Volba kmitočtového pásma patří mezi nejzávažnější rozhodnutí, které ovlivňuje finanční rozpočet celého projektu. Cílem této kapitoly je volba vhodného pásma, které se hodí pro provozování hotspotové sítě a je finančně nejméně nákladné. Nabízejí se nám následující pásma, každé má své specifické vlastnosti:

- 2,4 GHz.
- 3,5 GHz.
- 5 GHz
- 10 GHz

Jednotlivé vlastnosti, rozebrané níže, se pokusím obodovat ze subjektivního hlediska. Výhodné vlastnosti budou označeny (+) a za toto znaménko se následně dosadí hodnota (+1). Nevýhodné vlastnosti se označí znaménkem (-), znaménko koresponduje s hodnotou (-1). Po sečtení všech dílčích hodnot získáme orientační výsledek, který nám pomůže s výběrem vhodného pásma. Čím je výsledek vyšší, tím je pásmo pro naše potřeby vhodnější. Parametr licence pásma má dvojnásobnou váhu z důvodu velkých finančních nákladů a jiných problematik, spojených se získáním licence.

2,4 GHz: - bezlicencované pásmo(+,+), nízké pořizovací náklady (+), vysoká podpora koncových uživatelů (+), vysoké rušení okolními sítěmi (-);

3,5 GHz: - licencované pásmo (-,-), střední pořizovací náklady (0), minimální podpora koncových uživatelů (-), minimální rušení okolními sítěmi (+);

5 GHz: - bezlicencované pásmo (+,+), nízké pořizovací náklady (+), střední podpora koncových uživatelů (0), střední rušení okolními sítěmi (0);

10 GHz: - bezlicencované pásmo (+,+), vysoké pořizovací náklady (-), minimální podpora koncových uživatelů (-), minimální rušení okolními sítěmi (+);

$2,4\text{GHz} = (1+1)+1+1-1 = 3$
$3,5\text{GHz} = (-1-1)+0-1+1 = -2$
$5\text{GHz} = (1+1)+1+0+0 = 3$
$10\text{GHz} = (1+1)-1-1+1 = 1$

Tabulka 1: Kriterium pro volbu kmitočtového pásma

Z uvedených výsledků vychází nejlépe pásmo 2,4GHz a 5 GHz. Obě pásma jsou ohodnocena stejně. Výhodnější však bude nasazení pásma 2,4 GHz a to právě z důvodu zmiňované převažující podpory klientských stanic na daném kmitočtu a faktem, že nižší kmitočty lépe překonávají překážky v radiové trase mezi vysílačem a přijímačem. **Z popsaných důvodů jsem se tedy rozhodnul využít kmitočtové pásmo 2,4 GHz.**

Charakteristika kmitočtové pásmo 2,4GHz

Ve veřejně přístupném bezlicenčním pásmu jsou uživatelé nuceni dodržovat předepsaná ustanovení vydané ČTÚ, který je oprávněn penalizovat uživatele za případná porušení. Toto pásmo je kromě technologie WLAN, kterou hodláme využít při nasazení hotspotu, využíváno rovněž Bluetooth zařízeními, bezšňůrovými telefony, mikrovlnnými troubami atd..

Podmínky využití pásma 2,4 GHz

Podmínky ČTÚ, vztahující se na využití radiových kmitočtů a provozování vysílacích radiových zařízení pro širokopásmový přenos dat na principu rozprostřeného spektra nebo OFDM v pásmu 2,4 GHz [2]:

- stanice lze provozovat bez individuálního oprávnění radiových kmitočtů,
- maximální vyzářený výkon 100 mW e.i.r.p. (20 dBm),
- u stanic, užívající techniku přímé sekvence nebo modulaci OFDM, nesmí spektrální hustota e.i.r.p. překročit hodnotu -20 dBW/1 MHz,
- u stanic, užívající techniku přeskočků kmitočtu, nesmí spektrální hustota e.i.r.p. překročit hodnotu -10 dBW/100 kHz,
- stanice musí dodržet maximální vyzářený výkon e.i.r.p. a maximální střední spektrální hustotu při libovolné kombinaci výstupního vysílače a použité antény,
- stanice nesmějí být provozovány s přídatnými zesilovači vysokofrekvenčního výkonu a s převaděči,
- stanice jsou provozovány na sdílených kmitočtech,
- Stanice nesmí být elektricky a mechanicky měněna,
- provoz stanice nemá zajištěnou ochranu proti rušení způsobenému vysílacími radiovými stanicemi jiné radiokomunikační služby provozovanými na základě individuálního oprávnění k využívání radiových kmitočtů nebo jinými stanicemi pro širokopásmový přenos dat na principu rozprostřeného spektra

nebo OFDM. Případné rušení řeší fyzické a právnické osoby vzájemnou dohodou. Nedohodnou-li se, postupuje se podle zákona.

2.5 Standardy IEEE 802.11 v pásmu 2,4 GHz

Institut inženýrů elektrotechniky a elektroniky (IEEE) vyvíjí a schvaluje normy pro širokou řadu počítačových technologií, na jejichž základu mohou být založeny výrobky. Tím je zaručena kompatibilita a jsme schopni kombinovat zařízení i od různých výrobců. IEEE označuje síťové normy číslem 802. Normy pro bezdrátové sítě tvoří podskupinu norem 802 a jsou označeny číslem 11. Z tohoto důvodu jsou normy pro bezdrátové sítě označeny číslem 802.11. Technologie Wi-Fi (Wireless Fidelity) vychází ze specifikace 802.11 a je standardem sítí WLAN. Jejím původním cílem bylo zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální síť LAN (Local Area Network). S postupem času začala být využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit a tzv. hotspotů. Pro provozování hotspotové sítě lze využít tzv. infrastrukturní síť, jejichž podstata je popsána níže [4].

Infrastrukturní síť

Obsahují jeden nebo více přístupových bodů (AP – Access Point), které všesměrově vysílají svá SSID (Service Set Identifier) v intervalu každých 100ms. SSID signál je vyslán rychlostí 1 Mb/s, je krátkého trvání a nemá zásadní vliv na výkon. Jde o řetězec až 32 ASCII znaků, kterými se jednotlivé sítě rozlišují. Vzhledem k tomu, že rychlost 1 Mb/s je nejnižší přenosová rychlost Wi-Fi, je zajištěno, že každý koncový uživatel, který je schopen detekovat síť, může komunikovat minimálně rychlostí 1 Mb/s.

Kmitočtové pásmo 2,4GHz lze vzhledem k používání standardů Wi-Fi rozčlenit do kanálů, jejich počet je pro různé oblasti jiný.

Územní oblast	počet kanálů	Doporučení
Evropa	13	-----
Severní Amerika	11	Využití pouze kanálů 1, 6 a 11 z důvodů minimalizace interferencí.
Japonsko	14	-----

Tabulka 2: Maximální počet kanálů pro Wi-Fi zařízení

Standardy pro pásmo 2,4GHz vychází z normy 802.11 a přináší pouze drobné rozšíření nebo modifikace. Tyto modifikace se většinou týkají zabezpečení, přenosové rychlosti, případně používané modulace. Výčet několika standardů a jejich rozdíl od původní normy 802.11 je zobrazen níže:

- 802.11** – původní standard, přenosová rychlost 1 Mb/s a 2 Mb/s,
- 802.11b** – vylepšený 802.11 s podporou 5,5 Mb/s a 11 Mb/s,
- 802.11c** – bezdrátové přemostění (bridge),
- 802.11d** – mezinárodní roamingový dodatek, implementuje též 802.11c,
- 802.11g** – přenosová rychlost 54Mb/s, zpětně kompatibilní s 802.11b,
- 802.11i** – vylepšený autentizační a šifrovací algoritmus (WPA2),
- 802.11n** – zvýšena datová propustnost až na 600 Mb/s (technologie MIMO),
- 802.11p** – bezdrátový přístup pro pohyblivé prostředí (auto, vlaky, sanitky),
- 802.11r** – rychlé přesuny mezi přístupovými body,
- 802.11u** – spolupráce se sítěmi mimo 802 standardy (například s mobilními sítěmi),
- 802.11v** – správa bezdrátových sítí.

Standard	Reálná propustnost [Mb/s]	Teoretická propustnost [Mb/s]	Dosah - interiér [m]	Dosah - exteriér [m]	Fyzická vrstva
802.11	0,7	2	25m	75m	DSSS
802.11b	4	11	35m	110m	DSSS
802.11g	19	54	35m	115m	OFDM
802.11n	74	600	70m	160m	OFDM,MIMO

Tabulka 3: Vlastnosti některých standardů

Mezi nejvíce rozšířené standardy pro pásmo 2,4 GHz patří 802.11b a 802.11g. Jsou tudíž nejvhodnějšími kandidáty pro nasazení v hotspotových aplikacích.

2.5.1 Spektrum Wi-Fi signálu

Jednou z podmínek provozování WiFi zařízení je dle ČTÚ podpora technologie **rozprostírání spektra**. Tím lze zajistit distribuci signálu při použití menších vysílacích výkonů a částečné odrušení jednotlivých uživatelů.

Rozprostřené spektrum

Rozprostírá bezdrátové signály přes více frekvencí daného pásma namísto vysílání na frekvenci jedné. Rozprostřené spektrum používá větší šířku pásma než úzkopásmová komunikace, nabízí však větší spolehlivost, zabezpečení a integritu dat.

DSSS

Rozprostírá přenosy přes několik kanálů v určitém frekvenčním rozsahu za pomoci tzv. čipového kódu. Několik čipových bitů reprezentuje jeden bit informace (vznik redundance). Tyto bity se přenášejí ve stejném časovém intervalu, jaký by byl třeba k předání jednoho bitu. Takto upravený signál je rozprostřen do větší části radiového spektra, je méně citlivý vůči rušení. Příjemací strana musí čipový kód předem znát a za pomoci filtračního kodéru pro úpravu rozprostřeného spektra tento čipový kód opět odstraní a získá data ve formátu, ve

kterým byla původně poslána. Ostatním uživatelům, kteří neznají čipový kód, se jeví signál jako náhodný šum.

OFDM

Efektivně využívá dostupné spektrum tak, že jej rozděluje na podkanály a vysílá určitou část datového přenosu přes každý podkanál. Jednotlivé podkanály pracují ortogonálně (paralelně) a zaměřují se na malý objem přenášené informace.

2.5.2 Zabezpečení Wi-Fi

Zabezpečení bezdrátových sítí je obzvláště důležité. Na rozdíl od sítí metalických, nebo optických, se elektromagnetické radiové vlny nekontrolovatelně šíří i za hranice zabezpečeného prostoru. Síť se tak může stát terčem mnoha útočníků, kteří jsou schopni získat citlivé soukromé, či firemní informace, případně jinak zaškodit. Jako obranu lze použít některý z těchto mechanismů:

- potlačení všesměrového vysílání SSID,
- kontrola MAC adres,
- WEP (Wired Equivalent Privacy),
- WPA (Wi-Fi Protecte Access),
- WPA2.

Potlačení všesměrového vysílání SSID

Patří mezi nejjednodušší princip zabezpečení. Zablokováním SSID dosáhneme skrytí sítě. Koncovému uživateli zůstane síť při prohledávání radiového okolí skryta.

Kontrola MAC adres

Přístup k bezdrátové síti se uděluje pouze klientům, jejichž MAC adresa se nachází v tabulce, povolující přístup. Tabulka se nachází v bezdrátovém přístupovém bodě.

WEP

Šifrování komunikace pomocí statické symetrické šifry, která musí být nastavena na obou uzlech sítě ručně.

WPA

Šifrování pomocí WEP klíčů, které jsou dynamicky měněny. Mechanismus je zpětně kompatibilní s WEP. Autentizace přístupu do WPA sítě je prováděna pomocí PSK nebo Radius serveru.

2.6 Parametry ovlivňující kvalitu rádiového spoje

Aby bylo spojení pomocí standardu 802.11 dostatečně kvalitní, je nutné jej pečlivě naplánovat. Kvalitu rádiového spojení významně určují následující kritéria:

- **efektivní vysílací výkon** – součet vysílacího výkonu zařízení a zisku antény, od kterého se odečte ztráta na kabelu a konektorech,
- **ztráta při přenosu** – ztráty na signálu ve volném prostoru a ztráty vlivem první Fresnelovy zóny,
- **efektivní citlivost přijímače** – součet zisku antény a citlivosti přijímače s odečtem ztrát na kebelech a konektorech.

Úroveň signálu na přijímači:

$$P_r = P_t - L_p + G_t + G_r - L_t - L_r \quad [dBm]$$

P_r [dBm] – úroveň signálu na přijímači

P_t [dBm] – vysílací výkon vysílače

L_p [dB] – ztráty signálu při přenosu

G_t [dBi] – zisk antény vysílače

G_r [dBi] – zisk antény přijímače

L_t [dB] – útlum mezi vysílačem a anténou vysílače

L_r [dB] – útlum mezi přijímačem a anténou přijímače

Jedinou neznámou ve vzorci je ztráta signálu ve volném prostoru. Zbytek parametrů jsme schopni získat od výrobce. Výsledek vzorce udává očekávanou úroveň signálu na přijímači. Je rozhodující z pohledu navázání bezdrátového spoje a jeho přenosové rychlosti.

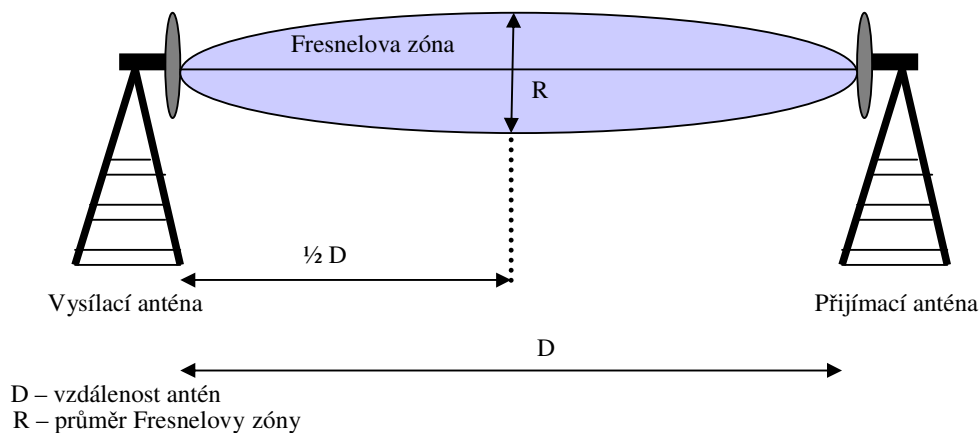
Ztráty signálu při přenosu

- **Refrakce (lom)** o zemskou atmosféru. WiFi technologie je vůči těmto ztrátám imunní, protože nízký vysílací výkon a poměrně vysoký kmitočet neumožňuje distribuci signálu do vzdálenosti zemské atmosféry.
- **Difrakce (ohyb)** o předměty v blízkosti trasy signálu. Oblast blízko šíření signálu nazýváme první Fresnelovou zónou.
- **Reflexe (odraz)** o zem. Tento jev se uplatňuje na trasách vzdálených více jak 4km, které jsou vedeny nad rovným terénem nebo nad vodní hladinou.

Z výše uvedených ztrát, které vznikají při přenosu signálu, naši aplikaci ovlivní pouze difrakce o předměty, zasahující do Fresnelovy zóny.

Fresnelova zóna

Prostor kolem spojnice přímky mezi vysílací a přijímací anténou. Zóna má doutníkovitý tvar (elipsoid) s nejširším průměrem uprostřed vzdálenosti mezi anténami. Narušení Fresnelovy zóny má za následek vznik nežádoucích odrazů, které mají nepříznivý vliv na kvalitu přenosu (snížení přenosové rychlosti, ztráta paketů atd). Při snaze navrhnout kvalitní spoj se snažíme dodržet alespoň 60% volného uvedeného průměru zóny.



Obrázek 1: Fresnelova zóna

Ztráty ve volném prostoru:

Ztráty způsobeny průchodem signálu atmosférou, dochází k nim vždy. Nejsou ovlivněny refrakcí, difrakcí ani reflexí.

$$L_p = 92,45 + 20 \cdot (\log_{10} F) + (\log_{10} d) \quad [dB]$$

F [GHz] - frekvence

d [km] - vzdálenost

Teoretická znalost parametrů ovlivňující kvalitu radiového spoje je velice důležitá, ale v naší aplikaci provozování hotspotu moc uplatnění nemá. Naší snahou je umožnit připojení mobilním bezdrátovým klientům v dosahu hotspotu, což nám znemožňuje radiovou trasu naplánovat. Nikdy předem nevíme, odkud se bezdrátový klient bude připojovat a nejsme tudíž schopni zaručit přímou viditelnost na hotspot, nebo dokonce prázdnou první Fresnelovu zónu. Nevíme také nic o citlivosti přijímacího zařízení, či zisku přijímací antény.

3. LEGISLATIVA PROVOZOVÁNÍ HOTSPOTOVÉ SÍTĚ

Legislativa provozování hotspotové sítě se liší pro různé zájmy provozovatele hotspotu, které mohou být následující.

- **Provozování hotspotu jako doplněk k některým nabízeným službám, bez nároků na zisk.**
- **Provozování hotspotu za účelem zisku.**

3.1 Provozování hotspotu bez nároku na zisk

V tomto případě je situace poměrně jednoduchá. Vycházíme z kapitoly 2, která se věnuje plánování hotspotové sítě. Zaměřuji se na bezlicencované kmitočtové pásmo 2,4 GHz. Za těchto okolností nám v provozování sítě prakticky nic nebrání. Není nutno činnost nikam ohlašovat, pouze musíme dodržet limity stanovené ČTÚ v kapitole 2.4.

3.2 Provozování hotspotu za účelem zisku

Nyní je situace již komplikovanější. Při provozování hotspotového systému za účelem zisku, je nutno postupovat podle zákona č. 127/2005 Sb. o elektronických komunikacích. Opět se zaměříme na bezlicencované pásmo 2,4 GHz. V opačném případě bychom se neobešli bez telekomunikační licence, která by znamenala poměrně vysoké finanční náklady. Heslovitě lze postup vedoucí k získání oprávnění provozování hotspotového systému za účelem zisku vyjádřit následovně:

- oznámení komunikační činnosti,
- splnění všeobecných podmínek,
- zaplacení správního poplatku.

Stejně jako v předchozím případě jsme při provozování sítě nuceni dodržovat stanovené limity ČTÚ pro dané kmitočtové pásmo (viz kapitola 2.4).

Zákon č. 127/2005 Sb. o elektronických komunikacích[3]

Zákon č. 127/2005 Sb. o elektronických komunikacích stanovuje fyzickým a právnickým osobám, hodlajícím vykonávat komunikační činnost, povinnost oznámit předem písemně tuto skutečnost ČTÚ. Při oznamování výkonu komunikačních činností, které jsou **podnikáním v elektronických komunikacích**, je třeba postupovat podle dále uvedených informací a pokynů.

Podnikáním se rozumí soustavná činnost prováděná samostatně podnikatelem vlastním jménem a na vlastní odpovědnost za účelem dosažení zisku. Předmětem podnikání v elektronických komunikacích je:

- **zajišťování veřejných komunikačních sítí,**
- **poskytování služeb elektronických komunikací.**

veřejnou komunikační síť se rozumí síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací.

Síť elektronických komunikací se rozumí přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, které umožňují přenos signálů po vedení, rádii, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.

Zajišťování sítě elektronických komunikací se rozumí zřízení této sítě, její provozování a dohled nad ní nebo její zpřístupnění.

Službou elektronických komunikací se rozumí služba obvykle poskytovaná za úplat, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací. Nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.

Veřejně dostupnou službou elektronických komunikací se rozumí služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.

1. Oznámení komunikační činnosti

Fyzická a právnická osoba oznamuje výkon komunikační činnosti, která je předmětem podnikání v elektronických komunikacích ČTÚ písemně, doručením řádně a úplně vyplněného formuláře „[Oznámení komunikační činnosti](#)“ včetně příloh podle § 13 a splněním obecných podmínek podle § 8 zákona č. 127/2005 Sb. (dále jen „Oznámení komunikační činnosti“).

Vyplněný formulář „[Oznámení komunikační činnosti](#)“ zašle fyzická a právnická osoba na adresu ČTÚ, odboru pro oblast, který je místně příslušný podle místa pobytu fyzické nebo sídla právnické osoby .

2. Osvědčení o oznámení komunikační činnosti

ČTÚ vydá do jednoho týdne osobě, která oznámila výkon komunikační činnosti potvrzení evidence žádosti. Oprávnění k podnikání oznamující osobě vzniká dnem doručení úplného oznámení výkonu komunikační činnosti, která je podnikáním v elektronických komunikacích.

3. Správní poplatky

Za vydání osvědčení o oznámení komunikační činnosti (podle § 13 odst. 5 zákona č. 127/2005 Sb.) je vybírán správní poplatek ve výši 1 000,- Kč. Správní poplatek je vybírán podle zákona č. 634/2004 Sb. o správních poplatcích.

4. NÁVRH KONCEPCE HOTSPOTOVÉHO SYSTÉMU

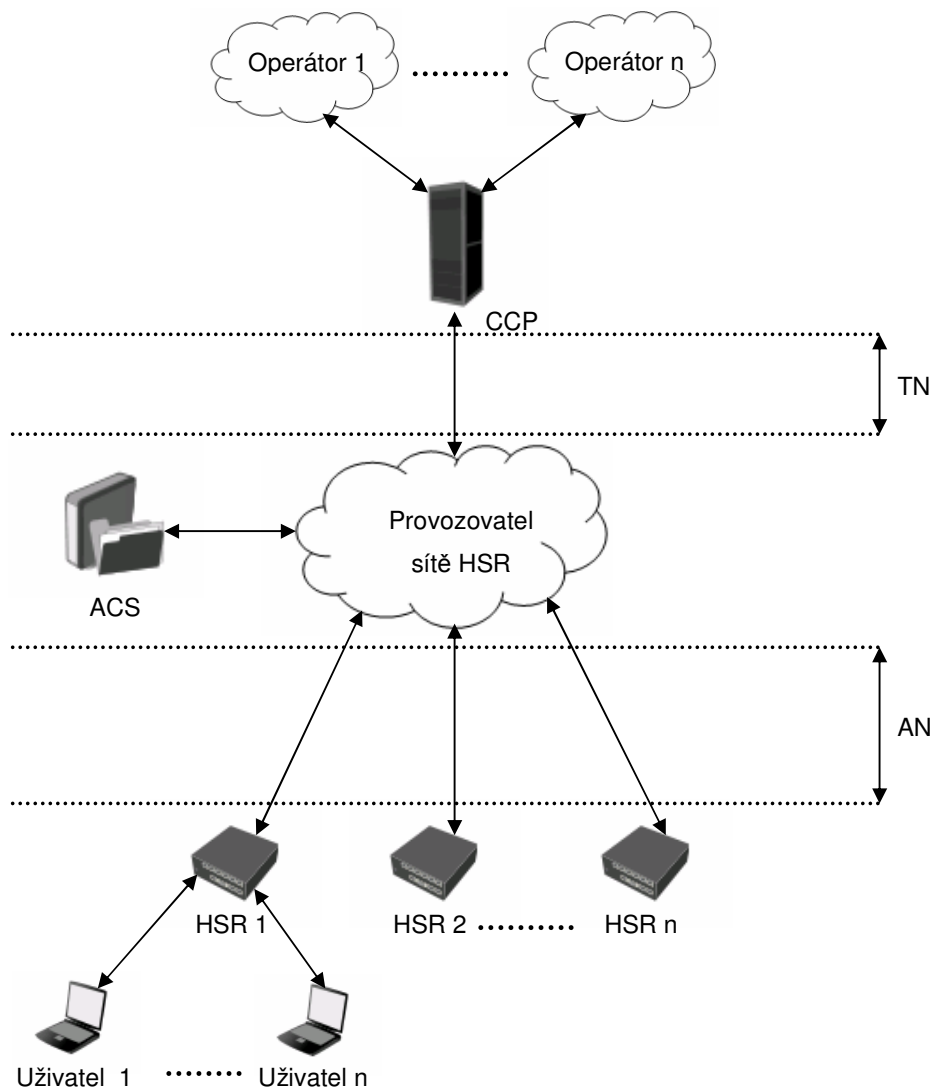
Hotspotový systém je navržen s ohledem na požadavky využití pouze jednoho fyzického síťového rozhraní, které umožní internetovým poskytovatelům (operátorům) prezentovat své služby pod vlastním názvem bezdrátové sítě. Tento požadavek lze realizovat funkcí VAP (Virtual Access Point). Oddělení koncových uživatelů jednotlivých operátorů je zajištěno prostřednictvím technologie VLAN (Virtual Local Area Network). Vhodné je též izolování uživatelů v rámci jednoho operátora, které se provádí vhodnou konfigurací bezdrátové karty příslušného hotspotu.

Hotspoty mohou být vystavěny na lukrativních místech nebo ve vzdálenostech, kde by se jejich signálová distribuce částečně překrývala. Tímto způsobem jsme schopni signálem pokrýt i rozlehlejší oblasti (například část měst atd). Dohled nad jednotlivými hotspoty je centralizován do jednoho bodu (přístupový řídicí server - ACS). Tento bod, jako jediný, má možnost měnit konfiguraci hotspotů, sledovat jejich kapacitní či výkonové vytížení, případně jiné důležité parametry.

4.1 Fyzická topologie systému

Fyzická topologie systému je prezentována v obrázku 2 a představuje umístění a vzájemné propojení hardwaru, které nám zaručí funkce nezbytné pro provozování hotspotového systému. Topologie dle obrázku 2 je tvořená následujícími prvky:

- koncoví uživatelé,
- hotspotové routery (HSR – Hotspot Router),
- síť provozovatele HSR,
- přístupový řídicí server (ACS – Access Control Server),
- centrální propojovací bod (CCP – Central Connection Point),
- síť operátorů,
- transportní síť (TN – Transport Network),
- přístupová síť (AN – Access Network),



Obrázek 2: Fyzická topologie systému

Operator 1-n

Sítě společností, které umožňují oprávněným klientům přístup k síťovým prostředkům nebo k internetu.

CCP (Central Connection Point)

Připojovací bod, připojuje provozovatele sítě HSR přes transportní síť k jednotlivým operátorům. Propojuje též jednotlivé operátory mezi sebou.

TN (Transport Network)

Fyzické propojení provozovatele sítě HSR a CCP. Jedná se o páteřní spoj, jsou kladeny vysoké nároky na přenosovou rychlost a kvalitu. Spoj musí být schopen obsloužit požadavky všech HSR nebo-li požadavky všech koncových uživatelů.

Provozovatel sítě HSR

Struktura sítě, která přeposílá signalizační a systémové pakety od HSR do ACS a uživatelské pakety směrem do CCP.

ACS (Access Control Server)

Jediný prvek v síti s možností konfigurace a monitorování struktury HSR. Spravuje globální uživatelskou databázi, účtuje přenesená data koncovým uživatelům a vytváří přehledné grafy.

AN (Access Network)

Fyzické propojení jednotlivých HSR se sítí provozovatele HSR. AN narozdíl od TN nepotřebuje extrémní přenosovou rychlost, zpracovává data pouze jednoho HSR. AN může být realizována libovolnou technologií podporující standard ethernet s tagovým provozem.

HSR 1-n

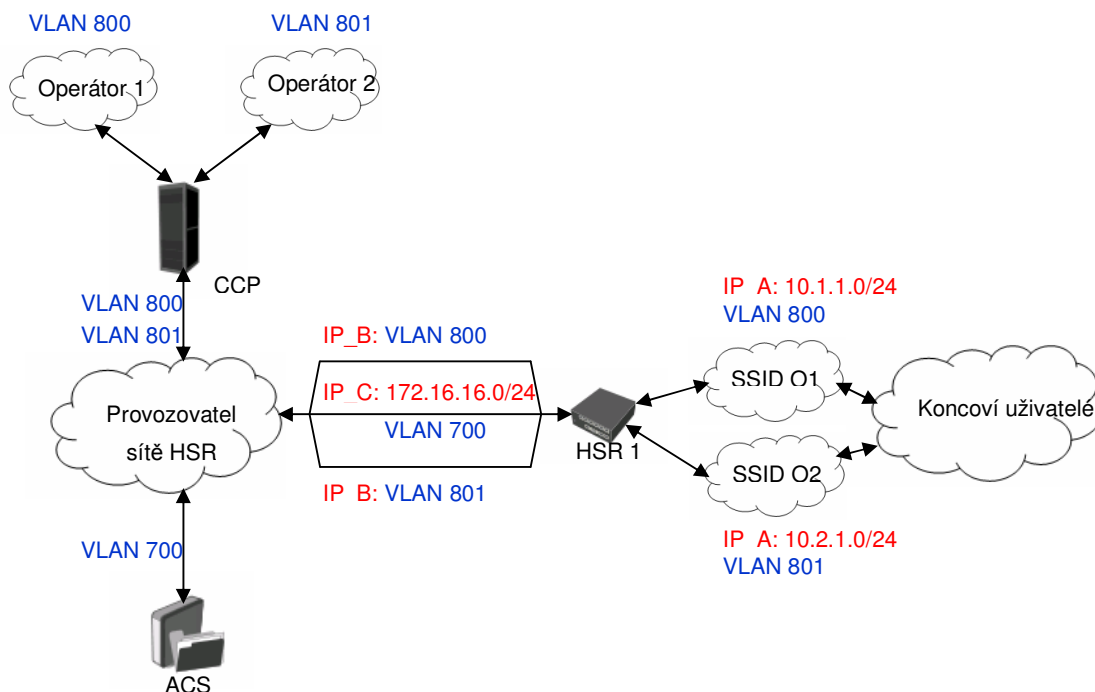
Síťové prvky kombinující funkci routeru, přístupového bodu, firewallu a manageru šířky pásma. Zprostředkovávají oprávněným uživatelům přístup k síti některého z operátorů, chrání koncové uživatele před útočníky z internetu a přidělují koncovým uživatelům objednanou přenosovou rychlost.

Uživatel 1-n

Koncoví uživatelé, kteří na základě ověření oprávnění přístupu do sítě užívají některé ze služeb daného operátora.

4.2 Logická topologie a adresace systému

Pro zjednodušení a názornost je logické propojení systému a jeho adresace demonstrována pouze na jednom prvku HSR s podporou dvou operátorů. Logická topologie určuje, které uzly sítě mohou mezi sebou komunikovat. Vzhledem k použité technologii VLAN je komunikace omezena pouze na uzly mající stejný VLAN identifikátor.



Obrázek 3: Logická topologie systému + adresace

Z předchozího textu a obrázku 3 je tedy patrné, že koncoví uživatelé, připojení k SSID O1, mohou užívat pouze služeb operátora 1 (VLAN800) a uživatelé připojení k SSID O2 pouze služeb operátora 2 (VLAN 801). Stejným způsobem je izolován provoz mezi ACS a HSR1 (VLAN 700), který se používá pro řídicí a signalizační informace.

Systém HSR používá několik adresních rozsahů viz obrázek 3.

IP_A – formát: 10.x.y.0 /24 - privátní adresní rozsah provozovatele HSR. Adresa třídy A, umožňuje nám adresovat velké množství koncových uživatelů.

x = pořadové číslo operátora

y = počet využitých HSR daným operátorem

IP_B – libovolný rozsah adres přidělený příslušným operátorem. Adresa z tohoto rozsahu slouží ke skrytí identity koncového uživatele ze strany internetu a také k překladu síťových adres (NAT).

IP_C – formát: 172.16.16.0 /24 – adresní rozsah provozovatele, slouží k administraci jednotlivý HSR prostřednictvím VLAN ID 700. Jedná se o adresu třídy B, umožňuje nám adresovat dostatečné množství prvků HSR.

4.3 Přístup uživatele do systému (první fáze)

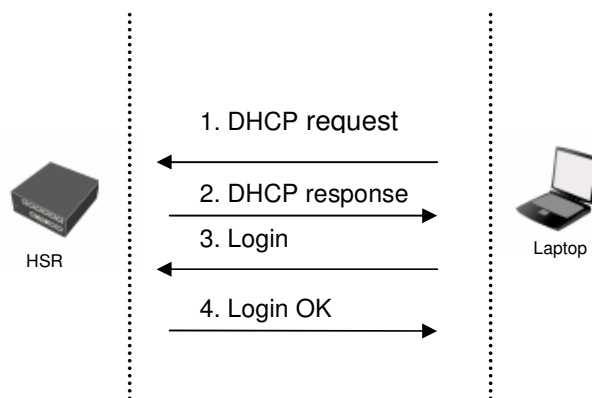
Koncový uživatel, který se nachází v oblasti signálového pokrytí hotspotu, prohledává radiové okolí a sestavuje si tabulku bezdrátových sítí k dispozici. Detekuje SSID jednotlivých operátorů a na základě předplacení služeb, nebo jiného oprávnění, se k jedné ze sítí připojuje. Obdrží IP adresu z rozsahu DHCP serveru a při snaze zobrazit libovolnou internetovou stránku dojde k přesměrování veškerých dotazů na vstupní hotspotový portál. Uživatel je vyzván k autentizačnímu procesu (ověření uživatelského jména a hesla). Při ověřování platnosti uživatelského účtu jsou prohledávány dvě databáze.

- lokální databáze (databáze hotspotu),
- globální databáze (databáze ACS).

Nejprve se zkoumá prezence uživatelského účtu v lokální databázi. V případě neúspěchu se za pomoci služby Radius prohledává globální databáze. Pokud se uživatelský účet nenachází v žádné z těchto databází, hotspotový portál generuje koncovému uživateli zprávu o neúspěšném přihlášení a vyzývá jej k opětovnému autentizačnímu procesu. V opačném případě je aktivována druhá fáze zabezpečení. Její náležitosti budou popsány v kapitole 4.4.

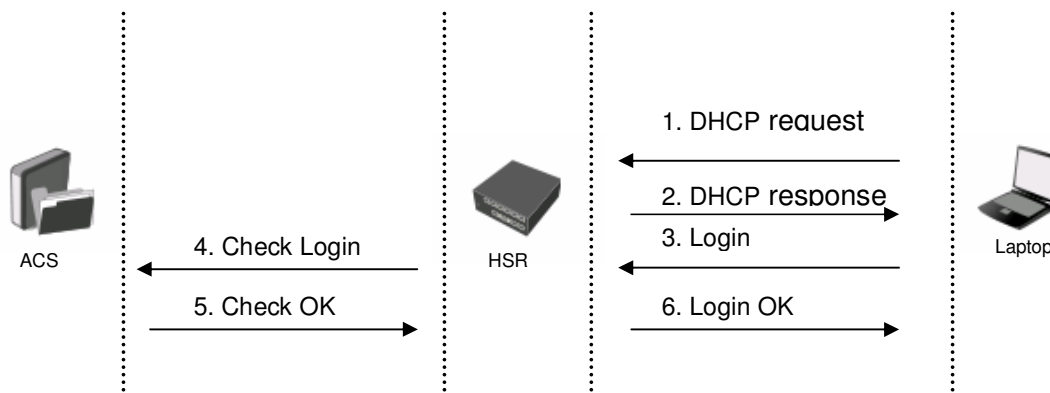
Proces připojení koncového uživatele k HSR a autentizace jeho uživatelského účtu lze vyjádřit též graficky (viz obrázky 4,5 a 6).

1. Uživatelský účet byl nalezen v lokální databázi příslušného hotspotu.



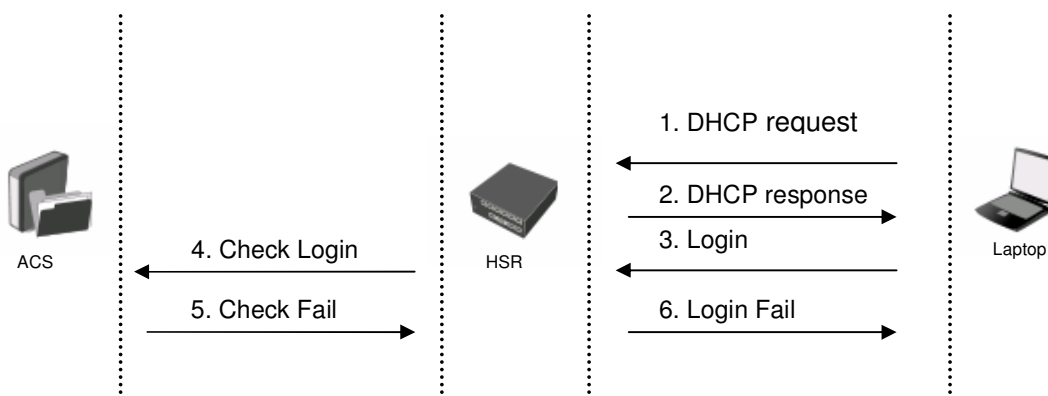
Obrázek 4: Místní přihlášení

2. Uživatelský účet byl nalezen v globální databázi.



Obrázek 5: Vzdálené přihlášení

3. Uživatelský účet nebyl nalezen v lokální, ani v globální databázi. Přihlášení do systému se nezdařilo.



Obrázek 6: Přihlášení se nezdařilo

DHCP request

Koncový uživatel se připojil k bezdrátovému rozhraní HSR a požaduje přidělení IP adresy.

DHCP response

DHCP server HSR přiděluje koncovému uživateli IP adresu ze statického seznamu nebo dynamického rozsahu.

Login

Přesměrování veškeré komunikace na vstupní portál. Uživatel je vyzván k autentizačnímu procesu (zadání uživatelského jména a hesla).

Login OK

Autentizace uživatele se zdařila, je aktivována druhá fáze zabezpečení (viz. kapitola 4.4)

Check Login

Proces autentizace nebyl v lokální databázi úspěšný, požadavek je přeposlán prostřednictvím služby Radius do globální databáze.

Check Fail

Proces autentizace nebyl úspěšný v lokální ani globální databázi uživatelů. ACS zasílá HSR zprávu o zamítnutí přístupu.

Login Fail

Uživatelský portál generuje koncovému uživateli zprávu o chybně zadaném uživatelském jménu, případně heslu. Uživatel je nucen znovu projít autentizačním procesem.

4.4 Přístup uživatele do systému (druhá fáze)

Po úspěšné autentizaci uživatelského účtu (první fáze autentizace), **se porovnává kombinace uživatelské MAC adresy a IP adresy se záznamy ve firewallu**. Pokud se nepodaří odpovídající záznam vyhledat, firewall automaticky začlení koncového uživatele do skupiny uživatelů s omezeným přístupem. Všechny požadavky komunikace této skupiny jsou přesměrovány na informační portál, který informuje daného uživatele o vzniklém problému a možnosti jeho odstranění.

4.5 Přiřazení šířky pásma

Pokud koncový uživatel projde první i druhou fází autentizace, hotspot deaktivuje přesměrování všech požadavků na vstupní portál a přiřadí mu tzv. **kvalitu služeb (QoS - Quality of Service)**. Tím jsou nastaveny potřebné parametry služby a uživatel je připojen k síti operátora. Spojení zůstává aktivní do jeho odhlášení nebo do expirace časového intervalu, při kterém nebyl generován žádný požadavek (ztráta signálu).

Možnosti nastavení QoS:

- nezávislé omezování přenosové rychlosti ve směru vysílání i příjmu,
- stanovení garantovaných a maximálních přenosových rychlostí,
- prioritizace libovolných datových toků,
- omezení fyzických rozhraní, virtuálních rozhraní, jednotlivých IP adres, rozsahů adres a libovolně označených paketů.

4.6 Účtování přenesených dat

O tuto záležitost se stará přístupový řídicí server ACS prostřednictvím služby SNMP Agent. Tato služba v pravidelných intervalech provádí sběr dat od jednotlivých HSR a ukládá je do databáze. Zde za pomoci skriptovacích jazyků se data konvertují do podoby grafů. Každý graf zachycuje přenosové rychlosti jednotlivých uživatelů v závislosti na čase, množství přenesených, informace o maximálním, průměrném a aktuálním vytížení linky. Jednotlivé grafy pak lze za pomoci služby web server publikovat na internetu pro veřejné nebo soukromé účely.

5. HARDWAROVÉ A SOFTWAREVÉ VYBAVENÍ SÍTĚ

5.1 Centrální propojovací bod (CCP)

Prvek CCP je v podstatě **SWITCH**. Řadí se mezi aktivní síťové prvky a vzájemně propojuje jednotlivé segmenty sítě. Ty se připojují do tzv. portů, kterých může mít switch libovolné množství (dle daného výrobce). Switch pracuje na linkové, některé typy na síťové vrstvě modelu ISO OSI. Na rozdíl od HUBu neposílá data všesměrově na všechny porty, nýbrž jen na port, kde se nachází adresát. Toho lze dosáhnout nasazením směrovacích tabulek, ve kterých si switch uchovává MAC adresy koncových uzlů. Tyto tabulky se průběžně aktualizují (protokol ARP). Nasazení switche tedy výrazně šetří síťové prostředky a umožňuje nám provozování plně duplexního spoje. S ohledem na koncepci hotspotové sítě je nezbytné, aby prvek CCP podporoval virtuální sítě, management, případně SNMP.

Rozhodnul jsem se z důvodu ceny a dostupnosti v roli CCP použít **switch SRW208** od firmy **Linksys**. Switch je osmiportový s podporou: VLAN, SNMP, QoS, autocross, autovyjednávání, diagnostika chybovostí ethernetových portů, monitorování ARP, spanning tree, zrcadlení portů atd.. Pro management SRW208 lze použít sériový port RS232C, nebo webového rozhraní. SRW208 pracuje na principu „store and forward“.

Store and Forward

Způsob přeposílání rámců, příchozí paket z určitého rozhraní je uložen do vyrovnávací paměti. Hlavička paketu je porovnána s tabulkou adres a paket je odeslán přes výstupní port adresátovi.

5.2 Přístupový řídicí server (ACS)

Prvek ACS je hardwarově realizován platformou osobního počítače se dvěma ethernetovými síťovými kartami, osazeného libovolným procesorem firmy AMD či Intel, který je vložen do kompatibilní základové desky. Velikost paměti RAM, výkon grafického akceleračního a celkový výkon sestavy volíme s ohledem na minimální požadavky operačního systému, který bude na sestavě provozován.

Vzhledem k funkcím, které má ACS vykonávat, je velmi vhodné použít jako operační systém „**Microsoft Windows Server 2003**“ a to z následujících důvodů:

- většina požadovaných služeb (NTP Client, DNS Server, SMTP Server, Radius Server, Remote Access, Web Server, atd.) je integrována v systému, tudíž není třeba hledat alternativní programy,

- operační systém umožňuje současné připojení více vzdálených klientů do systému. K tomuto účelu lze využít vzdálené plochy, console nebo jiné aplikace,
- mohutná databáze ovladačů pro přídavný hardware,
- systém lze používat jako router, firewall, print server, FTP server, VPN server / klient atd.

Minimální systémové požadavky:

CPU: minimální podporovaná frekvence 133 MHz
 minimální doporučená frekvence 550 MHz

RAM: 256MB

Minimální systémové požadavky není při dnešní technologii problém překročit i mnohonásobně. ACS však vzhledem k malému zpracovávanému objemu dat žádný extrémní výkon nepotřebuje.

5.3 Hotspotový směrovač (HSR)

Narozdíl od ACS bude volba vhodného hardwaru pro HSR více komplikovaná. Je třeba pečlivě zvážit jednotlivé komponenty, abychom dosáhli požadované přenosové kapacity, wifi pokrytí a stability systému.

5.3.1 Operační systém

Vzhledem k mým zkušenostem a znalostem systému firmy **MikroTik**, rozhodl jsem se pro hotspotový systém využít operačního systému **RouterOS v.3.10** (licence č.5). Operační systém je distribuován na Flash pamětech, microSD kartách a jiných nosičích. Lze jej nahrát do libovolného počítače nebo speciálně upraveného hardwaru a učinit z něj velice flexibilní síťový prvek. Hardware opatřený tímto operačním systémem lze po vhodné konfiguraci používat jako: router, switch, bridge, AP, VPN server, firewall, bandwidth manager, hotspot, VOIP brána atd.. Operační systém podporuje též svůj vlastní skriptovací jazyk.

5.3.2 Základová deska a procesor

Kompromisem mezi pořizovací cenou a požadavky na výkonnost HSR je speciální hardwarová platforma **RouterBoard**, opět od firmy **MikroTik**. Zaměřil jsem se na konkrétní model **RouterBoard 433AH** z důvodu kompromisu mezi cenou a výkonem.

RB433AH – 600Mhz (testováno na 2x 100Mb eth. rozhraních)			
Firewall	Sledování spojení	Mód	64B paket, Mb/s
N/A	vypnuto	Router	62,65
N/A	zapnuto	Router	49,79
Vypnut	vypnuto	Bridge	90,07
Zapnut	vypnuto	Bridge	57,14
Zapnut	zapnuto	Bridge	40,41

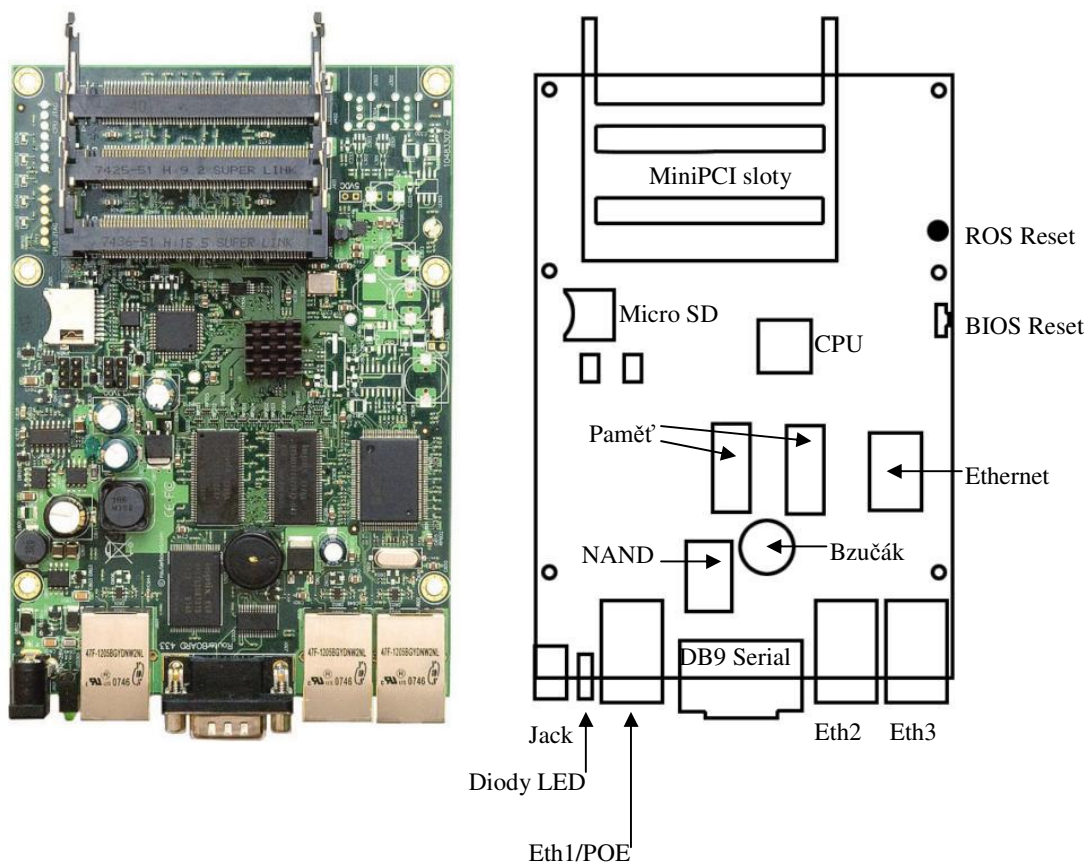
Tabulka 4: Teoretická přenosová rychlost RB-433AH

Tabulka 1 znázorňuje maximální teoretické přenosové rychlosti, kterých je RouterBoard 433AH schopen dosáhnout při kmitočtu 600MHz pro režim provozu jako Router nebo Bridge. Musíme však počítat s mnohem menší přenosovou rychlostí, z důvodu připojování koncových uživatelů přes bezdrátové rozhraní využívající normu 802.11b/g. Norma má uvedenou maximální teoretickou propustnost dat 54Mb/s.

Přehled parametrů :

CPU	Atheros AR7161 680MHz síťový procesor
RAM	128MB DDR SDRAM integrovaná paměť
Úložiště dat	64MB integrovaná NAND paměť + micro SD
Ethernet	3x 10/100 Mb/s eth. portů s Auto-MDI/X
MiniPCI	3 sloty
Extra	Resetovací přepínač, bzučák
Sériový port	DB9 RS232C asynchronní sériový port
LEDky	napájení, NAND, 5x uživatelských LED
Napájení	napájení po ethernetu 10..28V DC napájení přes JACK 10..28V DC
Spotřeba	3W, s osazenými mini PCI sloty max. 25W
Operační systém	MikroTik RouterOS v3, L5 licence

Tabulka 5: Přehled parametrů RB-433AH



Obrázek 7: Rozložení komponent RB-433AH

CPU

Výkonný čipset Atheros AR7161 s kmitočtem jádra 680MHz a možností přetaktování až na hodnotu 800Mhz.

Ethernetová rozhraní

Síťová rozhraní pro připojení ostatních periférií sítě prostřednictvím kříženého nebo přímého kabelu. Rozhraní podporují funkce autocross a autovyjednávání (nastaví přenosové rychlosti a duplexu podle protějšího zařízení).

MiniPCI sloty

Sloty pro rozšíření stávajícího hardwaru. Lze je osadit bezdrátovými, ethernetovými, GPRS, ISDN, nebo XDSL kartami atd..

Bzučák

Primárně signalizuje restart systému, lze však překonfigurovat, aby při ladění bezdrátových aplikací prezentoval měnícím se kmitočtem úroveň přijímaného signálu.

Sériový port

Jediné rozhraní určené pro konfiguraci RouterBoard, pokud jsou všechny ethernetové porty zablokovány. Slouží též pro přístup do BIOSU a k veškeré konfiguraci, při které ještě nebyl zaveden ovladač ethernetového portu nebo nebyla přidělena IP adresa.

Diody LED

Mimo standardní signalizace napájení a bootovací sekvence jsou uživatelské LED schopny za pomoci skriptů signalizovat nedostupnost internetové konektivity, přetížené CPU atd..

Napájení

Pro stabilní provoz je nutno použít kvalitní napájecí zdroj. Příkladem je typ 24HPOW (spínaný zdroj 24V; 38W; 1,6A). Platmoforma 433AH je totiž citlivá na slabý elektrický příkon či kolísání napájení. Napájení RouterBoardu lze řešit dvěma způsoby:

- připojením zdroje napájení přímo do konektoru JACK,
- k napájení využít první ethernetový port s podporou POE (Power Over Ethernet). Tím lze umístit RouterBoard na libovolné místo i mimo dosah elektrické zásuvky a napájecí napětí se přivede po síťovém kabelu.

5.3.3 Bezdrátové karty a příslušenství

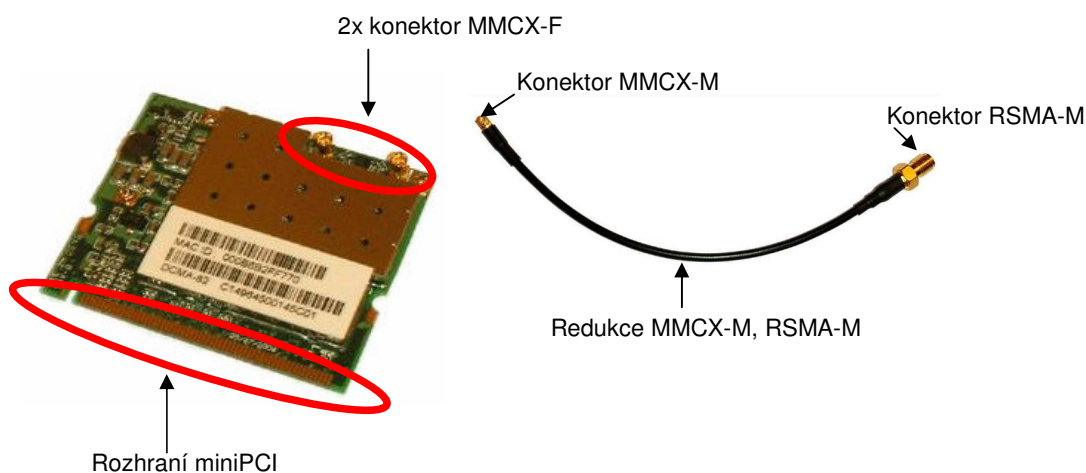
Bezdrátová karta slouží jako přístupový bod koncových uživatelů do systému. Má vliv na kvalitu a přenosovou rychlost celého spoje. Při její volbě je nutné zvážit několik důležitých parametrů:

- rozhraní,
- vysílací výkon,
- citlivost přijímaného signálu,
- provozovací kmitočet,
- podporované normy,
- modulace.

Volím Kartu **CM11-HP** od firmy **Atheros**, především z důvodu vysoké citlivosti a vysílacího výkonu, který lze regulovat. Další výhodou je její provedení. Obsahuje duální vysílač, lze jej nakonfigurovat pro práci v kmitočtovém pásu 2,4GHz i 5GHz. Karta je opatřena dvěma konektory, ty slouží pro připojení přídatné anténní soustavy. Souhrn těch nejdůležitějších parametrů je zobrazen v tabulce 6.

Specifikace bezdrátové karty CM-11HP	
Rozhraní:	miniPCI
Operační mód:	AP, Client, AD-HOC
Frekvence:	2,4 ; 5 GHz
Přenosová rychlost:	54Mb/s
Podporované normy:	802.11a/b/g
Chipset:	Atheros AR5414A
Konektory:	2x MMCX
Regulace výkonu:	ano
Max. výstupní výkon:	28dBm
Citlivost:	-96dBm
Modulace:	DSSS, OFDM

Tabulka 6: Specifikace bezdrátové karty CM-11 HP



Obrázek 8: CM-11HP + pigtail MMCX-M, RSMA-M

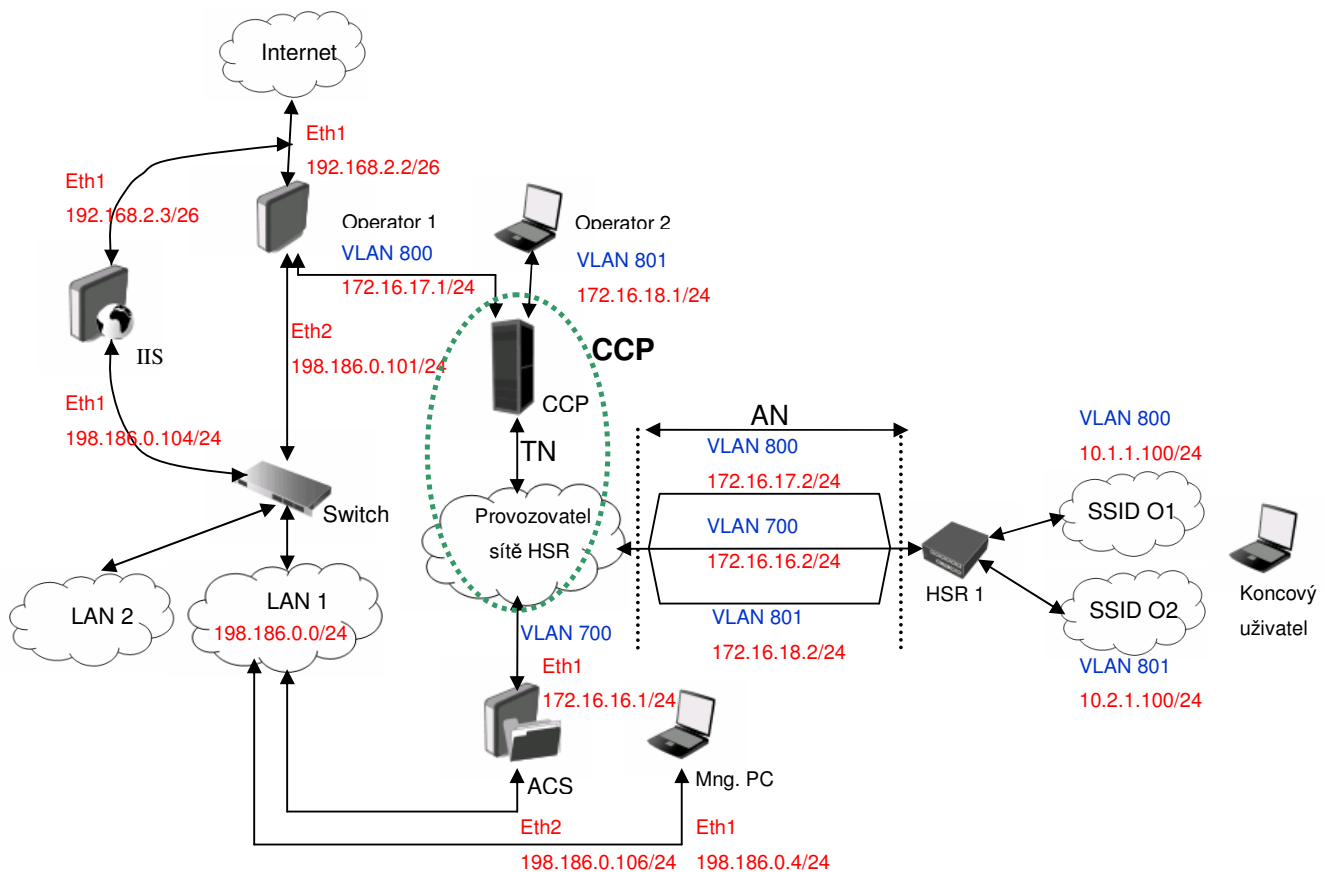
Kartu CM-11HP není možné přes integrované konektory spojit přímo z anténní soustavou z důvodu miniaturních rozměrů. Připojení k anténní soustavě musí být zprostředkováno přes redukci. Redukce se konektorem MMCX-M připojuje k bezdrátové kartě a konektorem RSMA-M je pevně uchycena ke kovovému krytu RouterBoardu. Celá propojka je vyrobena ze speciálního materiálu, který přenáší vysokofrekvenční signál s minimálním útlumem.

6. REALIZACE EXPERIMENTÁLNÍ SÍTĚ

V rámci této kapitoly je vytvořeno základní funkční zapojení experimentální sítě včetně popisu konfigurace jednotlivých síťových prvků. Zapojení experimentální sítě vychází z modelu publikovaném v kapitole číslo 4 (obrázek2, obrázek3). Původní model zapojení bude modifikován do podoby viz obrázek 9 z následujících důvodů:

- nedostatek hardwaru pro simulování více jak dvou operátorů,
- přehlednost zapojení,
- implementace experimentální sítě do stávající funkční infrastruktury.

Dále jsem provedl sloučení prvků Provozovatel sítě HSR, CCP a TN opět z důvodu nedostatku hardwaru. Všechny tyto popsané síťové prvky budou nahrazeny jedním CCP.



Obrázek 9: Schema zapojení – laboratorní prostředí

Operator 1

Směrovač, připojuje původní infrastrukturu (LAN1, LAN2) a VLAN 800 k internetu.

Operator 2

Notebook připojen k síti VLAN801, plní též funkci serveru pro testování přenosových rychlostí.

CCP

Centrální propojovací bod, slučuje v sobě prvky: Provozovatel sítě HSR, CCP, TN a primárně propojuje HSR se sítí operátorů.

HSR 1

Hotspotový směrovač, přístupový bod pro koncové uživatele.

Koncový živitel

Notebook využívající síťových prostředků některého z operátorů.

Mng. PC

Notebook pro správu ACS (vzdálený přístup) a jeho prostřednictvím též konfiguraci a monitorování činnosti HSR1.

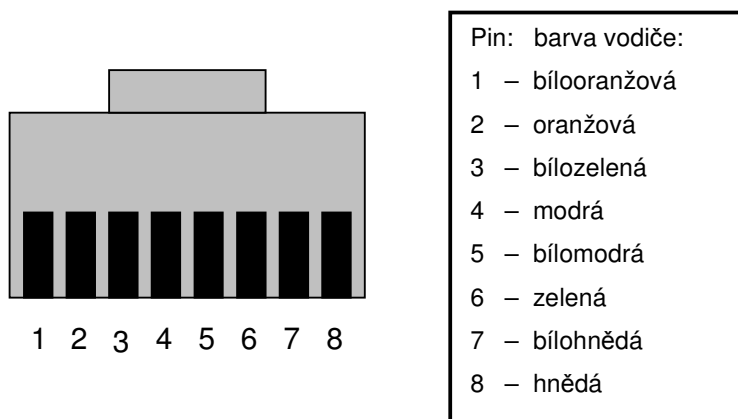
IIS

Informační webový portál pro potřeby HSR (chybové hlášení při selhání druhého stupně autentizace viz kapitola 4.4).

Návrh sítě dle obrázku 8 v sobě skrývá čtyři samostatné, navzájem izolované sítě.

1. **subnet 198.186.0.0/24** – tato část sítě připojuje uživatele segmentu LAN1, LAN2, ACS, IIS a Mng. PC dohromady. Všechny zmiňované prvky mají přístup k internetu skrze router s lokální IP 198.186.0.101/24
2. **VLAN 700 (monitorovací a konfigurační kanál)** – spojení mezi ACS a HSR1.
3. **VLAN 800 (datový kanál)** – spojení mezi koncovými uživateli připojenými k SSID1 a Operátorem 1.
4. **VLAN 801 (datový kanál)** – propoj mezi koncovými uživateli připojenými k SSID2 a Operátorem 2.

Přístupová síť (AN) je realizována metalickým přímým UTP kabelem kategorie 5. Oba konektory propojovacího kabelu jsou zapojeny dle barevného kódu viz obrázek 9.



Obrázek 10: Schema zapojení konektoru RJ45 – přímý kabel

6.1 Konfigurace hotspotového směrovače (HSR)

Vzhledem k tomu, že žádné z fyzických rozhraní HSR nemá v továrním stavu přidělenou IP adresu, je nutné prvotní konfiguraci provést přes MAC telnet, případně Hyperterminál. Je zvolena možnost připojení přes windowsovský program hyperterminál prostřednictvím asynchronního sériového portu RS232C. Nastavuji následující parametry linky.

Bity za sekundu:	115200
Datové bity:	8
Parita:	žádná
Počet stop-bitů:	1
Řízení toku:	Hardware

Tabulka 7: Konfigurace portu RS232C

Po připojení napájecího konektoru k HSR máme možnost sledovat bootovací proces, konfigurovat BIOS, případně vyčkat než proběhnou veškeré bootovací kroky a systém bude připraven k použití. Po zadání uživatelského jména a hesla se dostaneme do režimu konfigurace.

6.1.1 Bezdrátový síťový adaptér

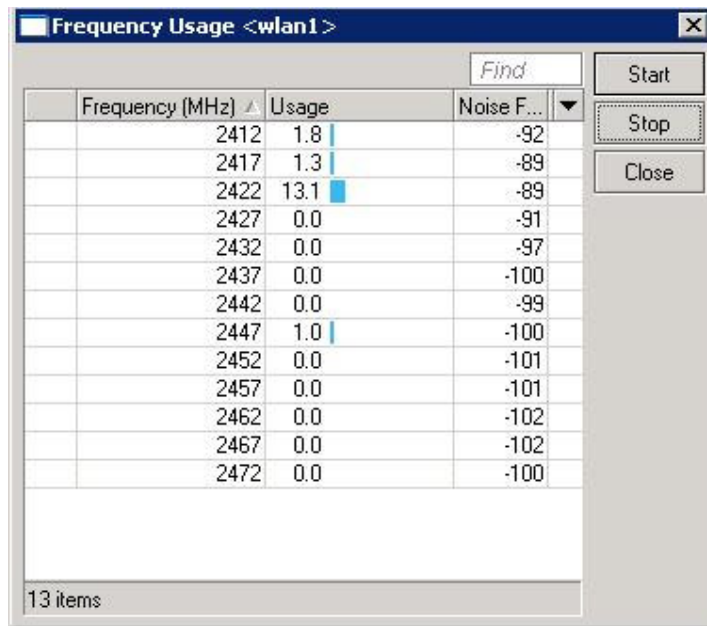
Bezdrátová karta je v továrním nastavení deaktivovaná. Než ji aktivujem, **je nezbytné připojit anténní soustavu**, která zaručí obvodové přizpůsobení. Vzhledem k tomu, že prozatím budeme hotspotový systém provozovat v interiérových prostorech, postačí jako anténa dipól se ziskem 3dB. Pokud anténu nepřipojíme, může dojít k poškození vstupních obvodů bezdrátové karty. Vysílací výkon by se vlivem špatného přizpůsobení v kabelové trase odrážel a vracel zpět na vstup karty. **Míra přizpůsobení je udána poměrem stojatých vln (PSV).**

Následující část kódu detailně popisuje výsledek konfigurace bezdrátové karty. Systém umožňuje na jednom fyzickém bezdrátovém rozhraní vytvořit až 127 virtuálních rozhraní. Každé z nich má odlišnou MAC-adresu a identifikátor SSID. Virtuální rozhraní se navenek koncovému uživateli jeví jako samostatná bezdrátové síť. **Jsou vytvořeny dvě virtuální rozhraní „wlan1“, „wlan2“ a každému z nich je přidělen identifikátor SSID. Podporované standardy jsou 802.11b/g.** Přístup do systému je omezen na základě úrovně přijímaného signálu ze strany klienta (RSL). Hodnota RSL je udávána v dBm a rozhodovací hladina je stanovena na -70dBm. Klientům, kteří nesplňují toto omezení, nebude umožněn přístup do systému. Tato restrikce je důležitá z pohledu kvalitního poskytování služeb a přenosové rychlosti. Klient s nepříznivou hodnotou RSL by totiž způsobil neustálé přepínání modulačních rychlostí a tím by způsobil zpoždění a celkovou degradaci přenosové rychlosti hotspotového systému. Celková přenosová rychlost se vždy přizpůsobuje nejpomalejšímu segmentu sítě. Bezdrátová karta je nakonfigurována pro pásmo 2,4Ghz - kmitočet 2462Mhz. K připojení anténní soustavy se používá konektor A. **Kmitočet provozování sítě byl vybrán na základě radiového měření okolí, hladiny šumu a vytížení jednotlivých kanálů.**

	Address	SSID	Band	Fre...	Signa...	Noise...	Signa...	Radio Name	RouterD...
AB	00:11:2F:90:E6:A6	killer wifi	2.4GHz-G	2412	-52	-100	48		
AB	00:30:4F:4A:FB:4A	Knetwork...	2.4GHz-G	2412	-90	-100	10		
AB	00:19:E0:6D:80:80	damborice7	2.4GHz-G	2422	-88	-100	12		
ABP	00:0C:42:26:77:94		2.4GHz-G	2447	-89	-100	11	000C42267794	3.14

4 items

Obrázek 11: Prozkoumávání radiového okolí



Obrázek 12: Vytížení jednotlivých radiových kanálů

Konfigurace bezdrátové karty:

```
[admin@MikroTik] /interface wireless> print
Flags: X - disabled, R - running
0 name="wlan1" mtu=1500 mac-address=00:0B:6B:2D:BA:A7 arp=enabled
  interface-type=Atheros AR5413 mode=ap-bridge ssid="HSR_Operator_1"
  frequency=2462 band=2.4ghz-b/g scan-list=default antenna-mode=ant-a
  wds-mode=disabled wds-default-bridge=none wds-ignore-ssid=no
  default-authentication=yes default-forwarding=no default-ap-tx-limit=0
  default-client-tx-limit=0 hide-ssid=no security-profile=default
  compression=no
1 name="wlan2" mtu=1500 mac-address=02:0B:6B:2D:BA:A7 arp=enabled
  master-interface=wlan1 ssid="HSR_Operator_2" wds-mode=disabled
  wds-default-bridge=none wds-ignore-ssid=no default-authentication=yes
  default-forwarding=no default-ap-tx-limit=0 default-client-tx-limit=0
  hide-ssid=no security-profile=default
```

Omezení přístupu do systému klientským stanicím, nevyhovujícím kritériu **RSL ≤ -70dBm**

```
[admin@Hotspot] /interface wireless access-list> print detail
Flags: X - disabled
0 ;; klienti_Wlan1
  mac-address=00:00:00:00:00:00 interface=wlan1 signal-range=-70.120
  authentication=yes forwarding=no ap-tx-limit=0 client-tx-limit=0
  private-algo=none private-key="" private-pre-shared-key=""
```

```

1 ;; klienti_Wlan2
  mac-address=00:00:00:00:00:00 interface=wlan2 signal-range=-70.120
  authentication=yes forwarding=no ap-tx-limit=0 client-tx-limit=0
  private-algo=none private-key="" private-pre-shared-key=""

2 ;; servis
  mac-address=00:16:6F:9C:CC:17 interface=2,4GHz signal-range=-120.120
  authentication=yes forwarding=yes ap-tx-limit=0 client-tx-limit=0
  private-algo=none private-key="" private-pre-shared-key=""

```

Bezdrátová karta je nyní nakonfigurována, osazena anténní soustavou a připravena k použití. Abychom se nedostali do rozporů s předpisy ČTÚ, je nezbytné změřit vysílací výkon bezdrátové karty a případně provést korekci. K měření vysílacího výkonu a PSV jsem použil měřicí přístroj : **PSV monitor DM2G4** a byly naměřeny následující parametry.

Pvýst	22,3dB
PSV	-14dB

Tabulka 9: Měření parametrů bezdrátové karty přístrojem PSV monitor DM2G4

Hodnota PSV v dB formě vypovídá o výkonu, který se odráží od nepřizpůsobené anténní soustavy a vrací se zpět na vstup bezdrátové karty. PSV jsem srovnal s tabulkou výrobce měřicího přístroje a lze jej klasifikovat slovem „**dobré**“.

Efektivní vysílací výkon je definován, jak jsem již uvedl v kapitole 3., součtem vysílacího výkonu bezdrátové karty a zisku anténní soustavy. Od tohoto výsledku se odečte útlum konektorů a kabelové trasy. V našem případě se dostaneme na hodnotu **P_{ef} = 24 dB**, což je **překročení povolené hodnoty o +4 dB. Je nutné provést korekci!**

Korekce vysílacího výkonu:

```
[admin@MikroTik] /interface wireless> set wlan1 tx-power-mode=all-rates-fixed 18
```

6.1.2 Konfigurace VLAN

Implementace protokolu 802.1Q umožňuje vytvoření až 4095 virtuálních kanálů na jednom ethernetovém nebo bezdrátovém rozhraní. Každý virtuální kanál je opatřen jedinečným VLAN ID. VLAN je logické seskupení, umožňující vzájemnou komunikaci uživatelů (majícím stejnou VLAN ID), jako by byli všichni spojeni v jedné izolované LAN, nezávisle na fyzické konfiguraci sítě. Virtuální rozhraní jsou nakonfigurována podle následující tabulky a jsou připojena k příslušnému fyzickému rozhraní.

```
[admin@MikroTik] /interface vlan> print
Flags: X - disabled, R - running, S - slave
#  NAME                MTU  ARP    VLAN-ID  INTERFACE
0  R  VLAN700              1500 enabled  700      ether1
1  R  VLAN_800_SSID1      1500 enabled  800      wlan1
2  R  VLAN_801_SSID2     1500 enabled  801      wlan2
3  R  VLAN800             1500 enabled  800      ether1
4  R  VLAN801             1500 enabled  801      ether1
```

6.1.3 Přemostění

Slouží k namapování koncových uživatelů do příslušných VLAN. Jsou vytvořeny dvě přemostění : **bridge 800** a **bridge 801**, vzájemně propojují rozhraní definované v tabulce portů.

```
[admin@MikroTik] /interface bridge> print
Flags: X - disabled, R - running
0  R  name="bridge800" mtu=1500 arp=enabled mac-address=00:0B:6B:2D:BA:A7
    protocol-mode=none priority=0x8000 auto-mac=yes
    admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s
    transmit-hold-count=6 ageing-time=5m

1  R  name="bridge801" mtu=1500 arp=enabled mac-address=00:00:00:00:00:00
    protocol-mode=none priority=0x8000 auto-mac=yes
    admin-mac=00:00:00:00:00:00 max-message-age=20s forward-delay=15s
    transmit-hold-count=6 ageing-time=5m
```

```
[admin@MikroTik] /interface bridge> port print
Flags: X - disabled, I - inactive, D - dynamic
#  INTERFACE          BRIDGE          PRIORITY  PATH-COST
0  VLAN_800_SSID1     bridge800       0x80      10
1  wlan1              bridge800       0x80      10
2  wlan2              bridge801       0x80      10
3  VLAN_801_SSID2     bridge801       0x80      10
```

6.1.4 IP adresace rozhraní

IP adresy jsou přiřazeny pouze virtuálním rozhráním, což nám zajistí požadavek propouštění pouze paketů opatřené značkou. Do systému nelze připojit žádné zařízení, které by nebylo součástí některé z VLAN.

```

-----
admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS      NETWORK      BROADCAST    INTERFACE
0   ;;; rozsah provozovatele
   172.16.16.2/24 172.16.16.0   172.16.16.255 VLAN700
1  10.1.1.100/24  10.1.1.0     10.1.1.255   VLAN_800_SSID1
2  10.2.1.100/24  10.2.1.0     10.2.1.255   VLAN_801_SSID2
3  ;;; rozsah operátora
   172.16.17.2/24 172.16.17.0   172.16.17.255 VLAN800
4  172.16.18.2/24 172.16.18.0   172.16.18.255 VLAN801
-----

```

6.1.5 DHCP server

DHCP server je služba přidělující koncovým uživatelům IP adresu z předem definovaného adresního rozsahu. Nejprve se tedy definují adresní rozsahy. Potřebujeme dva rozsahy, protože nabízíme služby dvou operátorů.

```

-----
[admin@MikroTik] /ip> pool print
# NAME          RANGES
0 SSID1_pool    10.1.1.1-10.1.1.10
1 SSID2_pool    10.2.1.1-10.2.1.10
-----

```

Příslušné rozsahy a přídatná nastavení pak aplikujeme na jednotlivé DHCP servery, které přidělují IP adresy přemostovacím rozhraním bridge 800 a bridge 801. Jako doplňkové informace jsou nastaveny IP adresy DNS serverů. Doba zapůjčení IP adresy je tři dny.

```

-----
[admin@MikroTik] /ip dhcp-server> print
Flags: X - disabled, I - invalid
# NAME  INTERFACE  ADDRESS-POOL  LEASE-TIME  ADD-ARP
0 vlan800 bridge800    SSID1_pool   3d          yes
1 vlan801 bridge801    SSID2_pool   3d          yes
-----

```

```

[admin@MikroTik] /ip dhcp-server> network print
# ADDRESS  GATEWAY  DNS-SERVER
0 10.1.1.0/24 10.1.1.100 10.1.1.100
1 10.2.1.0/24 10.2.1.100 10.2.1.100
-----

```

6.1.6 DNS

DNS server je služba obstarávající překlad jmen na IP adresy. Díky této službě si koncový uživatel nemusí pamatovat žádné IP adresy. Pro adresaci požadovaného zdroje si vystačí se jmenným názvem.

DHCP server se odkazuje na DNS HSR, je proto **nutné nakonfigurovat replikaci požadavků** v případě, kdy požadovaný překlad jména na adresu nenajdeme v tabulkách HSR. **Primary a secondary DNS servery jsou přiděleny Operátorem 1.**

```
[admin@MikroTik] /ip dns> print
primary-dns:          10.3.3.1
secondary-dns:       212.24.128.8
allow-remote-requests: yes
max-udp-packet-size: 512
cache-size:          2048KiB
cache-max-ttl:       1w
cache-used:          23KiB
```

6.1.7 Směrovací tabulky a NAT

Routeing je služba, zajišťující směrování paketů od odesílatele k příjemci. Snaha o nalezení nejkratší/nejefektivnější cesty mezi uzly. Směrování zajišťuje třetí vrstva modelu ISO OSI. Aby data byla posílána správným směrem a byl zastižen adresát, je třeba vytvořit směrovací tabulku. Tato tabulka nám určuje odkud kam budou data směrována.

```
[admin@MikroTik] /ip> route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
```

#	DST-ADDRESS	PREF-SRC		GATEWAY	DIST.	GATEWAY
0	A S 0.0.0.0/0	172.16.17.2	reachable	172.16.17.1	1	VLAN800
1	ADC 10.1.1.0/24	10.1.1.100			0	bridge800
2	ADC 10.2.1.0/24	10.2.1.100			0	bridge801
3	ADC 172.16.16.0/24	172.16.16.2			0	VLAN700
4	ADC 172.16.17.0/24	172.16.17.2			0	VLAN800
5	ADC 172.16.18.0/24	172.16.18.2			0	VLAN801

NAT je definován podle následujícího výpisu, zajišťuje překlad síťových adres a maskování koncových uživatelů za odpovídající rozhraní.

Položka „RESTRICTED“ přesměruje všechny uživatele, kteří korektně neprošli druhou fází autentizace na informační webové stránky. Zde jsou k dispozici informace nezbytné pro odstranění problémů s autentizací.

Položka „Test_IPERF“ proroutuje síť operátora a provozovatele hotspotového systému za účelem provozování diagnostické aplikace. Tato aplikace je schopna proměřit konstantním datovým TCP/UDP tokem přenosovou rychlost jednotlivých uživatelů v obou směrech.

```

-----
[admin@Hotspot] /ip firewall nat> print
Flags: X - disabled, I - invalid, D - dynamic
0 ;;; ---RESTRICTED---
  chain=hs-auth action=dst-nat to-addresses=192.168.2.3 to-ports=8001
  src-address-list=restricted hotspot=http protocol=tcp

1 ;;; ---NAT pro VLAN ID---
  chain=srcnat action=masquerade src-address=10.1.1.0/24
  out-interface=VLAN800

2 chain=srcnat action=masquerade src-address=10.2.1.0/24
  out-interface=VLAN801

3 ;;; ---Test_IPERF_VLAN800---
  chain=dstnat action=dst-nat to-addresses=10.1.1.10 to-ports=5001
  dst-address=172.16.17.2 in-interface=VLAN800 dst-port=5001 protocol=tcp

4 ;;; ---Test_IPERF_VLAN801---
  chain=dstnat action=dst-nat to-addresses=10.2.1.10 to-ports=5001
  dst-address=172.16.17.2 in-interface=VLAN801 dst-port=5001 protocol=tcp

5 ;;; ---Test_IPERF_VLAN801---
  chain=dstnat action=dst-nat to-addresses=10.2.1.9 to-ports=5002
  dst-address=172.16.17.2 in-interface=VLAN801 dst-port=5002 protocol=tcp
-----

```

6.1.8 Firewall

Firewall je služba propouštějící data ze vstupu HSR na výstup a naopak. Službu Firewall lze detailně konfigurovat pomocí tzv. seznamu pravidel. Jednotlivá pravidla se uplatňují v pořadí, ve kterém jsou zapsána. Při implementaci byla použita metoda, která zakazuje veškerý provoz a dodatečně jsou povoleny pouze služby, nezbytné pro provoz systému. Zabezpečení se týká především rozhraní VLAN700, které jako jediné umožňuje administraci systému. Dále je zabezpečen přístup koncových klientů k jednotlivým operátorům na základě porovnávání MAC adres (fruhá fáze autentizace).

```

-----
[admin@Hotspot] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
0 ;;; ---HSR_Interfaces---
  chain=input action=accept src-address-list=VLAN800_SSID1

1 chain=input action=accept src-address-list=VLAN801_SSID2

2 ;;; ---user_Romek---
  chain=input action=accept src-address-list=Romek
-----

```

```

3  ;;; ---RESTRICTED_addr_list---
  chain=input action=add-src-to-address-list src-address=10.1.1.0/24
  address-list=restricted address-list-timeout=5m

4  chain=input action=add-src-to-address-list src-address=10.2.1.0/24
  address-list=restricted address-list-timeout=5m

5  chain=input action=log src-address-list=restricted log-prefix=""

6  ;;; VLAN_700_time_synch
  chain=input action=accept in-interface=VLAN700 dst-port=123 protocol=udp

7  ;;; VLAN_700_ICMP
  chain=input action=accept in-interface=VLAN700 protocol=icmp

8  ;;; VLAN_700_winbox
  chain=input action=accept in-interface=VLAN700 dst-port=8291
  protocol=tcp

9  ;;; VLAN_700_SNMP
  chain=input action=accept in-interface=VLAN700 dst-port=161 protocol=udp

10 ;;; VLAN_700_RADIUS
  chain=input action=accept in-interface=VLAN700 src-port=1812-1813
  protocol=udp

11 ;;; VLAN_700_SYSLOG
  chain=output action=accept out-interface=VLAN700 dst-port=514
  protocol=udp

12 ;;; VLAN_700_DNS_mon
  chain=input action=accept in-interface=VLAN700 dst-port=53 protocol=udp

13 ;;; VLAN_700_SSH
  chain=input action=accept in-interface=VLAN700 dst-port=22 protocol=tcp

14 ;;; Deny_all_other_services
  chain=input action=drop in-interface=VLAN700

15 ;;; VLAN_800_winbox
  chain=input action=drop in-interface=VLAN800 dst-port=8291 protocol=tcp

16 ;;; VLAN_801_winbox
  chain=input action=drop in-interface=VLAN801 dst-port=8291 protocol=tcp

```

6.1.9 Značkování paketů (Mangle)

Značkování paketů je služba, která požadované TCP pakety opatří značkou a následně zpracovává dle definovaných pravidel. Následující zápis: **0, 1, 2, 3, 5, 6, 7, 8** zajišťuje označkování paketů datového toku v dopředném i zpětném směru pro rozhraní „**VLAN800**“, „**VLAN801**“ a uživatele „**Romek**“. U takto označených paketů můžeme sledovat statistiky o přenesených datech, aplikovat na ně různá nastavení firewallu a kvality služeb (QoS - duality of services) . Zápis: **4** ověřuje shodu MAC adres připojeného koncového klienta se statickým seznamem.

```
[admin@Hotspot] /ip firewall mangle> print
Flags: X - disabled, I - invalid, D - dynamic
0  ;;; VLAN800_dw
   chain=prerouting action=mark-packet new-packet-mark=VLAN800_dw
   passthrough=yes in-interface=VLAN800

1  ;;; VLAN800_up
   chain=postrouting action=mark-packet new-packet-mark=VLAN800_up
   passthrough=yes out-interface=VLAN800

2  ;;; VLAN801_dw
   chain=prerouting action=mark-packet new-packet-mark=VLAN801_dw
   passthrough=yes in-interface=VLAN801

3  ;;; VLAN801_up
   chain=postrouting action=mark-packet new-packet-mark=VLAN801_up
   passthrough=yes out-interface=VLAN801

4  ;;; USER Roman
   chain=prerouting action=add-src-to-address-list address-list=Romek
   address-list-timeout=1m src-mac-address=00:16:6F:9C:CC:18

5  chain=prerouting action=mark-connection new-connection-mark=Roman-con_up
   passthrough=yes src-address-list=Romek

6  chain=postrouting action=mark-connection new-connection-mark=Roman-con_dw
   passthrough=yes dst-address-list=Romek

7  chain=prerouting action=mark-packet new-packet-mark=Roman_up
   passthrough=yes src-address-list=Romek connection-mark=Roman-con_up

8  chain=postrouting action=mark-packet new-packet-mark=Roman_dw
   passthrough=yes dst-address-list=Romek connection-mark=Roman-con_dw
```

6.1.10 Virtuální hotspot

Virtuální hotspot je předchystaný soubor pravidel firewallu a NAT, který ověřuje oprávnění jednotlivých uživatelů k přístupu do systému. Tato pravidla se generují automaticky, je specifikováno pouze rozhraní, na která budou uplatněna (**Bridge 800**, **Bridge 801**) a rozsah platných IP adres.

```
-----  
admin@Hotspot] /ip hotspot> print  
Flags: X - disabled, I - invalid, S - HTTPS  
# NAME      INTERFACE  ADDRESS-POOL  PROFILE  
0 VLAN800    bridge800    SSID1_pool    default  
1 VLAN801    bridge801    SSID2_pool    default  
-----
```

Oba virtuální hotspotové servery jsou nakonfigurovány dle profilu: „default“, viz následující zdrojový kód.

html-directory=hotspot

Webová stránka, která se používá pro autentizaci uživatelů (uložena na flash paměti HSR).

login-by=cookie,http-chap,http-pap

Způsob autentizace koncového uživatele (uživatelského jméno a heslo).

use-radius=yes radius-accounting=yes

Autentizace je zprostředkována radius serverem ACS.

```
-----  
[admin@Hotspot] /ip hotspot profile> print  
Flags: * - default  
0 * name="default" hotspot-address=0.0.0.0 dns-name="" html-directory=hotspot  
rate-limit="" http-proxy=0.0.0.0:0 smtp-server=0.0.0.0  
login-by=cookie,http-chap,http-pap http-cookie-lifetime=3d  
split-user-domain=no use-radius=yes radius-accounting=yes  
radius-interim-update=received nas-port-type=ethernet  
radius-default-domain="" radius-location-id="" radius-location-name=""  
-----
```

6.1.11 Radius klient

Klient Radius je služba vytáčená klientem, prostřednictvím protokolu AAA slouží pro vzdálenou autentizaci, autorizaci a účtování koncových uživatelů. Následující výčet vysvětluje nejdůležitější nastavení:

service=hotspot

Rozhraní, ze kterého se budou přeposílat autentizační požadavky.

address=172.16.16.1

Cílová adresa Radius serveru = ACS.

secret="RB-433AH"

Heslo pro zabezpečení komunikace mezi Radius serverem a Radius klientem.

authentication-port=1812 accounting-port=1813

UDP porty, přes které probíhá ověřování koncových klientů.

POZN: UDP porty 1812 a 1813 je nezbytné též povolit ve firewallu.

```
[admin@Hotspot] /radius> print detail
```

```
Flags: X - disabled
```

```
0 service=hotspot called-id="" domain="" address=172.16.16.1
```

```
secret="RB-433AH" authentication-port=1812 accounting-port=1813
```

```
timeout=1s accounting-backup=no realm=""
```

6.1.12 SNMP server

SNMP je protokol (služba), který zasílá agentovi v pravidelných časových intervalech hodnoty svých čítačů. Tímto způsobem jsme schopni získat o zařízení nejrůznější informace jako jsou: vytížení CPU, uptime, aktuální přenosová rychlost jednotlivých fyzických rozhraní atd. Protokol je velice vhodný pro monitorování dílčích prvků sítě a na jeho principu je též založeno účtování přenesených dat dílčích uživatelů. HSR podporuje pouze SNMP v.1. Pro správnou funkci stačí vyplnit jméno komunity a IP adresu (případně rozsah IP) síťových prvků, mající oprávnění zpracovávat údaje od HSR. Konkrétní konfigurace je zobrazena v následujícím textu.

```
[admin@Hotspot] /snmp> community print
```

#	NAME	ADDRESS	SECURITY	READ-ACCESS
0	RB-433AH	172.16.16.1/32	none	yes

6.1.13 Kontrola šířky pásma a kvalita služeb (QoS)

Kontrola šířky pásma a kvalita služeb je metoda, která se využívá nejen k omezování přenosových rychlostí v obou směrech, ale hlavně k upřednostňování datových toků, případně zaručení spravedlivého rozložení přenosové kapacity. Pro potřebu hotspotového systému je navržena hierarchická struktura, která je zobrazena na obrázku 13.

Name	Parent	Packet Mark	Queue Type	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes
VLAN800_dw	global-out	VLAN800_dw	synchronous-default	10M	10M	0 bps	0 B	801.9 KiB
Lucie_dw	VLAN800_dw	Lucie_dw	synchronous-default	2M	5M	0 bps	0 B	0 B
Roman_dw	VLAN800_dw	Roman_dw	synchronous-default	4M	5M	0 bps	0 B	801.9 KiB
VLAN800_up	global-in	VLAN800_up	synchronous-default	10M	10M	0 bps	0 B	259.1 KiB
Lucie_up	VLAN800_up	Lucie_up	synchronous-default	2M	5M	0 bps	0 B	0 B
Roman_up	VLAN800_up	Roman_up	synchronous-default	4M	5M	0 bps	0 B	259.1 KiB
VLAN801_dw	global-out	VLAN801_dw	synchronous-default	5M	5M	0 bps	0 B	3421.1 MiB
Franta_dw	VLAN801_dw	Franta_dw	synchronous-default	3M	5M	0 bps	0 B	2760.9 MiB
Ondra_dw	VLAN801_dw	Ondra_dw	synchronous-default	2M	4M	0 bps	0 B	660.1 MiB
VLAN801_up	global-in	VLAN801_up	synchronous-default	5M	5M	0 bps	0 B	5.0 GiB
Franta_up	VLAN801_up	Franta_up	synchronous-default	3M	5M	0 bps	0 B	3949.7 MiB
Ondra_up	VLAN801_up	Ondra_up	synchronous-default	2M	4M	0 bps	0 B	1175.9 MiB

Obrázek 13: QoS

Z obrázku 13 jsou patrné dvě rodičovské větve: VLAN_800 a VLAN_801, každá s přenosovou kapacitou v dopředném i zpětném směru viz obrázek 13.. Mají také oproti koncovým uživatelům nastavenou nejvyšší prioritu odběru služeb. Těmto rodičovským větvím jsou přiděleni koncoví uživatelé. Jejich přenosová rychlost závisí na charakteru odebírané služby. Pro koncové uživatele se přenosová rychlost definuje ve dvou hladinách: **CIR = garantovaná přenosová rychlost** a **MIR = maximální přenosová rychlost**. Vzhledem k tomu, že koncoví uživatelé mají nastavenou stejnou prioritu, systém se snaží jejich požadavky komunikace odbavovat spravedlivě. **Aby systém mohl pracovat správně, je nutno dodržet následující podmínku:**

$$\sum CIR_{user} \leq CIR_{parent}$$

To znamená, že součet garantovaných přenosových rychlostí všech uživatelů musí být menší nebo roven garantované přenosové rychlosti rodičovské větve.

Pokud je předchozí podmínka splněna, uživatel odebírá službu s parametry MIR až do doby, než se připojí další uživatelé. V tomto případě rodičovská větev není nadále schopna zajistit MIR pro všechny koncové uživatele a redukuje jejich přenosovou rychlost, maximálně však na hodnotu CIR. Redukci přenosového pásma zajišťuje algoritmus:“ **Random Early Detection**“ (**RED**). Tento algoritmus v případě potřeby zahazuje jednotlivým relacím náhodně pakety a tím je dosaženo požadované redukce datového toku. Algoritmus má v sobě též implementovaný tzv „ **paketový burst**“. Paketový burst je akcelérátor, který umožní stanovenému počtu paketů dosáhnout větší přenosové rychlosti, než je dána parametrem MIR. Tato funkce je pouze krátkodobá a je vhodná především při načítání webových stránek. Umožňuje tak koncovým uživatelům s nízkou přenosovou rychlostí svižné načítání webových stránek.

6.1.14 Ostatní služby

Klient NTP

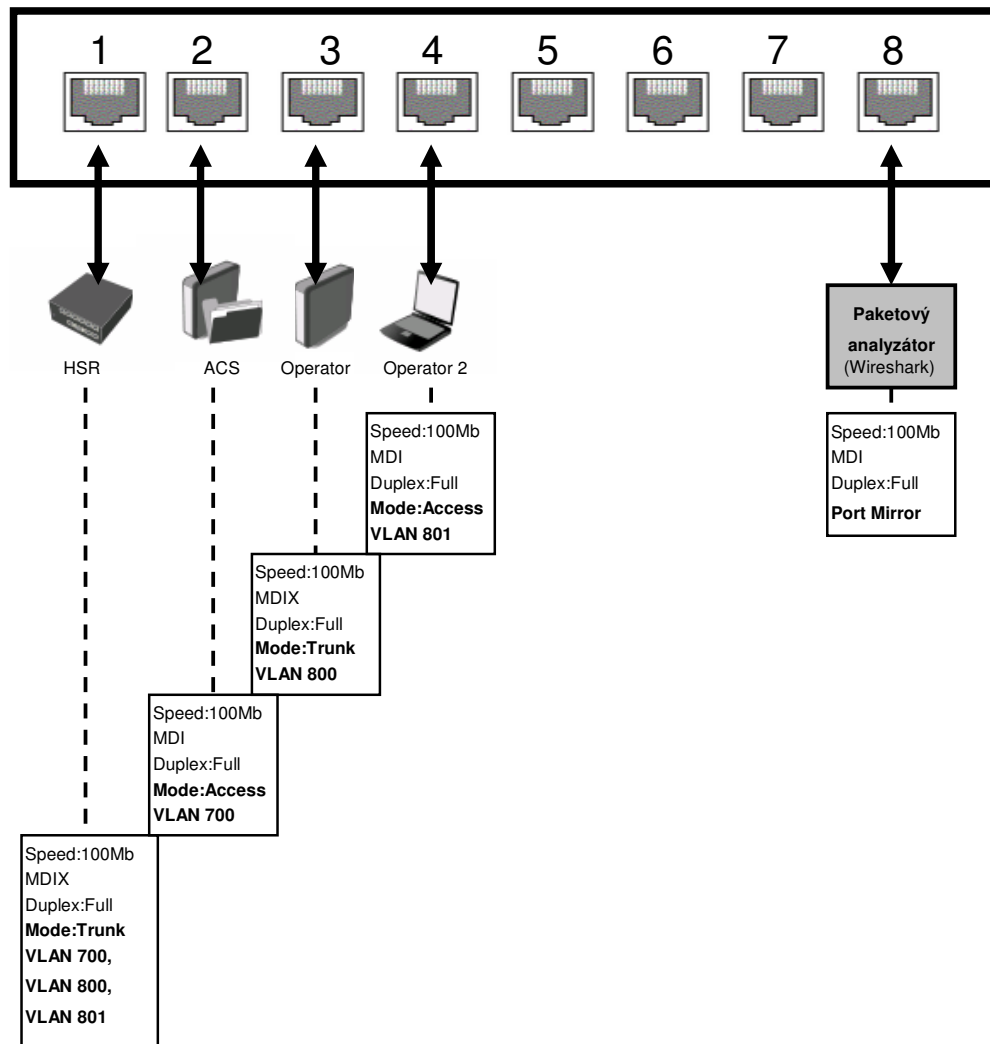
Služba využívající NTP protokolu (UDP port:123) pro synchronizaci hodin přes paketové sítě. Všechny HSR budou synchronizovány z ACS.

Logování událostí

Systém HSR umožňuje nastavit různé úrovně logování událostí (varování, informace, chyba, kritická chyba). Tyto události jsou ukládány do paměti flash, nebo přeposílány na požadovanou IP adresu. V naší aplikaci je použita druhá varianta a všechny události se přeposílají na ACS (UDP port:514). Tento způsob zpracování je výhodný především při rozsáhlejší síti (více HSR), kdy zaručuje centralizované zpracování všech událostí sítě.

6.2 Konfigurace centrálního propoj. bodu (CCP)

Nastavení CCP pro aplikaci hotspotového systému pro více operátorů je patrné z obrázku 14.



Obrázek 14: Konfigurace portů CCP

6.3.2 Vzdálený přístup

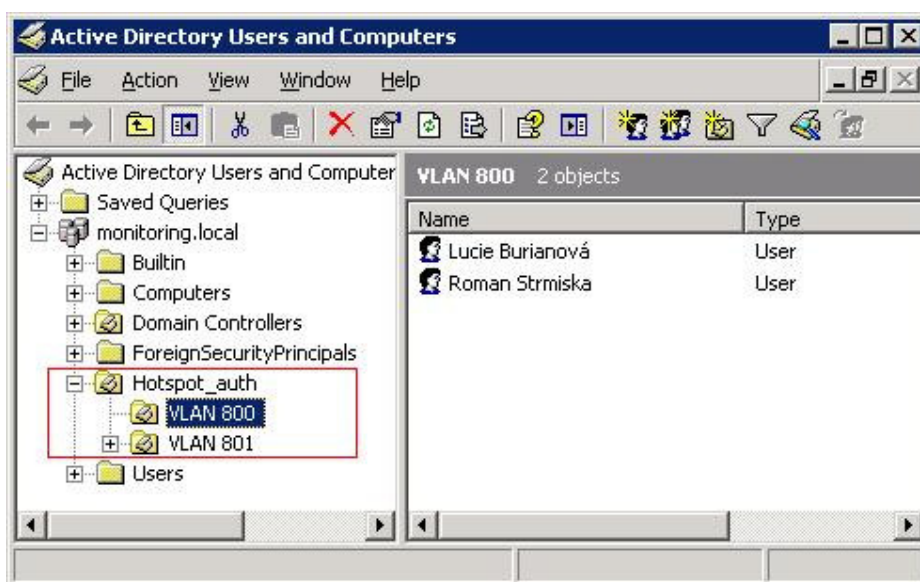
ACS bude provozován jako terminál bez klávesnice i monitoru. Přístup ke správě tohoto serveru bude realizován prostřednictvím vzdálené plochy. Je nutno nastavit systém podle obrázku 15. Tímto je povolen vzdálený přístup pouze členům skupiny **Administrators**.



Obrázek 15: Konfigurace vzdáleného přístupu

6.3.3 Role doménového kontroleru

ACS je nakonfigurován do role doménového kontroleru, který spravuje kompletní strukturu Active Directory (AD). AD je hierarchická struktura, spravuje fyzické i logické prvky sítě a umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. **Active Directory ukládá své informace a nastavení v centrální organizované databázi.** Tato databáze bude použita pro **správu koncových uživatelů**, kteří budou přistupovat k síťovým prostředkům HSR. Obrázek 16 demonstruje vytvoření dvou uživatelských účtů, kteří mají přístup k síťovým prostředkům Operátora 1. Každý z uživatelů má nastavené implicitní heslo a oprávnění pro přístup do systému.



Obrázek 16: Struktura Active Directory

ACS v roli doménového kontroleru funguje též jako zdroj hodin, jednotlivé HSR se s ním synchronizují prostřednictvím protokolu NTP. Tím je zaručena synchronizace času v celé struktuře HSR, což je nezbytná podmínka pro korektní logování událostí.

6.3.4 Mail server

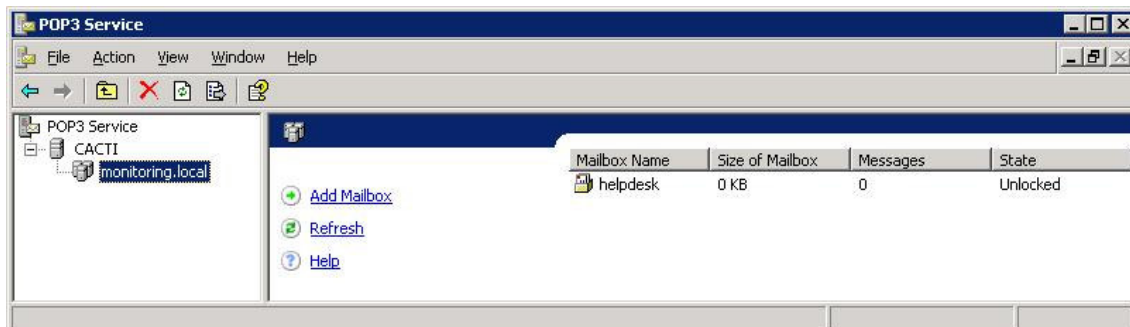
Služba pro přenos zpráv v elektronické podobě. Vhodná především pro automatizovanou notifikaci v případě problému na síti provozovatele HSR. Mail server pro svou činnost užívá následujících protokolů:

SMTP

Zajišťuje transfer elektronické zprávy od odesílatele do poštovní schránky příjemce (port TCP 25). Sslužeb SMTP mohou využívat pouze uživatelé AD.

POP3

Protokol pro stahování emailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení (port TCP 110). Nezabezpečená verze protokolu, data se přenáší v nešifrované podobě. Přístup ke vzdálenému serveru je podmíněn zadáním korektního přihlašovacího jména a hesla.

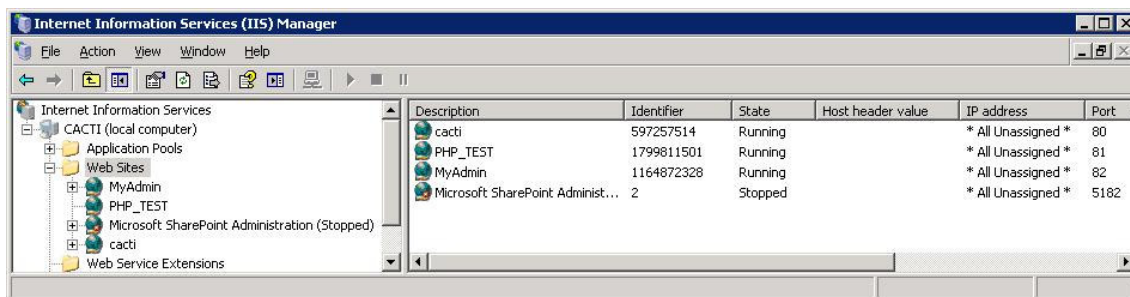


Obrázek 17: Vytvoření emailové schránky uživateli "helpdesk"

Pro automatizovanou notifikaci je vytvořen speciální účet v AD jménem „helpdesk“, kterému je přidělena poštovní schránka. Systém pak v případě vyhodnocení komplikací na síti automaticky generuje emailovou zprávu a prostřednictvím protokolu SMTP jej doručuje do schránky uživatele helpdesk. Uživatel helpdesk má na monitorovacím počítači nainstalovaného poštovního klienta (např. MS Outlook) a v pravidelných časových intervalech synchronizuje svého klienta s poštovní schránkou ACS. Synchronizaci zajišťuje protokol POP3.

6.3.5 Aplikační server (IIS)

Aplikační server IIS nabízí prostřednictvím distribuce Microsoft Windows Server 2003 integrovaný, spolehlivý, bezpečný a managementovatelný Web server. Lze jej provozovat na intranetu, případně internetu. Mezi další libovolně instalovatelné moduly patří FTP a NNT, které však pro aplikaci HSR nemají uplatnění.



Obrázek 18: Přehled webových stránek které spravuje IIS

Nejdůležitějšími položkami na obrázku 18 jsou: „Web Sites“ a „Web Service Extension“.

Web Sites

Zobrazuje stručný přehled provozovaných webových stránek, které lze z této pozice též spravovat. Pro každou stránku se konfiguruje oprávnění, provozní port, domovský adresář, IP adresa rozhraní, chybové hlášky a spousta dalších parametrů.

Přehled a význam aktivních Web Sites:

- cacti – správa účtovacího systému
- PHP-TEST – ověření funkčnosti PHP skriptovacího jazyku
- MyAdmin – správa MySQL databáze pro účtovací systém

Web Service Extension

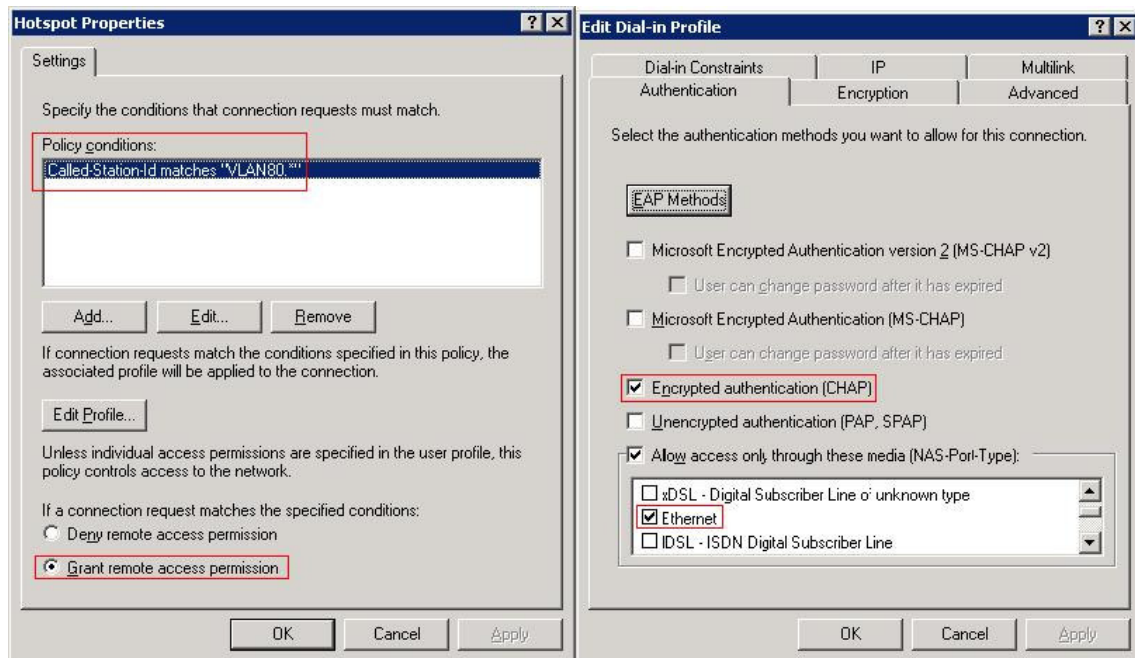
Přídavné rozšíření, umožňuje IIS podporu PHP, případně jiných modulů.

6.3.6 Autentizační servis (IAS)

Internet Autentization Service (IAS) představuje formu autentizačního serveru Radius, jehož úkolem je na základě stanovených politik přijmout autentizační požadavky od Radius klienta. V podstatě jde o ověření uživatelského jména a hesla, které zadává koncový uživatel přes webové rozhraní hotspotu. Uživatelské jméno i heslo se přenáší v šifrované formě a jejich validita se ověřuje porovnáním s účty AD. V případě shody je koncovým uživatelům povolen přístup do systému.

Rostup konfigurace IAS

1. Instalace služby IAS z přídavných komponent systému Windows server 2003.
2. Registrace služby v AD.
3. Definování Radius klientů, pro které bude IAS představovat autentizační server.
4. Logování serveru nastaveno do lokálního textového souboru.
5. Vytvořena politika koncových uživatelů.



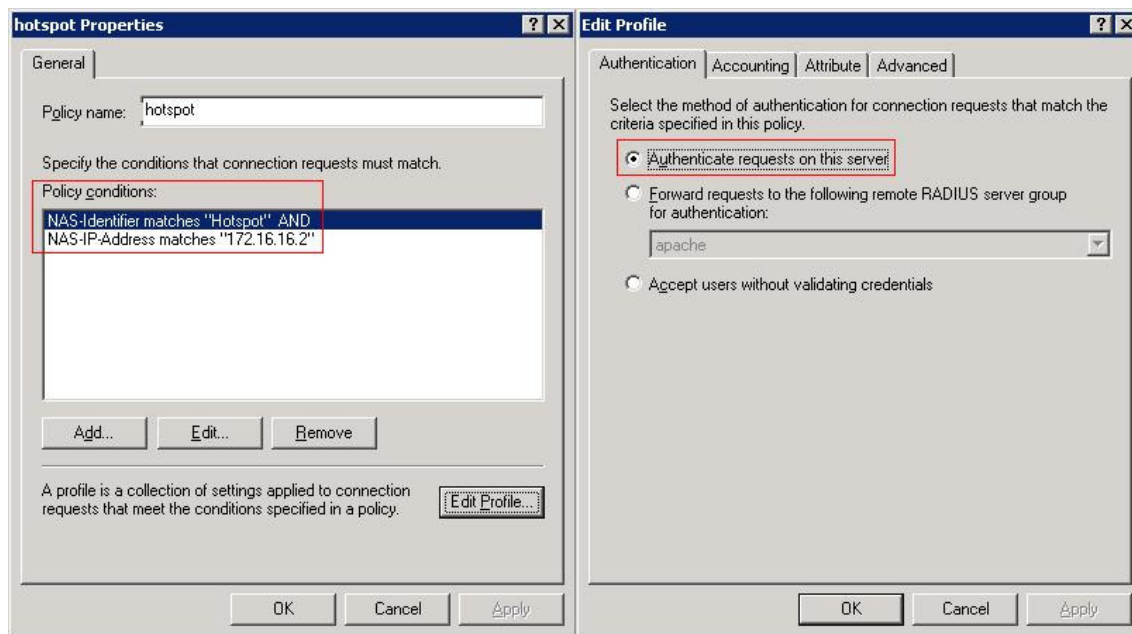
Obrázek 19: Politika koncových uživatelů

Požadavek **autentizace** bude zpracován pouze u klientů, kteří přistupují k hotspotu přes **ethernetové rozhaní VLAN 800 – VLAN 809**. Podmínkou je též **podpora šifrování „Challenge Handshake Authentication Protocol,, (CHAP)**.

CHAP

Protokol pro prokazování totožnosti při použití protokolu PPP. Jedná se o druh **symetrického šifrování** (server i klient sdílí stejný klíč).

6. Vytvořena politika Radius klientů

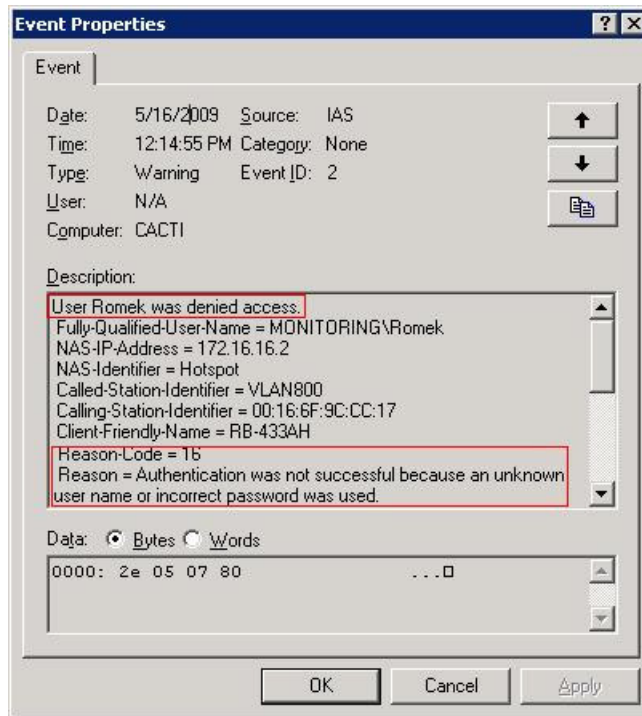


Obrázek 20: Politika Radius Klientů

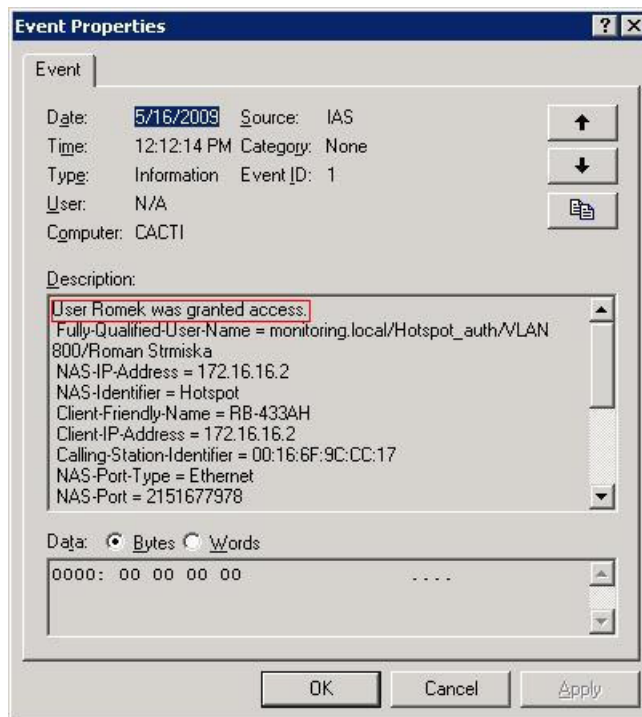
Z konfigurace na obrázku 20 vyplývá, že **server si řeší požadavky autentizace sám a komunikuje pouze s povolenými segmenty sítě**, které musí splňovat následující kritéria:

- IP adresa: 172.16.16.2
- Identifikátor: „Hotspot“

Nyní je systém připraven k provozu a jeho funkci lze sledovat v prohlížeči událostí systému windows. Prohlížeč událostí je vhodný nejen pro sledování provozu IAS, ale též pro prvotní implementaci politik a pro různé řešení problémů s IAS. Na obrázku 21 lze vidět příklad neúspěšné autentizace včetně důvodu selhání (chybné uživatelské jméno, nebo heslo).Obrázek 22 pak představuje pozitivní výsledek, kdy se přihlášení do systému zdařilo.



Obrázek 21: Úspěšná autentizace s IAS



Obrázek 22: Neúspěšná autentizace s IAS

6.3.7 Monitorování sítě HSR

Jako monitorovací systém byla použita volně distribuovaná aplikace „**The Dude**“, která je jednoduchá, přehledná, intuitivní a má v sobě integrovány všechny potřebné funkce.

The Dude je server/client aplikace s grafickým rozhraním, lze ji použít nejen pro monitorování, ale též pro správu jednotlivých prvků struktury. Jednotlivé prvky jsou navzájem propojeny a umístěny do samostatných grafických diagramů. Tímto získává systém i při složité topologii na přehlednosti. The Dude je schopen monitorovat jednotlivé služby běžící na sledovaných prvcích a upozorňovat obsluhu v případě jakékoliv změny jejich stavů. Umí též vyčítat statistiky, případně z hodnot generuje přímo grafy.

Dude server

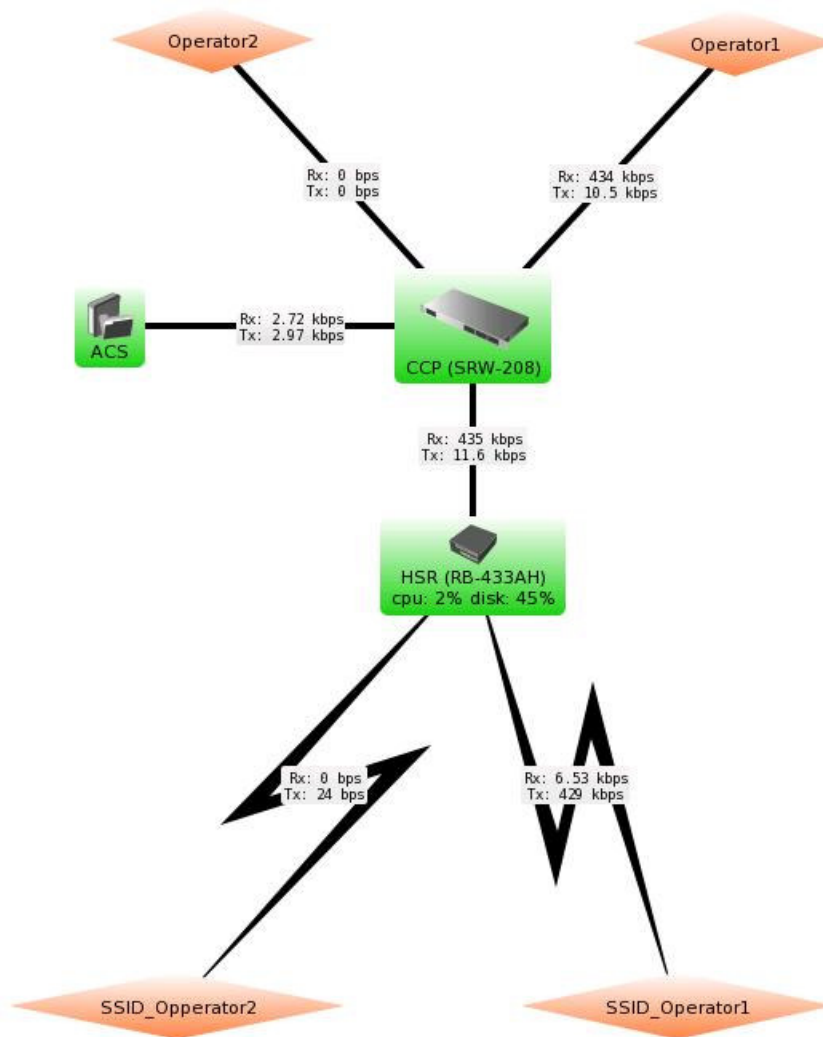
Program, který běží na pozadí. Nemá žádné grafické rozhraní a může být řízen pouze aplikací Dude klient. Server uchovává všechnu konfiguraci včetně grafů a lze jej nastavit pro automatizované spuštění při startu operačního systému.

Dude klient

Se připojuje k místnímu, nebo vzdálenému Dude serveru a je opatřen grafickým rozhraním. Všechny akce se spouštějí na serveru, při odpojení klienta nedochází ke ztrátě dat.

6.3.7.1 Návrh topologie

Topologie vychází z obrázku zapojení experimentálního pracoviště. Snahou je monitorovat pouze prvky, které souvisí s provozem sítě HSR. Vzhledem k umístění ACS a faktem, že pro management je vyhrazena VLANA 700, lze monitorovat pouze ACS, HSR, CCP a aktuální přenosovou rychlost jejich rozhraní. Obrázek 23 prezentuje monitorovanou topologii sítě. Pro jednoduchost je v topologii pouze jeden HSR, v případě expanze by se k CCP paprskovitě připojovali další prvky. Pro zobrazování aktuálních přenosových rychlostí a jiných statistik síťových prvků je využit protokol SNMP. Každý z těchto prvků má svůj profil (viz. kapitola 6.1.12). Aktuální hodnota přenosové rychlosti je součtem všech požadavků koncových klientů, kteří jsou například připojeni k logickému bezdrátovému rozhraní „SSID_Operator1“ a aktuálně využívají služeb „Operátora1“. Zelená barva ikon ACS, HSR a CCP indikuje, že všechny sledované služby jsou aktivní – dostupné.



Obrázek 23: Monitorovaná topologie sítě

6.3.7.2 Sledované služby

Aby monitorovací systém mohl pracovat správně, požaduje nastavení služeb, jejichž stav se bude v pravidelných intervalech sledovat. V první řadě budou nastaveny globální podmínky pro všechny služby a následně budou jednotlivé služby samostatně definovány.

Globální podmínky: Probe Interval = 30s
 Probe Timeout = 3s
 Probe Down Count = 5

POZN: Služby se budou testovat každých 30s, pokud bude některá ze služeb v pravidelném testovacím intervalu nedostupná déle než tři vteřiny, inkrementuje se čítač. Pokud čítač dosáhne hodnoty pět, služba se vyhodnotí jako nefunkční.

Sledované služby

Sledované služby se řadí do skupin, podle příslušnosti k danému síťovému prvku (obrázek 24). Pro sledování stavu služeb musíme nastavit: administrátorské oprávnění, síťový a port, na kterém služba pracuje.



Device	Type	Problem	
ACS - Device	dns	ok	
	http	ok	
	ping	ok	
	pop3	ok	
	radius	ok	
	smtp	ok	
CCP (SRW-208) - Device	ping	ok	
HSR (RB-433AH) - Device	cpu	ok	
	disk	ok	
	dns	ok	
	ping	ok	

Obrázek 24: Sledované služby

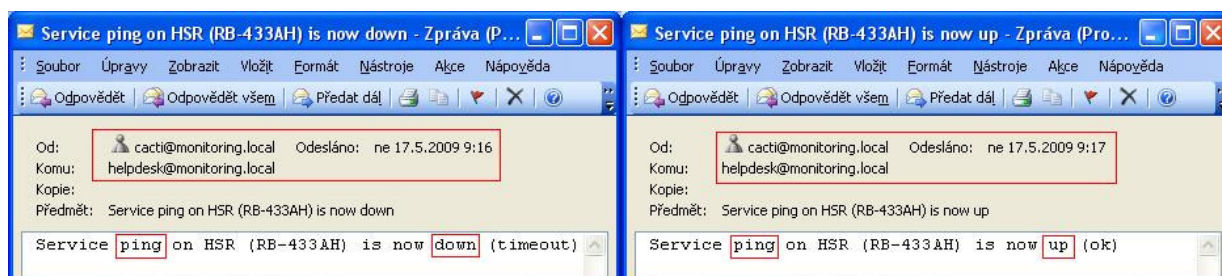
6.3.7.3 Notifikace

Notifikace je automatizovaný způsob upozornění obsluhy v případě nedostupnosti některé ze sledovaných služeb. Jedná se o velice zásadní věc, výrazně šetří čas, který by musel být využit k diagnostice vzniklého problému. Pro stávající systém budou využity dva druhy notifikace. Oba informují o vzniklém problému a následně o jeho odstranění.

- **Zaznamenání události do logu.**
- **Upozornění prostřednictvím emailu.**

POZN: Pro správnou funkci notifikace upozornění prostřednictvím emailu je nezbytné nastavit aplikaci **SMTP** server na adresu **localhost** a **odchozí emailovou adresu na: cacti@monitoring.local**.

Na následujícím obrázku je příklad emailové notifikace služby „ping“ síťového prvku HSR. Systém The Dude vygeneroval dva emaily (nahlášení poruchy, odstranění poruchy). Emaily byly doručeny uživateli helpdesk (doména monitoring.local) do jeho poštovní schránky. Uživatel Helpdesk následně provedl synchronizaci poštovní schránky se svým emailovým klientem MS Outlook.

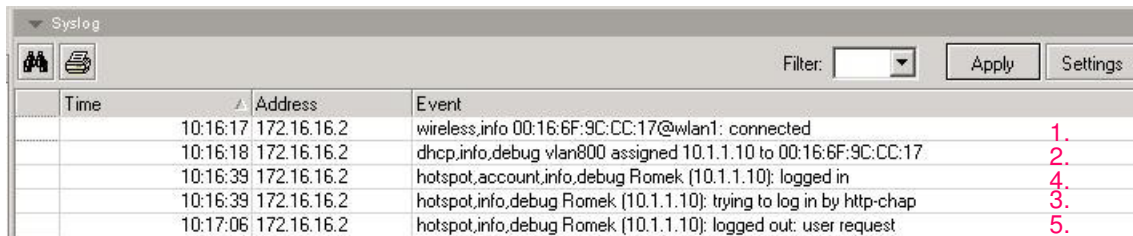


Obrázek 25: Emailová notifikace

6.3.7.4 Syslog

Služba s otevřeným TCP portem 514 slouží pro sběr systémových zpráv generovaných HSR. Pro využití této služby ji stačí pouze povolit v The Dude a nastavit rozsah adres, ze kterých bude syslog přijímat hlášení. Zpracovávají se informace od firewallu, bezdrátové karty, hotspotu atd.. Na následujícím obrázku je zachycen postup autentizace koncového uživatele do systému.

1. Připojení k bezdrátovému rozhraní.
2. Přiřazení IP adresy MAC adrese uživatele a navázání do VLAN 800.
3. Autentizace přes http-chap.
4. Úspěšné přihlášení uživatele „Romek“.
5. Uživatel „Romek“ se odhlásil.



Time	Address	Event	
10:16:17	172.16.16.2	wireless.info 00:16:6F:9C:CC:17@wlan1: connected	1.
10:16:18	172.16.16.2	dhcp.info,debug vlan800 assigned 10.1.1.10 to 00:16:6F:9C:CC:17	2.
10:16:39	172.16.16.2	hotspot,account.info,debug Romek (10.1.1.10): logged in	4.
10:16:39	172.16.16.2	hotspot.info,debug Romek (10.1.1.10): trying to log in by http-chap	3.
10:17:06	172.16.16.2	hotspot.info,debug Romek (10.1.1.10): logged out: user request	5.

Obrázek 26: Syslog

6.3.8 Účtování přenesených dat – aplikace Cacti

Pro sběr a uchovávání statistik uživatelských dat bude nasazen bezplatný nástroj „Cacti“, který funguje pod Linux/Unix i Windows. Cacti je velice univerzální, dovoluje nám širokou volnost při vytváření monitorování. Výstupem aplikace jsou přehledné grafy, které lze jednoduše zoomovat, nebo jinak zpracovávat. Sběr dat je založen na protokolu SNMP a celý systém je nadstavbou nad nástrojem RRDtool.

6.3.8.1 Instalace Cacti

Tento proces je poměrně složitý a je dostatečně popsán v manuálu, který je přiložen na DVD u diplomové práce (formát PDF). Tato kapitola bude zaměřena na význam jednotlivých instalovaných komponent. Cacti bude provozováno na ACS, který je vybaven operačním systémem Windows Server 2003. Proto i instalace bude tomuto systému přizpůsobena.

softwarové komponenty

- Webový server IIS
- PHP
- MySQL
- Cygwin
- NET-SNMP
- RRDtool
- Cacti

Webový server IIS

Již nainstalována komponenta (viz kapitola 6.3.5) a nastavena pro podporu skriptů PHP. IIS umožňuje správu MySQL databáze a aplikace Cacti prostřednictvím webového rozhraní.

PHP

PHP [5] je skriptovací programovací jazyk, určený především pro programování dynamických internetových stránek. Nejčastěji se začleňuje přímo do struktury jazyka HTML, XHTML či WML, což lze využít při tvorbě webových aplikací. PHP lze použít i k tvorbě konzolových a desktopových aplikací. PHP skripty jsou většinou prováděny na straně serveru, k uživateli je přenášěn až výsledek jejich činnosti. Interpret PHP skriptu je možné volat pomocí příkazové řádky. Syntaxe jazyka je inspirována několika programovacími jazyky (Perl, C, Pascal a Java). PHP je nezávislý na platformě, skripty fungují bez větších úprav na mnoha různých operačních systémech. PHP se stalo velmi oblíbeným především díky jednoduchosti použití a tomu, že kombinuje vlastnosti více programovacích jazyků a nechává tak vývojáři částečnou svobodu v syntaxi.

MySQL

Databázový server, spolupracuje s aplikací Cacti. Při instalaci MySQL byla použita aplikace „XAMPP“, která zjednodušila proces instalace do nejvyšší možné míry (průvodce instalací). Databázový server je pro jednoduchost spravován přes webové rozhraní nástrojem „phpMyAdmin“.

Cygwin

Volně šířitelná aplikace, koncentruje v sobě spoustu menších programů, jejich cílem je portování programů napsaných pro platformu Linux/Unix na Windows s minimem úprav. Hlavní částí aplikace Cygwin jsou knihovny (implementace Linuxových/Unixových systémových volání pomocí Win32), překladač, a programy unixových aplikací.

NET-SNMP

Softwaru pro využití vlastnosti SNMP protokolu (v1, v2c, v3). Podporuje protokoly IPv4, IPv6, IPX a AAL5. Obsahuje všeobecnou klientskou knihovnu, aplikace pro příkazovou řádku a rozšířeného SNMP agenta.

RRDtool

Nástroj pro ukládání a zobrazování dat získané protokolem SNMP. Data uložena tímto nástrojem mají stále konstantní velikosti. K zobrazení dat ve formě grafů slouží opět RRDtool s bohatou nabídkou možností.

Cacti

Řídící aplikace, pro svoji činnost využívá všech předešlých softwarových komponent. Aplikace přijímá příkazy přes webové rozhraní a předává je podřízeným komponentám.

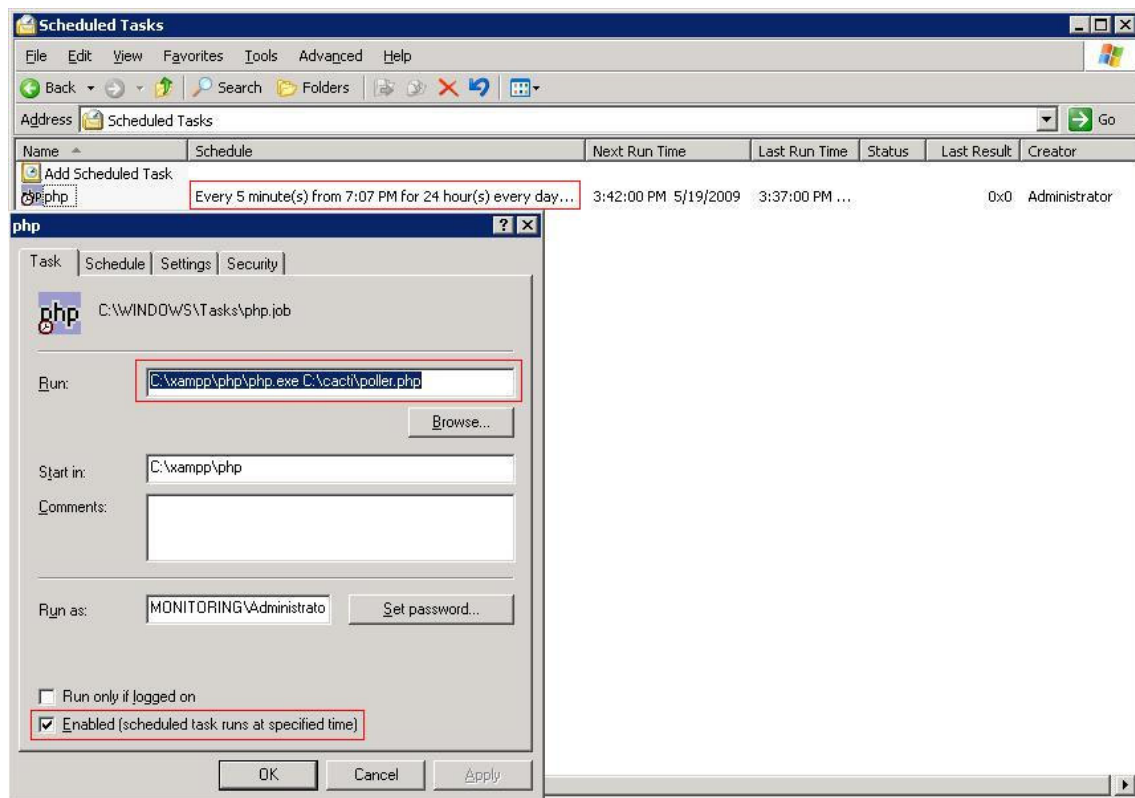
6.3.8.2 Princip funkce Cacti

Funkce jsou rozděleny do tří základních částí, každá z těchto částí využívá různé komponenty popsané v kapitole 6.3.8.1.

- Získání dat.
- Uložení dat.
- Prezentace dat.

Získání dat

Proces při kterém operační systém spouští v pravidelných časových intervalech tzv. „poller“. Jedná se o skript napsaný v aplikaci PHP, který protokolem SNMP snímá hodnoty čítačů HSR. Získaná data se následně předávají aplikaci Cacti.



Obrázek 27: Automatizované spuštění pooleru

Na obrázku 26 lze vidět automatizovaný proces operačního systému pro spuštění pooleru. Z konfigurace je patrné, že skript pooler.php se bude spouštět v pětiminutovém intervalu a pro jeho spuštění poslouží aplikace PHP.

Uložení dat

Proces při kterém Cacti přijímá data od pooleru a předává je komponentě RRDtool. RRDtool je zkratkou pro „Round Robin Database (RRD)“, což je systém pro ukládání a zobrazování dat v závislosti na čase. Data jsou ukládána ve velmi kompaktním formátu a velikost souboru zůstává stále konstantní. Při každé změně dat se modifikuje původní soubor, doplní se aktuální hodnoty a staré jsou zapomenuty. Tímto způsobem lze uchovávat data maximálního stáří jeden rok.

Prezentace dat

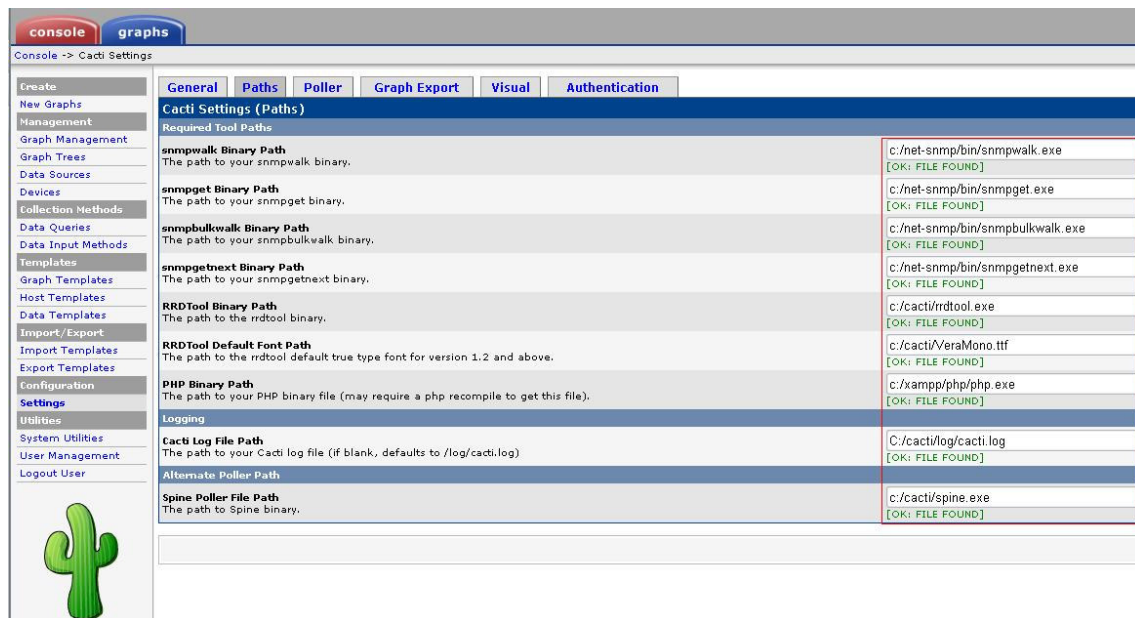
Prezentace dat v Cacti užívá RRDtool, který disponuje zabudovanými funkcemi pro tvorbu grafů. Kombinace grafů a podpory zobrazení ve webovém rozhraní umožňuje přístup k datům přes libovolný webový prohlížeč.

Některé funkce RRDtool pro účely prezentace dat:

- autoscail,
- normální/logaritmické zobrazení,
- zápis více veličin do jednoho grafu,
- volba barevného schéma grafu,
- tvorba legendy
- výpis nejmenší/průměrné/nejvyšší hodnoty ve sledovaném časovém úseku,
- atd.

6.3.8.3 Provozování Cacti

Systém pro účtování dat je nainstalován. Nyní zajistíme jeho spolupráci s komponenty, které jsou popsány v kapitole 6.3.8.1. V podstatě se jedná o nastavení cest ke spouštěcím souborům.



Path Name	Path Value	Status
snmpwalk Binary Path	c:/net-snmp/bin/snmpwalk.exe	[OK: FILE FOUND]
snmpget Binary Path	c:/net-snmp/bin/snmpget.exe	[OK: FILE FOUND]
snmpbulkwalk Binary Path	c:/net-snmp/bin/snmpbulkwalk.exe	[OK: FILE FOUND]
snmpgetnext Binary Path	c:/net-snmp/bin/snmpgetnext.exe	[OK: FILE FOUND]
RRDTool Binary Path	c:/cacti/rrdtool.exe	[OK: FILE FOUND]
RRDTool Default Font Path	c:/cacti/VeraMono.ttf	[OK: FILE FOUND]
PHP Binary Path	c:/xampp/php/php.exe	[OK: FILE FOUND]
Cacti Log File Path	C:/cacti/log/cacti.log	[OK: FILE FOUND]
Alternate Poller Path		
Spine Poller File Path	c:/cacti/spine.exe	[OK: FILE FOUND]

Obrázek 28: Konfigurace komponent – Cacti

Nesmíme též opomenout nastavit některý z fontů písma, kterým se bude vypisovat legenda grafů. V opačném případě by se nezobrazoval žádný text.

Sledované zařízení

Sledované zařízení je pro nás prvek, ze kterého chceme poolerem sbírat data a následně zpracovávat. V našem případě se jedná o prvek HSR. Konfigurace je znázorněna na obrázku 29. Funkčnost SNMP lze ověřit výpisem informací: „uptime“ , „ hostname“ (obr. 29 vlevo nahoře).

The screenshot shows the Cacti configuration page for a device named RB-433AH (172.16.16.2). The page is divided into several sections: System Information, Devices, Availability/Reachability Options, and SNMP Options. The System Information section shows the device's uptime as 808900 (0 days, 2 hours, 14 minutes) and its location as 'Kotspot'. The Devices section includes fields for Description, Hostname (172.16.16.2), and Host Template (Mikrotik). The Availability/Reachability Options section includes settings for Downed Device Detection (Ping and SNMP), Ping Method (ICMP Ping), Ping Timeout Value (400), and Ping Retry Count (1). The SNMP Options section includes settings for SNMP Version (Version 1), SNMP Community (RB-433AH), SNMP Port (161), SNMP Timeout (500), and Maximum OID's Per Get Request (10). A sidebar on the left contains navigation links for various Cacti functions, and a green cactus icon is visible at the bottom left of the sidebar.

Obrázek 29: Výběr zdroje dat - Cacti

Zdroj dat

Zdroj dat lze vygenerovat automaticky výběrem některé z dostupných šablon nebo ručně. Ruční metoda je podmíněna znalostí **identifikátoru sledovaného objektu (OID)**. Volím ruční metodu z důvodu vlastní customizace grafů. Vytvořím pro každý uživatelský účet několik zdrojů dat a následně je vykreslím v jednom grafu. OID lze získat prostřednictvím aplikace SNMP walk nebo přímo exportem z prvku HSR. Při vytváření jednotlivých zdrojů dat z OID je třeba rozeznávat, k jakému účelu bude hodnota sledovaného čítače použita. Například pro zobrazení aktuální přenosové rychlosti a celkového množství přenesených dat v daném směru použiji u obou zdrojů OID = bytes (viz obr. 30). Rozdíl je pouze v tom, že pro celkové množství přenesených dat bude použita kumulovaná hodnota čítače (stále se inkrementuje) a pro aktuální přenosovou rychlost jeho okamžitá hodnota.

```

Terminal
Flags: X - disabled, I - invalid
#  NAME      PARENT      PACKET-MARK  LIMIT-AT  MAX-LIMIT
0  Ondra_up   VLAN801_up  Ondra_up     0          0
1  Ondra_dw   VLAN801_dw  Ondra_dw     0          0
2  VLAN801_dw global-out   VLAN801_dw   0          0
3  VLAN801_up global-in    VLAN801_up   0          0
4  VLAN800_dw global-out   VLAN800_dw   0          0
5  VLAN800_up global-in    VLAN800_up   0          0
6  Roman_dw   VLAN800_dw  Roman_dw     0          0
7  Roman_up   VLAN800_up  Roman_up     0          0
8  Lucie_dw   VLAN800_dw  Lucie_dw     0          0
9  Lucie_up   VLAN800_up  Lucie_up     0          0
10 Franta_dw  VLAN801_dw  Franta_dw    0          0
11 Franta_up  VLAN801_up  Franta_up    0          0
[admin@Hotspot] /queue tree> print oid
Flags: X - disabled, I - invalid
0  name=.1.3.6.1.4.1.14988.1.1.2.2.1.2.16777225
   packet-mark=.1.3.6.1.4.1.14988.1.1.2.2.1.3.16777225
   bytes=.1.3.6.1.4.1.14988.1.1.2.2.1.5.16777225
   packets=.1.3.6.1.4.1.14988.1.1.2.2.1.6.16777225

1  name=.1.3.6.1.4.1.14988.1.1.2.2.1.2.16777227
   packet-mark=.1.3.6.1.4.1.14988.1.1.2.2.1.3.16777227
   bytes=.1.3.6.1.4.1.14988.1.1.2.2.1.5.16777227
   packets=.1.3.6.1.4.1.14988.1.1.2.2.1.6.16777227

```

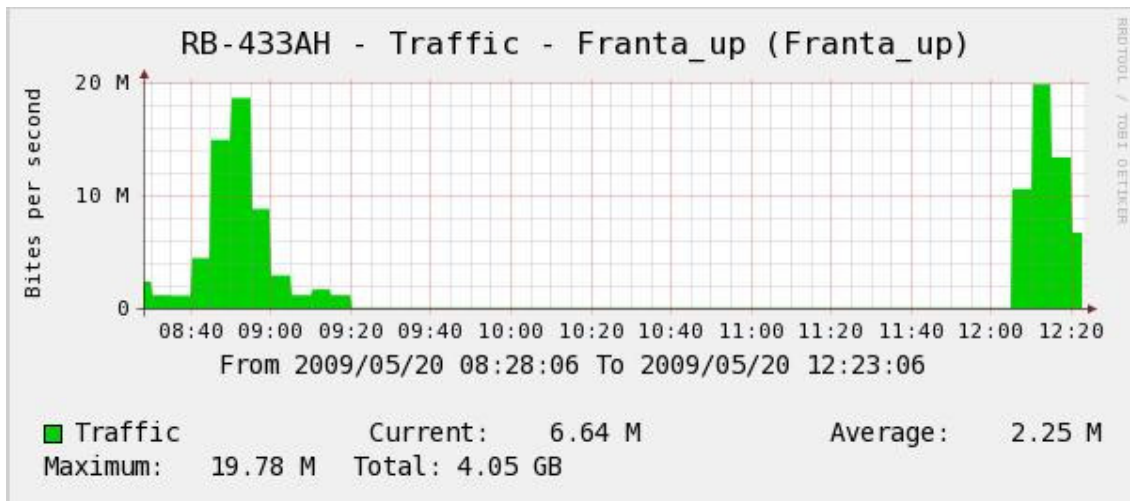
Obrázek 30: Objektový identifikátor (OID) uživatele Ondra - Cacti

Pomocná funkce CDEFs

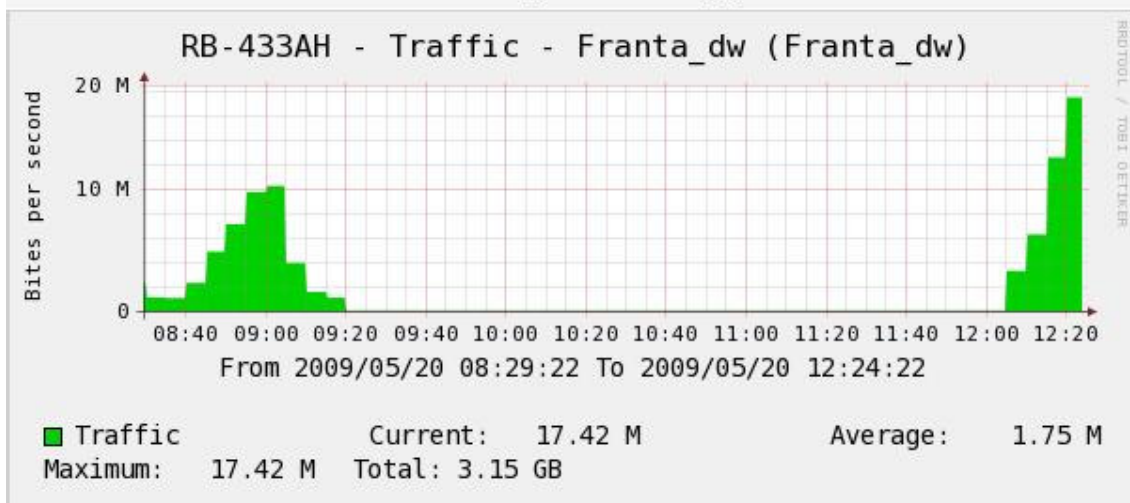
Uživatелеm definovaná funkce, lze ji použít pro konverzi datových jednotek zobrazovaných hodnot (převod z Bytů na bity), změnu měřítka, případně jiné modifikace.

Graf

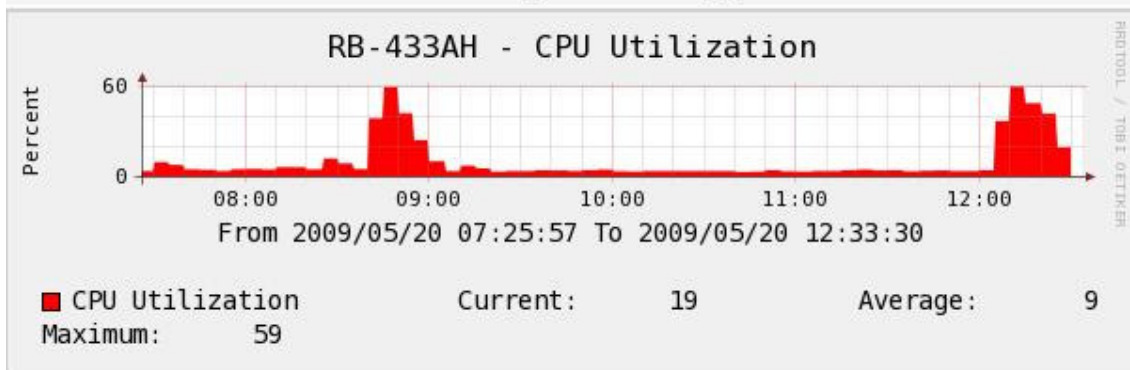
Graf tvoří výslednou reprezentaci sledované hodnoty. Je určen zdrojem dat, pomocnou funkcí CDEFs, popiskem, legendou, měřítkem atd. Obrázek 31 je příkladem vyúčtování uživatele Franta v libovolně zvoleném časovém intervale. Sledovanými veličinami jsou: prošlá data v daném směru, aktuální, průměrná a maximální přenosová rychlost. Zvolil jsem úmyslně krátký časový interval, aby byl patrný datový povoz. Při změně měřítka se všechny sledované veličiny přepočtou. Poslední graf znázorňující vyčízení CPU HSR. Tuto veličinu jsem zařadil spíše se zájmovostí.



Hourly (1 Minute Average)



Hourly (1 Minute Average)



Obrázek 31: Grafický výstup - Cacti

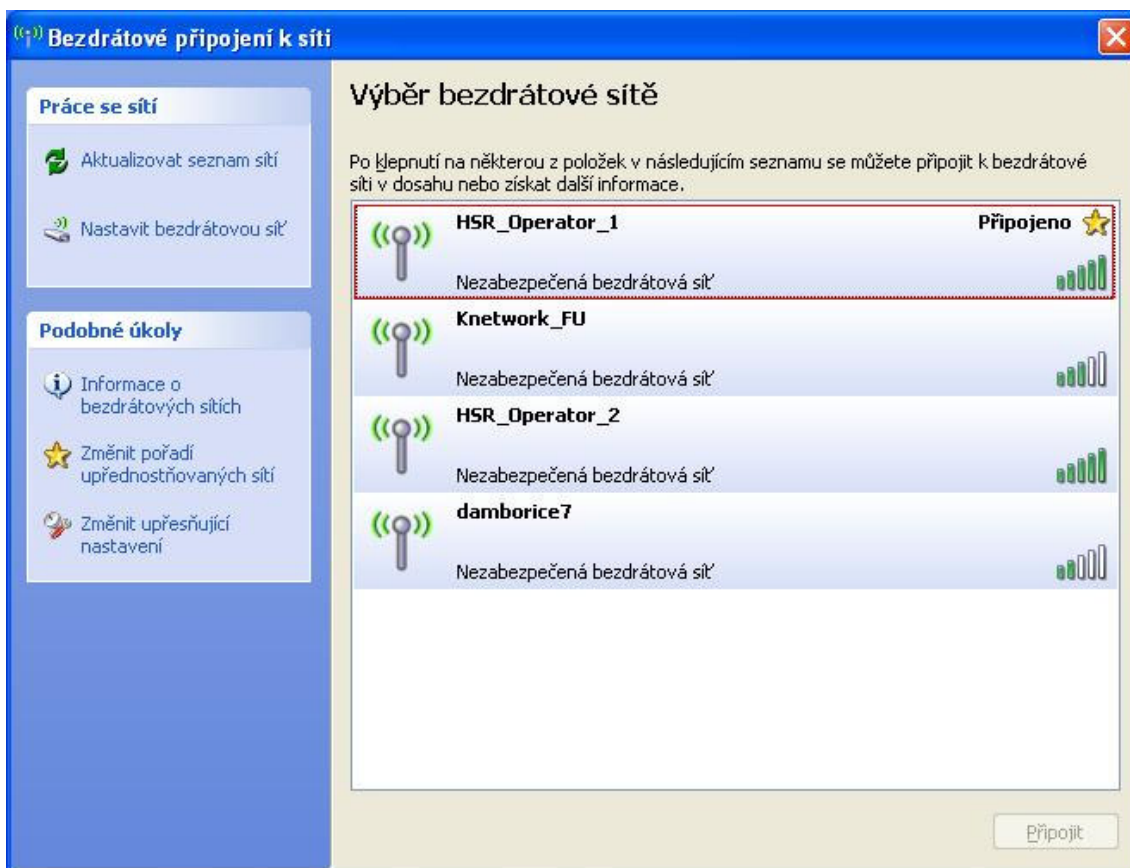
7. TESTOVÁNÍ EXPERIMENTÁLNÍ SÍTĚ

Testování experimentální sítě je zaměřeno na ověření základních funkcí systému, přenosovou rychlost a kvalitu služeb.

7.1 Ověření základních funkcí systému

V rámci tohoto testu je vytvořen popis připojení koncového uživatele k systému a případné stavy, které mohou nastat.

Koncový uživatel se nachází v oblasti pokryté radiovým signálem systému HSR. Jeho snahou je připojit se k síťovým prostředkům operátora jedna, u něhož má vytvořený uživatelský účet. Koncový uživatel tedy prohlíží radiové okolí a připojuje se k patřičnému operátorovi.



Obrázek 32: Prohledání radiového okolí

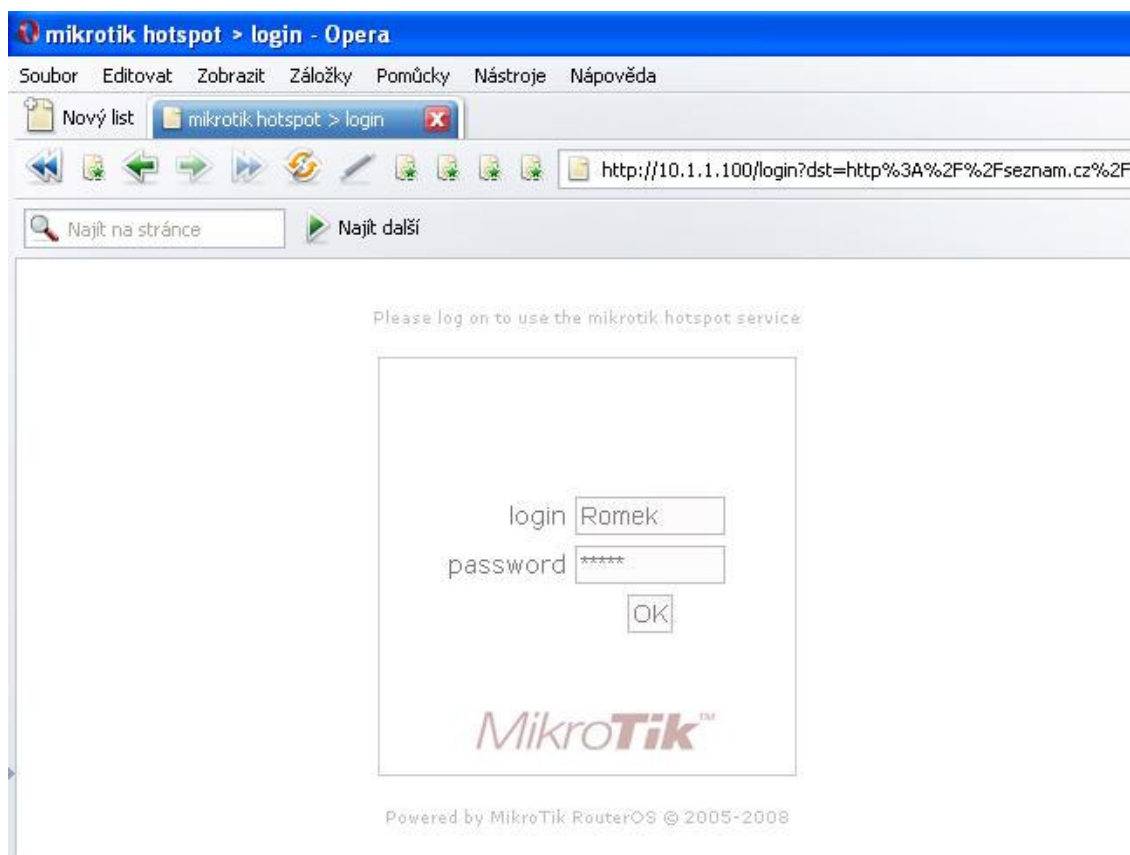
Po připojení je uživatelem generován požadavek přiřazení IP adresy. HSR reaguje prostřednictvím svého DHCP serveru a přiřadí koncovému uživateli některou z IP adres svého rozsahu.



Address	Active Address	Active MAC Address	Active Host Name	Expires After	Status
D	10.1.1.9	00:16:6F:9C:CC:17	speedy	23:49:52	bound

Obrázek 33: Přiřazení IP adresy koncovému uživateli

V tomto okamžiku jsou kombinací pravidel ve firewallu a NAT přeměrovány všechny požadavky komunikace na vstupní portál hotspotu. Následuje autentizace uživatele metodou „http CHAP“ proti Radius serveru ACS.



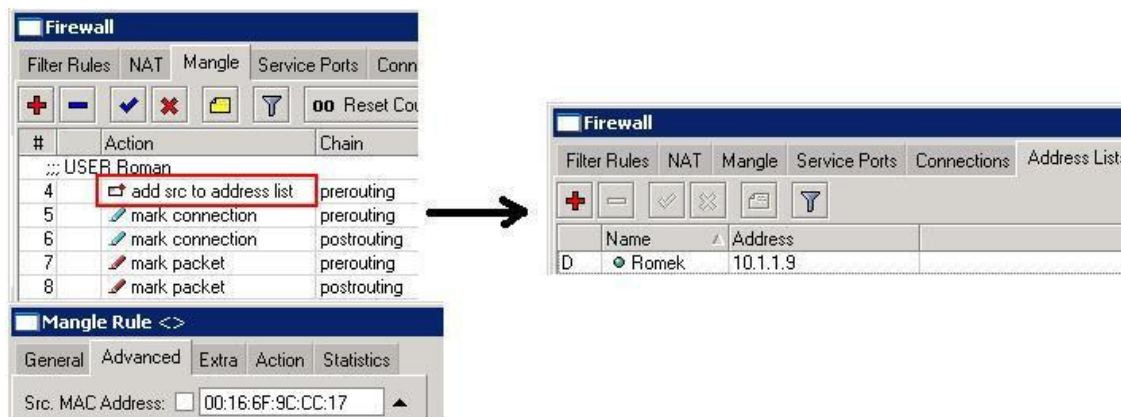
Obrázek 34: Vstupní portál hotspotu

Autentizace probíhá do té doby, než je zadána správná kombinace loginu a hesla. Pokud se uživateli podaří připojit do systému, vygeneruje se okno viz obrázek 35 s aktuálními informacemi uživatelské relace. Okno se automaticky obnovuje v intervalu jedné minuty. Uživatelské iniciály použité při úspěšné autentizaci se uloží do cookies s platností tří dnů. Tato funkce umožňuje opětovné připojení do systému bez nutnosti nové autentizace.



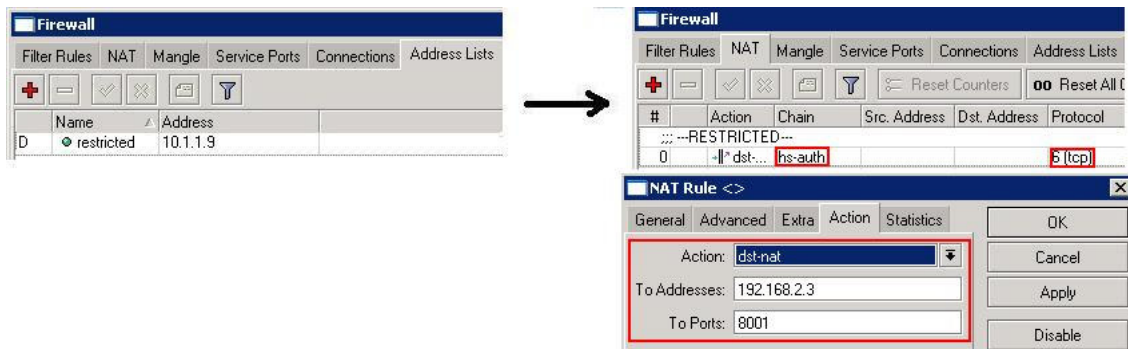
Obrázek 35: Informace o uživatelské relaci

Po úspěšném logování do systému nastává druhá fáze autentizace. HSR porovnává uživatelskou MAC adresu se seznamem povolených adres. V případě že se vyskytne shoda, HSR generuje dynamický zápis do firewallu, na jehož základě bude umožněn přístup koncového uživatele do systému. MAC adresa se porovnává i během komunikace v pravidelném časovém intervalu třiceti vteřin. Mechanismus zaručuje větší míru autentičnosti.



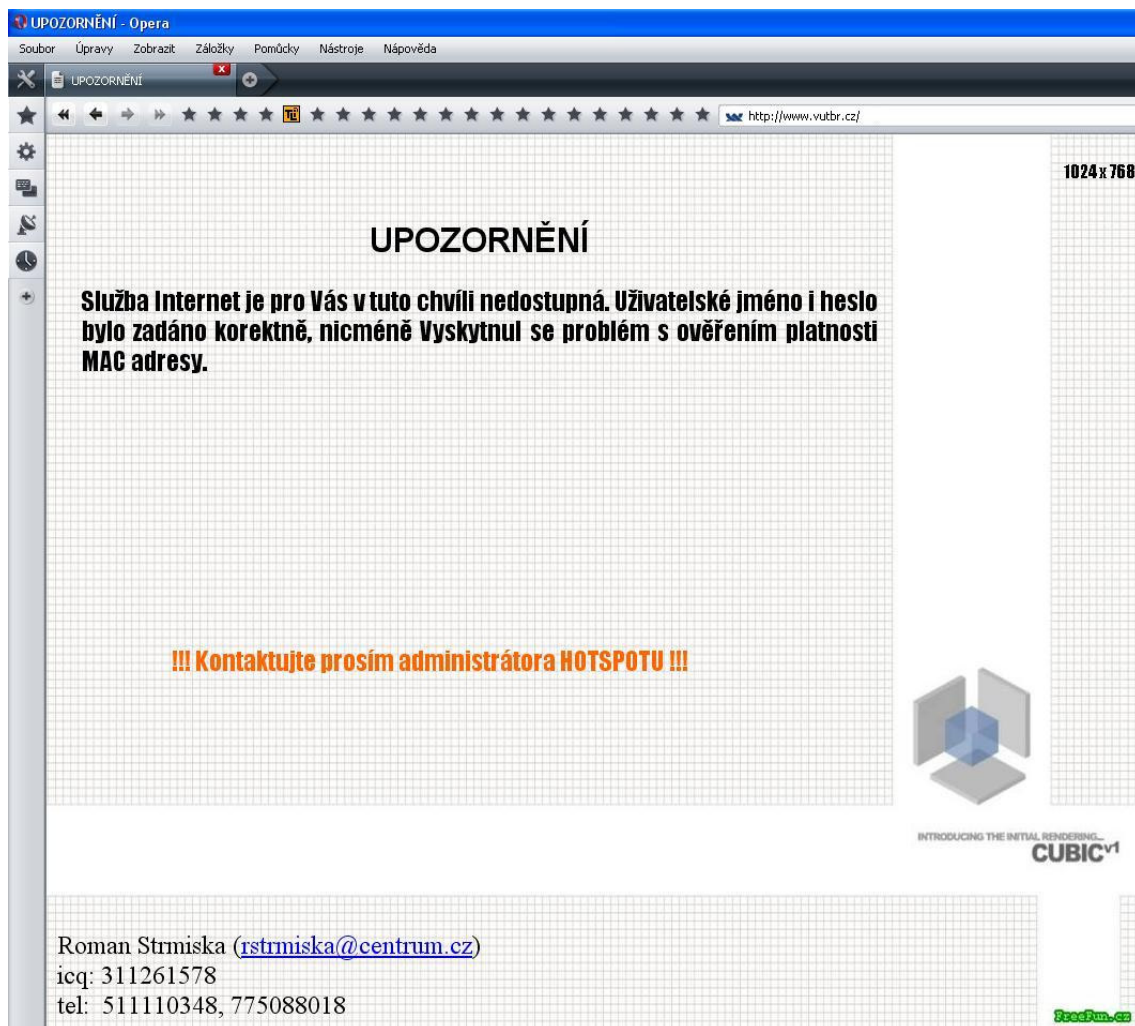
Obrázek 36: Úspěšná autentizace podle MAC

Na obrázku 36 lze vidět úspěšné porovnání MAC adres. Tuto funkci zajišťuje pravidlo číslo čtyři, ostatní pravidla pět až osm jsou pro označení spojení a paketů v obou směrech. Na tyto označené pakety se dále aplikuje QoS.



Obrázek 37: Neúspěšná autentizace podle MAC

Obrázek 37 znázorňuje případ, kdy uživatelská adresa neodpovídá žádnému záznamu povolených adres. Je vytvořeno dynamické pravidlo, které prostřednictvím firewallu a NAT směruje všechny uživatelské požadavky zobrazení webových stránek na informační portál.



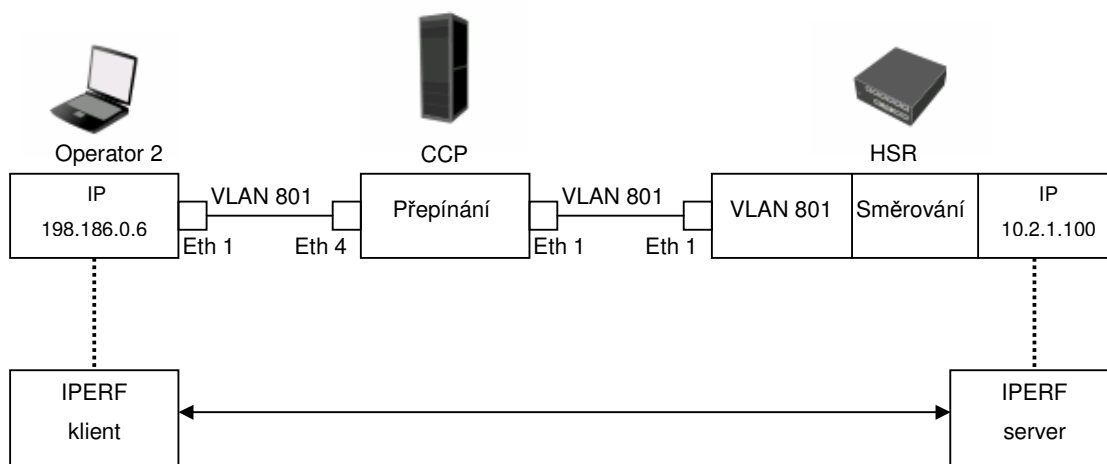
Obrázek 38: Informační portál

7.2 Přenosové možnosti hotspotového směrovače

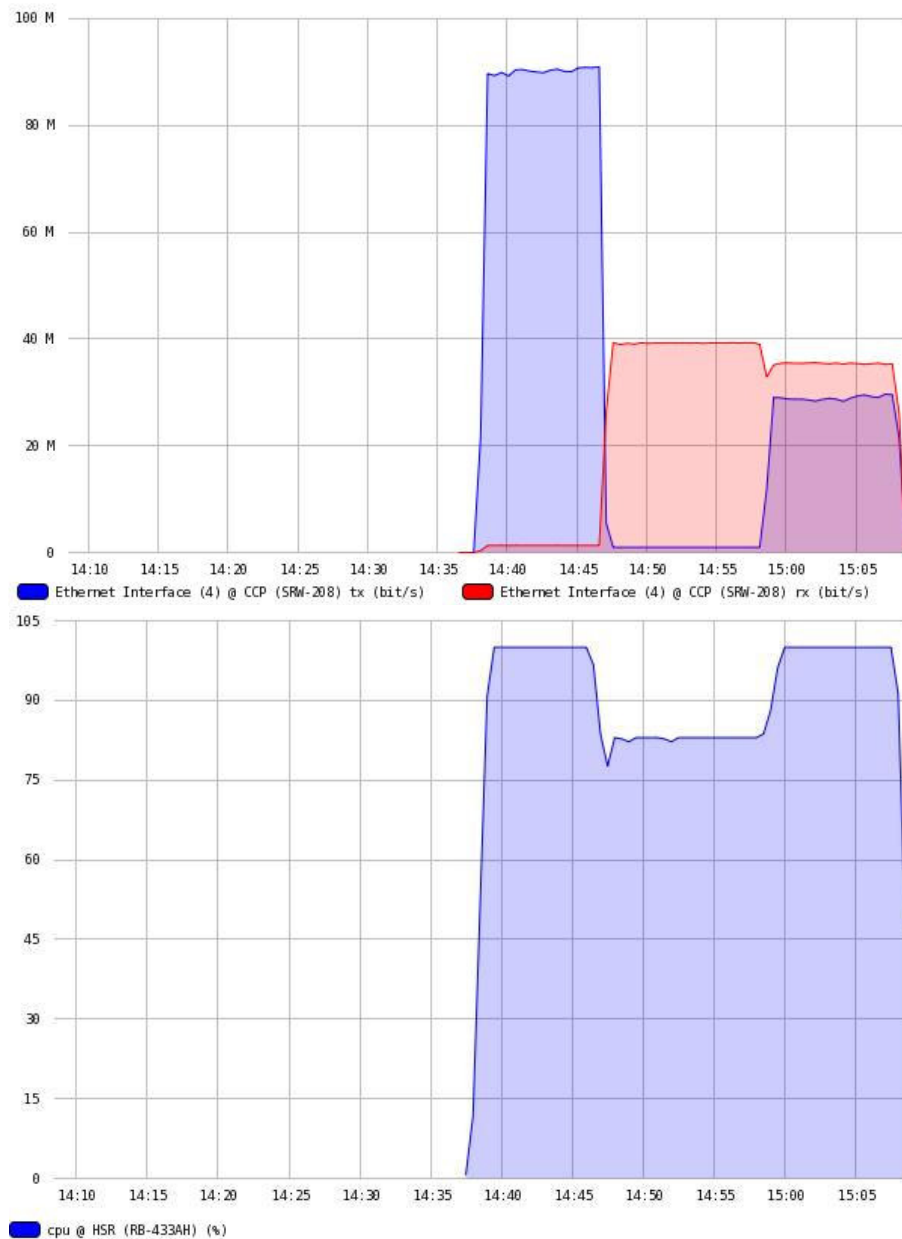
Cílem této podkapitoly je aplikace série testů, které prověří přenosové schopnosti HSR dané platformy. Sledovanými parametry jsou přenosová rychlost v obou směrech a vytížení CPU HSR. Testy jsou realizovány volně šiřitelnou server – klient aplikací IPERF. Tato aplikace je schopna generovat TCP i UDP datový tok, nastavovat různou délku paketu a počítat průměrnou přenosovou rychlost. Oba testy budou mít stejné podmínky, zaměřím se na testování provozu TCP s maximální délkou paketu rovnou 1500B. Generovaný TCP provoz je spojovaný s potvrzováním příchozích paketů, tudíž je náročnější na vytížení CPU směrovače. HSR je zapojen v módu směrovače a je povolena funkce sledování spojení. V zobrazovaných grafech je přenosová rychlost Tx i Rx vztažena k síťovému prvku HSR.

Měřící bod 1

Zapojení viz obrázek 39 proměřuje **přenosovou rychlost kabelové trasy bez bezdrátového rozhraní**. Byly realizovány tři měření, každé s intervalem deseti minut a jejich výsledky znázorňuje obrázek 40. První dva testy jsou zaměřeny na samostatné proměření Tx a Rx.. V posledním testu je generován oboustranný přenos (plně duplexní režim provozu). Z těchto testů vyplývá, že pro směr Rx, kdy vytížení CPU spadlo na pouhých cca 82%, je pravděpodobně problém v kabelové trase mezi CCP a Operátorem 2. **Pro plně duplexní režim provozování HSR je přenosová rychlost cca 28Mb/s**



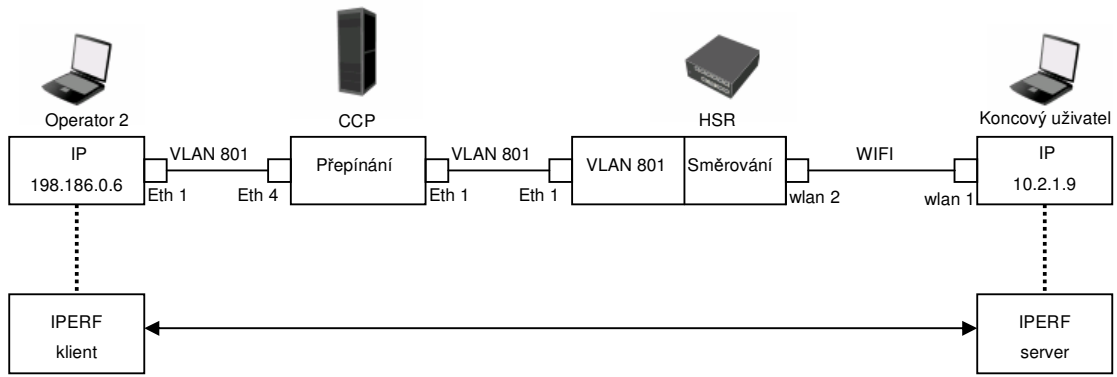
Obrázek 39: Měřící bod 1



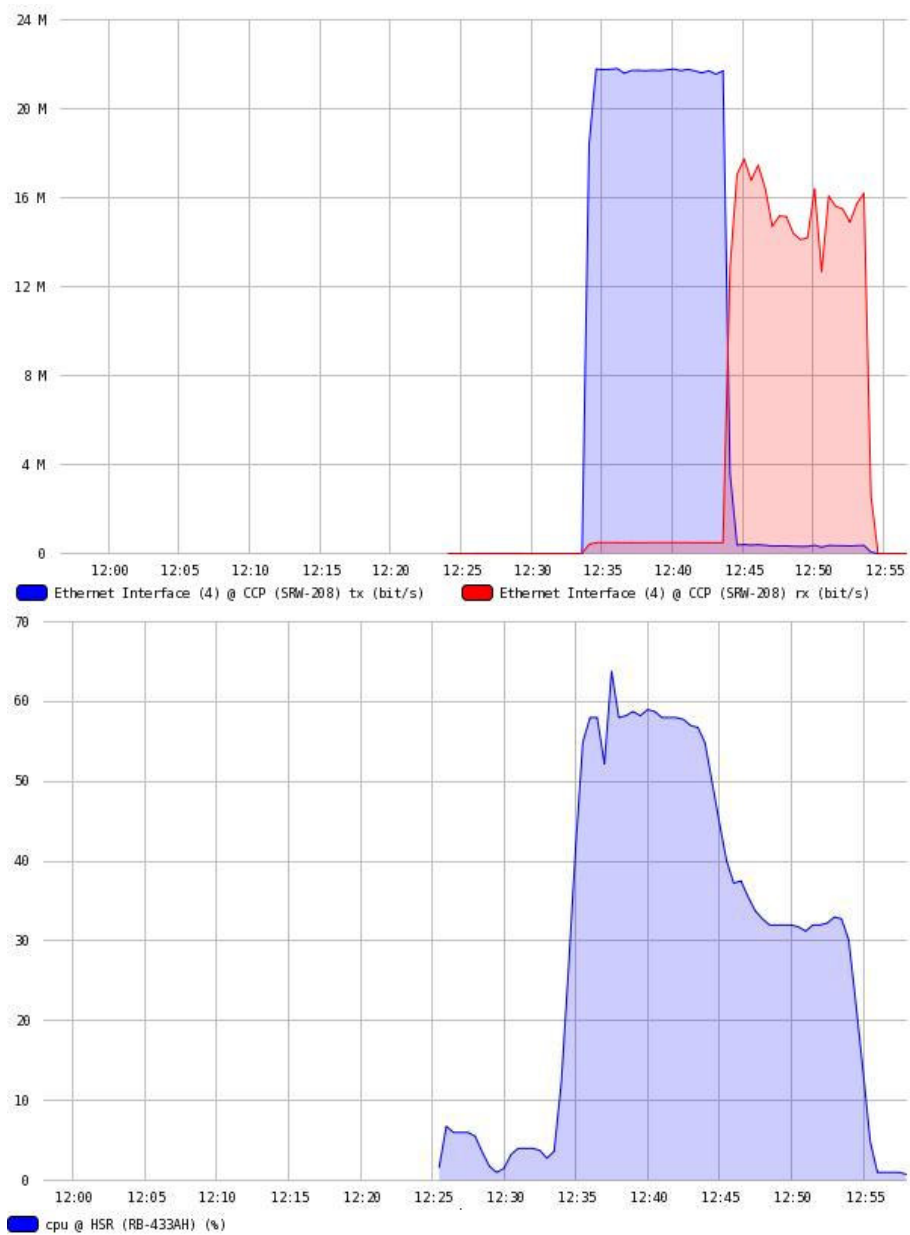
Obrázek 40: Přenosové rychlosti a vytížení CPU – Měřící bod 1

Měřící bod 2

Zapojení viz obrázek 41 proměřuje **přenosovou rychlost kabelové trasy včetně bezdrátového rozhraní**. Proběhly dva testy, každý s měřícím intervalem deseti minut. Jednotlivé průběhy měření jsou zachyceny na obrázku 42. Během měření se dosáhlo následujících průměrných hodnot : **tx = 20,8 Mb/s**, **rx = 15,2 Mb/s**. Směr rx je opět z nějakého důvodu degradován. Na vině může být například rozdílný chipset bezdrátových karet HSR (Atheros) a karty koncového klienta (Intel).



Obrázek 41: Měřící bod 2



Obrázek 42: Přenosové rychlosti a vytížení CPU – Měřící bod 2

7.3 Kvalita služeb (QoS)

Závěrečný test pro ověření funkčnosti QoS je podmíněn vhodně nastavenou rodičovskou větví VLAN 801, pod kterou jsou začleněni testovaní uživatelé. Test z důvodu přehlednosti grafu bude realizován pouze ve směru upload vůči koncovým uživatelům. Vychází se z poznatků získaných v kapitole 7.2 a parametry CIR a MIR jsou nastaveny následujícím způsobem:

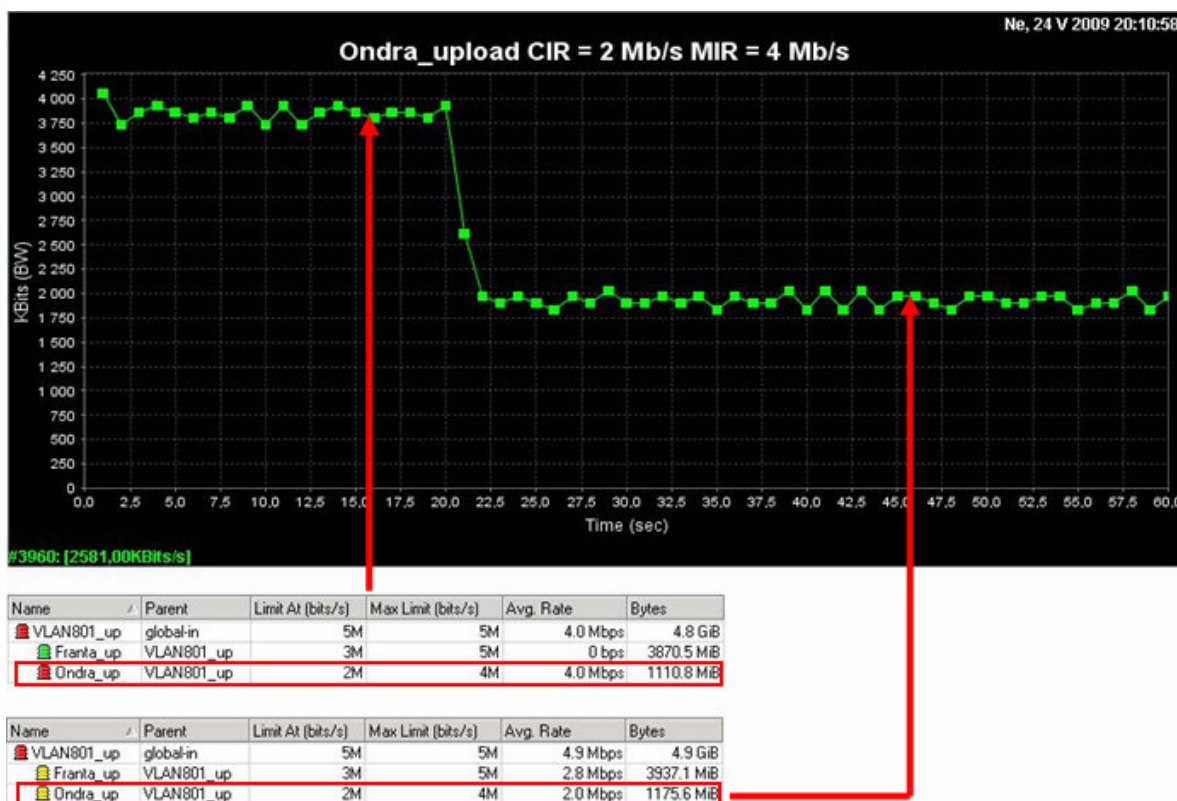
Směr od uživatele = upload

VLAN801_dw CIR = 5 Mb/s MIR = 5 Mb/s priority = 2

Franta CIR = 3 Mb/s MIR = 5 Mb/s priority = 3

Ondra CIR = 2 Mb/s MIR = 4 Mb/s priority = 3

Rodičovská větev VLAN801 je schválně poddimenzována, aby byla schopna zadanou šířku pásma bezpečně transformovat až ke koncovým klientům.



Obrázek 43: Test funkčnosti QoS

Princip činnosti QoS je patrný z obrázku 43. Uživatel Ondra, který je připojen k Operátorovi 2 (VLAN 801) čerpá jeho konektivitu přenosovou rychlostí MIR. Přesně po dvaceti vteřinovém intervalu s k Operátorovi 2 připojuje také uživatel Franta. Oba uživatelé mají stejnou prioritu a proto se jejich přenosová rychlost rozdělí tak, aby pokryla požadavky stanovené garantovanou šířkou pásma CIR. Z toho důvodu klesne v časovém intervalu (20;60> vteřin přenosová rychlost uživateli Ondra na stanovenou hodnotu CIR. Vytížení CPU se během tohoto testu pohybovalo kolem osmi procent.

8. ZÁVĚR

Cílem diplomové práce bylo komplexní popsání problematiky hotspotových systémů určených pro provoz více operátorů a na základě získaných zkušeností vybudovat vlastní experimentální síť, která řeší problematiku autentizace, přidělování kvality služeb a účtování přenesených dat.

Práci jsem rozdělil do několika témat.

V první části věnované plánování hotspotové sítě se zaměřuji na problematiku hledání vhodné lokality, volbu kmitočtového pásma a stanovení podmínek, které musí být při provozování sítě splněny.

Druhá část je věnována standardům IEEE 802.11. V rámci této kapitoly vybírám z mého pohledu nejvhodnější standard, věnuji se možnosti zabezpečení bezdrátové sítě a specifikuji faktory, které nejvíce ovlivňují parametry bezdrátového spoje.

Třetí část je samostatná kapitola věnovaná legislativě spojené s provozováním hotspotové sítě. Nastínil jsem dvě možnosti provozování hotspotové sítě (bez nároku na zisk, s nárokem na zisk).

Ve čtvrté části se zaměřuji na vlastní návrh koncepce hotspotového systému, který by splňoval podmínky zadání práce. Prezentuji fyzickou i logickou topologii a popisuji jednotlivé funkce, které realizují specifikované body zadání.

Pátá část je přípravou k realizaci vlastní experimentální sítě, rozhoduje o volbě vhodného hardwarového a softwarového vybavení dílčích prvků sítě. Jednotlivá rozhodnutí v rámci výběru hardwaru jsou s ohledem na poměr cena / výkon.

Šestá část se zabývá vlastní realizací experimentální sítě. Základní zapojení vychází z teoretických předloh, je však mírně modifikované z důvodu úspory hardwaru a implementace do stávající funkční infrastruktury. Podrobně je popsána konfigurace jednotlivých prvků sítě a vysvětlen její význam v praxi.

V závěrečné sedmé kapitole se věnuji testování experimentální sítě. Testy jsou koncipovány na základní ověření funkčnosti systému, proměření přenosových možností hotspotového směrovače (pro danou hardwarovou konfiguraci) a ověření funkčnosti mechanismu přidělování požadované šířky pásma.

Prakticky se mi podařilo splnit všechny body zadání a navíc jsem implementoval dohledový systém kompletní infrastruktury hotspotového systému. Při testech propustnosti a kvality služeb jsem narazil na problém s kompatibilitou některých bezdrátových karet, tudíž byly závěrečné testy provedeny pouze pro menší přenosové rychlosti. V tomto módu testování jsem dosáhnul velice pozitivních výsledků. Systém se mi jeví v praxi jako velice stabilní a reálně využitelný. Vylepšení systému nasazením výkonnějšího hardwaru by nám přineslo větší přenosové rychlosti. Za významnější vylepšení bych však považoval využití skriptovacích jazyků hotspotových směrovačů. Při složitější topologii sítě hotspotů (více HSR) by bylo velice neefektivní do každého směrovače konfigurovat QoS pro jednotlivé uživatele ručně. Ideálním způsobem je vytvoření skriptu, který na základě změně vstupních

proměnných (jméno uživatele, MAC adresa, přenosové rychlosti CIR a MIR) generuje potřebná pravidla sám. Takto vytvořený skript by se přes dávkový soubor za pomoci aplikace Putty přenesl z ACS na jednotlivé hotspotové směrovače a ve vybraný časový interval se spustil. Možností vylepšení systému je opravdu široká škála, jedná se však o časově náročné řešení.

9. SEZNAM POUŽITÝCH ZDROJŮ

- [1] Shelly, B. *Wi-Fi – Postavte si svou vlastní wi-fi síť*. Neocortex, Praha, 2004
- [2] *VO_R_12_08_2005_34*. Dostupné na WWW: < <http://www.ctu.cz> >
- [3] *Oznámení telekomunikační činnosti*. Dostupné na WWW: < <http://www.ctu.cz> >
- [4] *Standardy Wi-Fi*. Dostupné na WWW: < <http://cs.wikipedia.org/wiki/802.11>>
- [5] *PHP*. Dostupné na WWW: < <http://cs.wikipedia.org/wiki/PHP>>

10. SEZNAM POUŽITÝCH ZKRATEK

Wireless Local Area Network – WLAN
Český telekomunikační úřadu – ČTÚ
Institut inženýrů elektrotechniky a elektroniky – IEEE
Local Area Network – LAN
Přístupový bod – AP
Service Set Identifier – SSID
Wired Equivalent Privacy – WEP
Wi-Fi Protecte Access – WPA
Virtual Access Point – VAP
Virtual Local Area Network – VLAN
Přístupový řídicí server – ACS
Hotspotový směrovač – HSR
Centrální propojovací bod – CCP
Transportní síť – TN
Přístupová síť – AN
Kvalita služeb – QoS
Napájení po ethernetu - POE
Poměr stojatých vln – PSV
Random Early Detection – RED
Active Directory – AD
Aplikační server – IIS
Autentizační server – IAS
Challenge Handshake Authentication Protocol – CHAP
Round Robin Database – RRD
Identifikátoru sledovaného objektu – OID
Centrální procesorová jednotka – CPU