

Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

WiFi Hotspot systémy
(WiFi Hotspot systém na platformě Mikrotik)
Diplomová práce

Autor: Jiří Líbal

Studijní obor: Informační management, IM5

Vedoucí práce: Ing. Vladimír Soběslav, Ph.D.

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 10. prosince 2014

Jiří Líbal

Poděkování

Rád bych poděkoval vedoucímu mé práce, Ing. Vladimíru Soběslavovi, Ph.D., za jeho ochotu, čas a cenné připomínky, které mi napomohly při vypracování této diplomové práce.

Anotace

Předmětem této diplomové práce je představení a porovnání WiFi Hotspotu na několika platformách včetně implementace na platformu Mikrotik s využitím několika RADIUS serverů. Práce zahrnuje jak nutnou teorii k obeznámení s danou problematikou, tak praktickou ukázkou implementace na dvou reálných projektech bezdrátového Hotspotu.

V teoretické části je probrána zejména problematika protokolu 802.11, zabezpečení WiFi sítí, AAA protokol, kvalita služeb (QoS), problematika Hotspotu a základní obeznámení s platformou Mikrotik. V souvislosti s nasazením Hotspotu je představena také platforma Cisco a Linux. Následuje porovnání výhod a nevýhod řešení Hotspotu na jednotlivých platformách a návrh řešení na nasazení platební brány. V praktické části jsou tyto poznatky a znalosti aplikovány na reálné projekty WiFi Hotspotu provozovaného na platformě Mikrotik. Současně bylo také otestováno a porovnáno několik variant RADIUS serverů, které byly nakonfigurovány pro spolupráci s Mikrotik platformou. Práce je určena svým obsahem zejména čtenářům se základními znalostmi problematiky počítačových sítí.

Annotation

Title: WiFi Hotspot systems

The subject of this Diploma Thesis is introduction and comparison of WiFi Hotspot system on multiple platforms including implementation on Mikrotik platform with use of several RADIUS servers. The paper subsumes theoretical knowledge which is necessary for understanding of this issue also practical demonstration of implementation on real projects of wireless Hotspot.

In theoretical part of this paper is discussed issue of 802.11 protocol, security of WiFi networks, AAA protocol, Quality of Service (QoS), Hotspot issue and basic overview of Mikrotik platform. In connection with Hotspot issue there were also introduced Cisco and Linux platform. Afterwards there were compared advantages and disadvantages of deployment WiFi Hotspot on Mikrotik platform, CISCO and Linux platform and discussed solution design of payment gateway. In practical part is this knowledge applied on real projects of WiFi Hotspot operated on Mikrotik platform. At the same time there were tested and compared more variants of RADIUS servers which were configured to cooperate with Mikrotik platform. The work itself is intended for the reader who is familiar with basic issue of computer networking knowledge.

Obsah

1	Úvod.....	1
2	Bezdrátové technologie pro Hotspot.....	6
2.1	Standard IEEE 802.11	6
2.1.1	IEEE 802.11b.....	8
2.1.2	IEEE 802.11g.....	8
2.1.3	IEEE 802.11a	9
2.1.4	IEEE 802.11n.....	9
2.1.5	IEEE 802.11ac.....	11
2.1.6	IEEE 802.11ad.....	12
2.2	Přenosové parametry.....	13
2.2.1	Koncové zpoždění.....	14
2.2.2	Kolísání zpoždění.....	14
2.2.3	Ztrátovost paketů	15
2.2.4	Šířka pásma.....	15
2.3	Režimy komunikace.....	16
2.3.1	DCF	16
2.3.2	PCF.....	18
2.3.3	EDCF	18
2.3.4	HCF.....	19
3	Brána pro připojení k Internetu - Hotspot.....	21
3.1	Popis Hotspotu.....	21
3.2	Funkce Hotspotu	22
3.3	Typy řízení Hotspotu.....	24
3.3.1	Samostatně spravované AP	24
3.3.2	Centrálně řízený Hotspot.....	24
3.4	Zabezpečení Hotspotu	26

3.4.1	Šifrování přenosu	27
3.4.1.1	WEP	27
3.4.1.2	WPA.....	28
3.4.1.3	WPA2 – 802.11i	29
3.4.2	AAA protokol.....	29
3.4.2.1	Autentizace.....	31
3.4.2.1.1	Otevřený systém (Open system)	31
3.4.2.1.2	802.1x.....	32
3.4.2.2	Autorizace.....	34
3.4.2.3	Účtování.....	34
3.4.3	Další možnosti zvýšení zabezpečení	35
3.4.3.1	MAC autentizace.....	35
3.4.3.2	Skrytí SSID	36
3.4.3.3	Deaktivace DHCP.....	36
3.5	Kvalita služeb - QoS.....	37
3.5.1	Parametry využívané kvalitou služeb.....	38
3.5.2	Standard IEEE 802.11e.....	38
3.5.3	Základní architektury QoS	39
3.5.3.1	Best-effort services	39
3.5.3.2	Integrated services.....	40
3.5.3.3	Differentiated services.....	40
3.6	Platforma Mikrotik.....	40
3.6.1	Obecné představení RouterBOARDů	41
3.6.1.1	Mini PCI WiFi karty	42
3.6.2	Operační systém RouterOS	44
3.6.2.1	Management RouterOS.....	45
3.6.2.1.1	WinBox	46

3.6.3	Centrálně kontrolované přístupové body - CAPsMAN.....	48
3.7	Další platformy	49
3.7.1	Platforma Cisco.....	49
3.7.1.1	Cisco IOS	50
3.7.1.2	Cisco WLC.....	51
3.7.1.2.1	Benefity Cisco WLC.....	51
3.7.2	Platforma Linux.....	54
3.7.2.1	GRASE Hotspot.....	55
3.7.2.1.1	Rozhraní a funkcionalita GRASE Hotspotu.....	56
3.8	Porovnání platforem	58
3.9	Návrh platební brány	62
3.9.1	Typy platebních bran	62
3.9.1.1	Elektronická peněženka	62
3.9.1.2	Online platební karta.....	63
3.9.1.3	SMS platby	63
3.9.2	Návrh na implementaci 1	64
3.9.3	Návrh na implementaci 2	65
3.9.4	Návrh na implementaci 3	67
4	Realizace Hotspotu na platformě Mikrotik	68
4.1	Návrh sítí.....	68
4.2	Použitý hardware	71
4.2.1	RouterBOARD	71
4.2.2	MiniPCI WiFi karty.....	74
4.2.3	Server PC.....	75
4.3	Hotspot v RouterOS	75
4.3.1	Hotspotové řešení 1 - restaurace	75
4.3.1.1	User Manager.....	78

4.3.1.1.1	User Manager – Vouchery	81
4.3.2	Hotspotové řešení 2 – Poskytovatel Internetu.....	82
4.3.2.1	Windows Server RADIUS a Active directory	88
4.3.2.1.1	Konfigurace Windows 2003 Serveru.....	88
4.4	TekRadius server	91
4.5	Porovnání RADIUS serverů.....	93
4.6	Testování Hotspotu.....	94
4.6.1	Test infrastruktury pro restauraci.....	94
4.6.2	Test infrastruktury pro poskytovatele Internetu	96
4.7	Problémy a jejich řešení.....	101
4.7.1	Zastaralý RouterOS	101
4.7.1.1	Upgrade RouterOS	102
4.7.2	Změna přihlašovací stránky Hotspotu	103
5	Závěr.....	105
6	Seznam použité literatury a další prameny	107

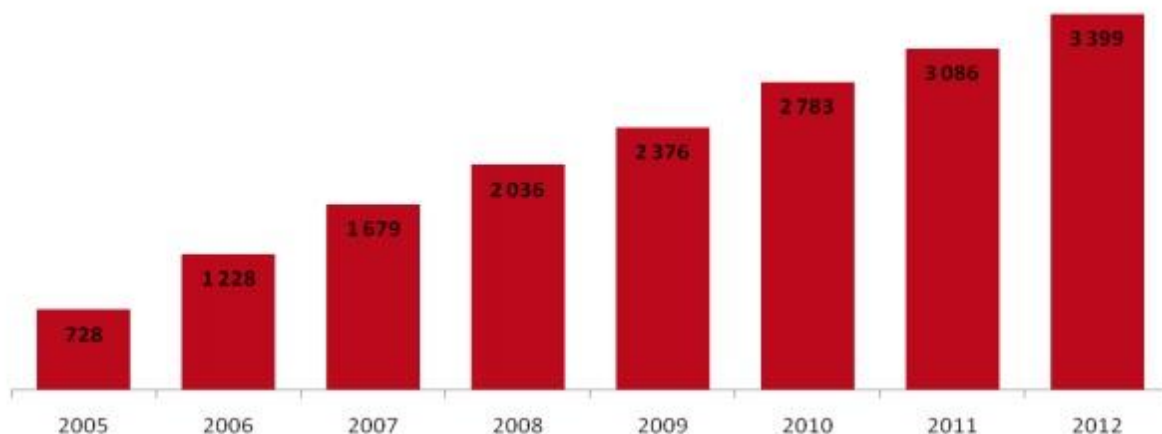
1 Úvod

21. století, doba ohromného a neustálého rozmachu informačních technologií, s sebou přináší mimo jiné i velký pokrok v rozvoji a využívání Internetu. S tím je spojený i rozmach bran připojení k Internetu, jejich technologie a zabezpečení. V současnosti již není internetové připojení otázkou pouze velkých firem či státních institucí, ba dokonce i Internet v každé domácnosti je již téměř, až na výjimky, naprostou samozřejmostí. Není tedy divu, že počet uživatelů Internetu dle statistik dosahuje hodnoty téměř 3 miliard uživatelů. Jen v České republice je zaznamenáno okolo 7 milionů uživatelů a tato čísla neustále narůstají [1].

Téma mojí diplomové práce je zaměřeno na veřejné brány umožňující přístup k Internetu, tzv. Hotspoty. Ty umožňují širšímu počtu potenciálních uživatelů se připojit pomocí bezdrátové technologie WiFi¹ k Internetu kdekoliv ve městě, či veřejném prostranství, které bude pokryto signálem některého z Hotspotů. Vzhledem k tématu mojí diplomové práce uznávám za vhodné pro začátek uvést, jak moc je v dnešní době Internet využíván a jakým směrem se trend ubírá. Tyto poznatky umožní posléze lépe určit, v jakých lokalitách má stavba Hotspotu největší šanci na úspěch. Někteří uživatelé využívají Internet pouze v práci, někteří naopak pouze doma a stále větší skupina uživatelů ho využívá neustále. Díky dnešním „chytrým“ telefonům a jiným mobilním zařízením mohou uživatelé využívat Internet neustále, ať už se nacházejí kdekoliv. Také je zajímavé se podívat na rozložení využití Internetu dle věkových skupin, či skupin rozdělených dle postavení ve společnosti (studenti, zaměstnaní, nezaměstnaní, důchodci atd.). To vše je potřeba brát v potaz při rozhodování, jak rozmístit jednotlivé aktivní prvky Hotspotu tak, aby pokrývaly místa s největším počtem potenciálních uživatelů.

Hladovost po Internetu a jeho rychlosti s dobou neustále roste. Když se podíváme na vývoj počtu trvale dostupných vysokorychlostních přípojek k Internetu v České republice od roku 2005 do roku 2012, zjistíme, že počet těchto přípojek vzrostl za tuto dobu více než 4,5x. [2]

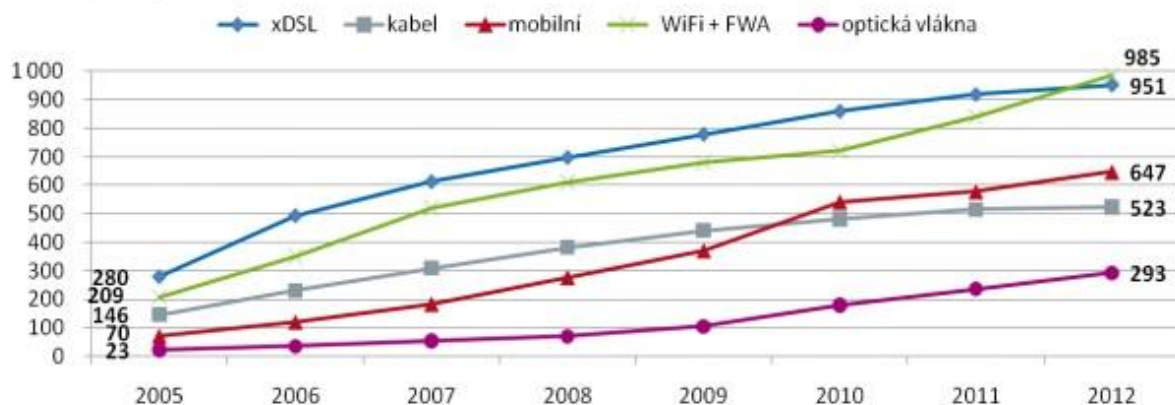
¹ Wireless Fidelity



Obrázek 1.1: Počet vysokorychlostních přípojek k Internetu v ČR (v tisících) [2]

Neméně zajímavé je také zjištění, jak se vyvíjí trend jednotlivých technologií vysokorychlostního připojení v České republice. [2] Mezi srovnávanými jsou následující technologie: linky xDSL², kabelové připojení přes televizi, mobilní připojení, bezdrátové WiFi přípojky a připojení pomocí optických vláken. Všechny technologie v čase samozřejmě v počtu svých uživatelů narůstají. Je potřeba ale zdůraznit, že u některých se nárůst začíná ustalovat, zatímco u jiných narůstá nadměrně oproti ostatním. Do budoucna mají rozhodně velkou vizi optická vlákna, která nabízejí nejkvalitnější a nejrychlejší připojení se zároveň nejmenším problémem, co se týče rušení a okolních vlivů. Jediným, a to hlavním problémem je, že to není technologie bezdrátová, a tudíž celkem náročná na pokrytí většího území. Za poslední dobu dosahuje největšího rozmachu, a dokonce obsazuje první místo, právě WiFi technologie, která je relativně snadná k zavedení na rozlehlejších území a poskytuje dostatečnou přenosovou rychlost pro většinu aplikací, které uživatel potřebuje. To je také hlavním důvodem, proč jsem se rozhodl probrat problematiku Hotspotů, které tvoří veřejnou bránu pro připojení k Internetu prostřednictvím bezdrátové sítě - WiFi.

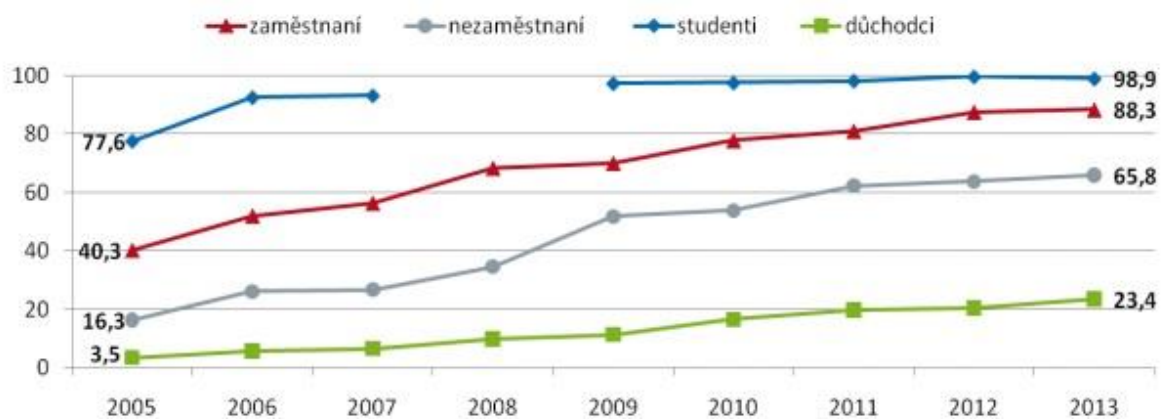
² Digital Subscriber Line



Obrázek 1.2 Počty uživatelů jednotlivých typů vysokorychlostních přípojek k Internetu v ČR (v tisících) [2]

Nyní dochází k ohromnému rozmachu trendu využívání připojení k Internetu kdekoliv a kdykoliv. Takové připojení již využívá velká skupina uživatelů prostřednictvím datových tarifů u svých mobilních operátorů. Toto řešení má sice své výhody, ale i nevýhody, a tak se spousta uživatelů poohlíží po alternativním připojení, kterým může být právě bezdrátový Hotspot. Ten oproti datovému připojení nabízí vyšší přenosovou rychlost a další výhody s tím spojené.

Posledním zjištěním, kterým jsem se zabýval, je využití Internetu jednotlivci dle ekonomické aktivity. Ve výzkumu jsou následující skupiny: zaměstnaní, nezaměstnaní, studenti a důchodci. Největší využití Internetu z těchto skupin mají studenti. Je to i logické, jelikož potřebují Internet ke své práci na různých školních projektech, komunikaci a další aktivity. Naopak nejslabší skupinou jsou důchodci. Je tomu tak pravděpodobně díky nižší gramotnosti starší generace ve využívání Internetu a ovládání počítače vůbec.[2]



Obrázek 1.3 Jednotlivci používající Internet dle ekonomické aktivity (hodnoty jsou v % z celkového počtu)[2]

V první části mé diplomové práce je probrána problematika WiFi sítí, jak fungují, různé technologie přenosu a v neposlední řadě velice důležité zabezpečení. Proberu problematiku Hotspotu na několika platformách a uvedu možnosti nasazení platební brány. V praktické části poté navrhnu dvě topologie pro WiFi Hotspot, které budou moci v budoucnu být využity v praxi. Jedna topologie poskytuje řešení pro restauraci, zatímco druhá, větší topologie, nabízí řešení pro nasazení hotspotového systému poskytovatelem Internetu ve městě Trutnov. Dalším krokem bude provedení simulace těchto topologií a odzkoušení funkčnosti na reálných zařízeních. Veškeré konfigurace a testování proběhne na platformě Mikrotik.

Hlavním zaměřením teoretické části mé práce je probrání problematiky Hotspotů a technologií, které Hotspoty využívají, či které značně ovlivňují jejich funkci. Převážná většina Hotspotů je založena na bezdrátových sítích. Z tohoto důvodu je nejprve nutné uvedení do problematiky protokolu 802.11x, který je bezdrátovými Hotspoty využíván. Následně popíšu problematiku přenosových parametrů, které ovlivňují přenos a zároveň také slouží jako měřítko pro kvalitu a rychlost přenosu signálu v bezdrátových Hotspotech. Samotný přenos signálu může probíhat prostřednictvím různých režimů komunikace. Představím režimy, které jsou bezdrátovými Hotspoty nejvíce využívány a jejich inovované nástupce, kteří umožnily využití kontroly kvality služeb QoS. Všechny tyto části, kterými se budu zabývat v druhé kapitole mé diplomové práce, jsou nezbytné pro samotné důkladné pochopení fungování bezdrátového Hotspotu. Z tohoto důvodu jím je věnováno místo

ještě před samotným podrobným rozebráním Hotspotů a jejich funkcí, které budou následně navazovat v kapitole třetí. Kromě samotné problematiky Hotspotů, kvality služeb a jejich zabezpečení, také představím několik platforem, na kterých je možné Hotspot provozovat. Uvedu jejich výhody a nevýhody a provedu následné srovnání. Závěrem třetí kapitoly ještě popíši problematiku platebních bran pro Hotspoty a popíši několik možných návrhů na implementaci hotspotové platební brány. Jelikož je v poslední době čím dál více využívána a nasazována platforma Mikrotik, bude jí během představení jednotlivých platforem věnován větší prostor. Kapitola čtvrtá bude popisovat implementaci Hotspotu na platformě Mikrotik. Hotspot bude implementován na dvě topologie a také s několika různými RADIUS servery, které budou následně porovnány, co se týče jejich výhod a nevýhod. V poslední kapitole provedu závěrečné shrnutí a vyhodnocení celé práce.

Struktura celé práce je uzpůsobena tak, aby byly nejprve představeny určité technologie a standardy, které jsou Hotspoty a jejich funkcemi využívány. Následně při představení samotných Hotspotů a jejich funkcí je již čtenář obeznámen s určitými technologiemi, o kterých se zde pojednává, a může si tedy propojit teorii s praxí. Práce obsahuje anglicismy, které jsou v tomto oboru běžné a výstižnější než jejich české ekvivalenty, které dokonce u některých slov doposud v přesném překladu neexistují.

2 Bezdrátové technologie pro Hotspot

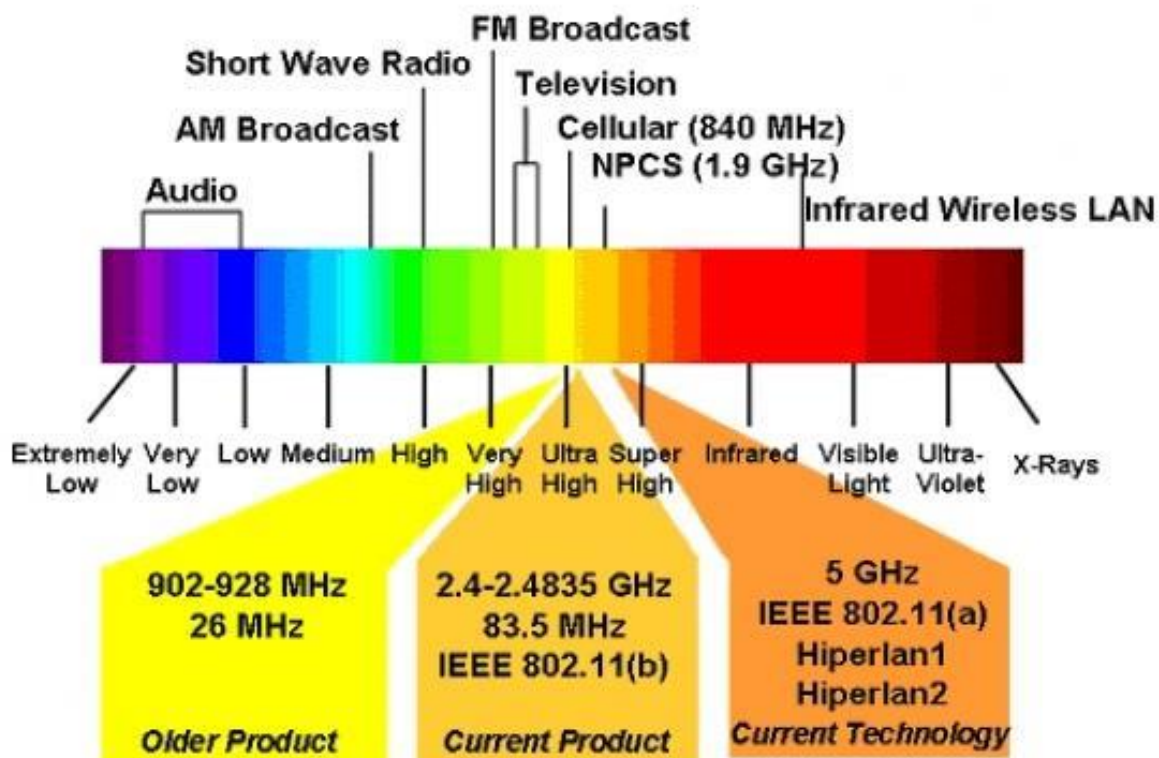
Tato kapitola slouží jako základní uvedení do problematiky bezdrátových technologií a standardů, které využívají. Zaměřím se zde na standard IEEE 802.11 a jeho vývoj, rozdíly mezi jednotlivými standardy a jejich výhody a nevýhody. Dále chci představit přenosové parametry, které nám ovlivňují přenos dat v bezdrátových sítích a jsou pro využití Hotspotu a případného pozdějšího nasazení QoS důležité. V poslední části této kapitoly popíšu základní režimy komunikace, které jsou používány při přenosu dat prostřednictvím bezdrátových technologií a jejich inovované verze, které jsou důležité pro pozdější využití QoS.

2.1 Standard IEEE 802.11

[31] Pokud se podíváme trochu do historie, první kámen ke vzniku standardu IEEE³ 802.11 položila v roce 1985 FCC⁴, která povolila užívání několika pásem bezdrátového spektra bez nutnosti vlastnit licenci schválenou vládou. Tato pásma, nazývaná často jako „garbage bands“ (v překladu odpadová pásma), byla původně vyhrazena pro využití elektronickými zařízeními, jako je například mikrovlnná trouba, která využívá tyto vlny pro ohřev potravin. Pro bezdrátový přenos dat se ale muselo toto pásmo upravit. Aby mohla bezdrátová zařízení pracovat v prostoru a na větší vzdálenosti, muselo se využít rozšířeného pásma. To umožňuje vysílat radiové vlny v rozsahu širokého spektra frekvencí. Díky tomu je signál méně náchylný na interferenci vlnění a dá se lépe přijímat i přes různé překážky.

³ Institute of Electrical and Electronics Engineers

⁴ United States Federal Communications Commission



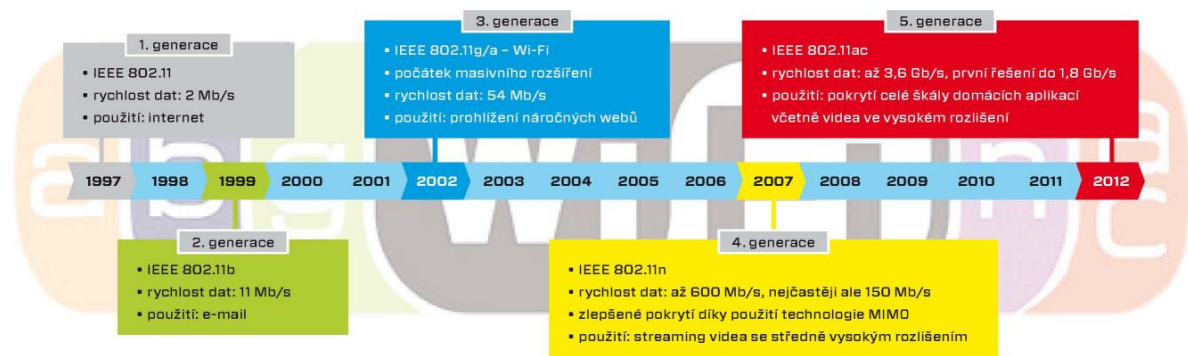
Obrázek 2.1 Přehled jednotlivých pásem v rámci celého spektra vlnění [3]

Standard IEEE 802.11 jako takový tedy specifikuje obecně bezdrátové rozhraní mezi bezdrátovým klientem a AP⁵, nebo mezi dvěma či více bezdrátovými klienty. Toto bezdrátové rozhraní využívají zejména místní sítě, metropolitní sítě a lokální bezdrátové sítě typu LAN⁶ nebo WAN⁷. S postupným vývojem bylo ale potřeba tento standard nadále rozdělit, aby bylo možné přesněji specifikovat a odlišit jednotlivé typy a technologie bezdrátového přenosu dat. Postupně tedy vznikaly dílčí standardy standardu 802.11, které jsou označovány zpravidla dodáním písmene nakonec. Co se týče typu přenosu a využití určitého pásma, známe v současné době následující standardy: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac a 802.11ad.

⁵ Access Point – přístupový bod

⁶ Local Area Network

⁷ Wide Area Network



Obrázek 2.2 Vývoj jednotlivých standardů 802.11 na časové ose [4]

2.1.1 IEEE 802.11b

Standard IEEE 802.11b je prvním masově nasazeným a využívaným standardem. [30] a [31] Pracuje v pásmu 2,4GHz a za ideálních podmínek dosahuje maximální přenosové rychlosti 11Mb/s. Na fyzické vrstvě využívá k přenosu technologii DSSS⁸. Vysílací výkon zařízení se pohybuje okolo 200mW. V dnešní době je již tento standard značně zastaralý a byl nahrazen novějším standardem 802.11g, který je s tímto standardem zpětně kompatibilní.

2.1.2 IEEE 802.11g

Standard IEEE 802.11g je dlouho očekávaným nástupcem standardu IEEE 802.11b. Pracuje ve stejném pásmu 2,4GHz a díky tomu je tedy zpětně kompatibilní s předchozím standardem 802.11b. V době tohoto standardu nastal neskutečný rozmach bezdrátových zařízení, zejména pro bezdrátové přípojky domácností. Také nachází své využití ve stále narůstajícím počtu firem. [30] Jeho hlavní výhodou je přenosová rychlost, která v ideálních podmínkách může dosáhnout hodnoty až 54Mb/s. Touto hodnotou několikanásobně předstihuje svého předchůdce a velice rychle jej nahradil. Dalším rozdílem je technologie přenosu dat na fyzické vrstvě. Při rychlostech, na kterých fungoval předchozí standard 802.11b, o hodnotách 1Mb/s, 2Mb/s, 5,5Mb/s a 11Mb/s, využívá stejnou technologii jako standard 802.11b, tedy DSSS. Ovšem při rychlostech vyšších, konkrétně 6Mb/s, 9Mb/s, 12Mb/s, 18Mb/s,

⁸ Direct Sequence Spread Spectrum

24Mb/s, 36Mb/s, 48Mb/s a 54Mb/s, využívá technologii odlišnou a to sice OFDM⁹. Také byl zaznamenán pokrok ve snížení vysílacího výkonu, který poklesl na hodnotu okolo 65mW. Přesto, že je v dnešní době již tento standard zastaralý, nalezneme ještě stále nespočet míst a domácností, které jej stále ve velké míře využívají.

2.1.3 IEEE 802.11a

Tento standard byl vytvořen zhruba ve stejné době jako standard 802.11b. V té době ale nebyl tak značně nasazován a využíván zejména díky svojí větší ceně, která se odvíjela od vyšších nákladů na výrobu. Svého rozmachu se tedy dočkal až později, a to sice v obdobné době jako standard 802.11g. [30] Hlavním rozdílem standardu 802.11a oproti standardům 802.11b, 802.11g a 802.11n je, že funguje v pásmu 5GHz, přesněji v pásmech 5,15-5,35GHz, 5,47-5,725GHz a 5,725-5,825GHz. Díky využití této vyšší frekvence není kompatibilní s výše probranými standardy. Právě proto je nasazován do oblastí, kde je husté pokrytí v pásmu 2,4GHz, a tedy nasazení dalšího zařízení ze stejného pásma by vedlo k interferenci vlnění a následnému rušení signálu. Poskytovatelé Internetu jej s oblibou využívají na bezdrátové spoje dvou síťových prvků mezi zástavbami, které jsou hustě pokryty AP v domácnostech uživatelů, vysílajících právě v pásmu 2,4GHz. Vyšší frekvence s sebou ale přináší i určité nevýhody. Hlavní z nich je menší propustnost a ohebnost signálu přes různé překážky.

Co se týče ostatních parametrů, standard IEEE 802.11a využívá stejné technologie přenosu jako standard IEEE 802.11g, tedy OFDM. Přenosová rychlost dosahuje při ideálních podmínkách stejně jako u standardu IEEE 802.11g hodnoty 54Mb/s.

2.1.4 IEEE 802.11n

Když se v roce 2007 objevil další nový standard s názvem 802.11n, už se tušilo, že to bude něco velkého. Tento standard sliboval dosažení teoretické přenosové rychlosti až 600Mb/s. Tuto hodnotu ovšem v praxi nelze naměřit téměř na žádném zařízení. Většina zařízení, která přišla na trh, nabízela reálnou přenosovou rychlost 150Mb/s v obousměrném provozu (full duplex). K dosažení této rychlosti je ale

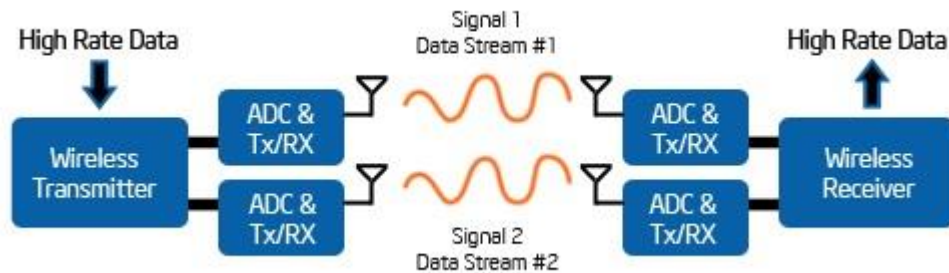
⁹ Orthogonal Frequency Division Multiplexing

zapotřebí použít v síti pouze zařízení podporující standard 802.11n, jinak bude rychlost razantně nižší. Tento standard je totiž zpětně kompatibilní se všemi předchozími standardy (802.11b, 802.11g, 802.11a), a umí tedy pracovat v pásmu jak 2,4GHz tak 5GHz. Pokud jsme nuceni z nějakého důvodu využít kompatibility se staršími zařízeními, máme možnost volby ze dvou možností. První se nazývá Legacy mód, ve kterém budou zařízení pracovat pouze v režimu standardů 802.11b, 802.11g nebo 802.11a. Taková možnost ale znemožní využití jakékoliv výhody plynoucí z nasazení nového standardu 802.11n. Druhou možností je tzv. Mixed mód, ve kterém se využívají všechny předchozí standardy jako u Legacy módu, ale navíc je zahrnut právě i nový standard 802.11n, který mohou využívat všechna zařízení v síti, která tento standard podporují.

Jak už bylo zmíněno, tento standard podporuje kvůli kompatibilitě obě frekvenční pásma. Pokud chceme dosáhnout co nejlepšího výkonu, měli bychom využít pásmo 5GHz, které nám nabízí širší spektrum. Dalším pokrokem je možnost volby buď tří 20MHz kanálů nebo jednoho 40MHz kanálu. Pro dosažení co největší šířky pásma je doporučeno použít právě 40MHz kanálu [5].

Další novinkou tohoto standardu je technologie MIMO¹⁰. Jedná se o využití většího počtu antén jak na vysílacím, tak na přijímacím zařízení. Díky tomu může být přenášeno několik různých datových toků na jednom kanálu. Čím více dokážeme přenést naráz různých datových toků, tím více dat za jednotku času můžeme přenést. Počet různých datových toků, které mohou být přeneseny, je závislý na počtu antén. Čím více antén, tím více datových toků může být naráz přenášeno. MIMO technologie těží z toho, že využívá všech radiových vln, dokonce i těch odražených od různých překážek. V tom je zásadní rozdíl proti předchozím technologiím, kde naopak odražené vlny způsobovaly interferenci s vlnami neodraženými. Díky většímu počtu antén může každá anténa zpracovávat signál z různých datových toků [6].

¹⁰ Multiple Input Multiple Output



Obrázek 2.3 Jak funguje systém MIMO [7]

2.1.5 IEEE 802.11ac

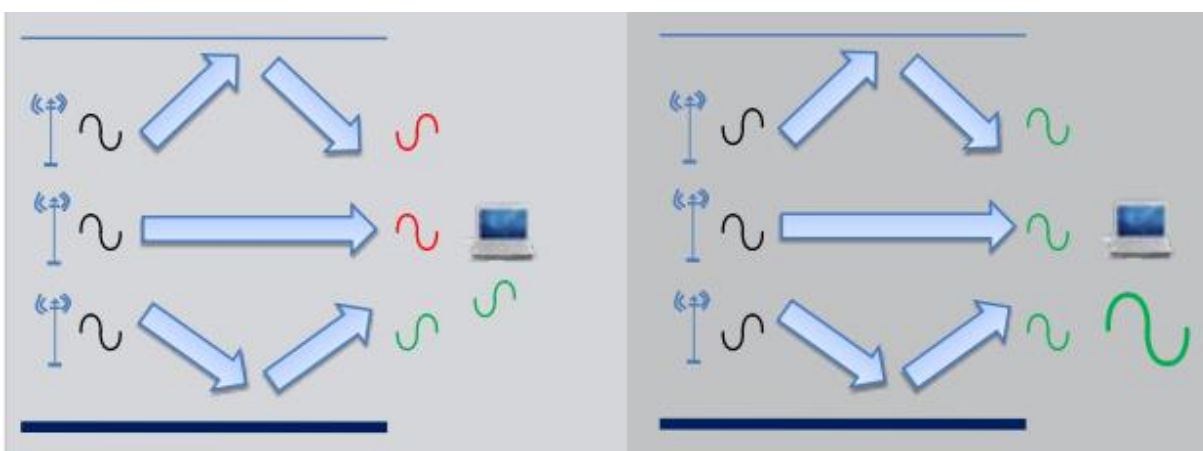
S pokročilou dobou a stále rostoucími požadavky na rychlost bezdrátových sítí přišlo řešení v podobě standardu IEEE 802.11ac, který byl zaveden v roce 2012. Oproti svým předchůdcům byl tento standard značně vylepšen a má několik novinek. Tento standard pracuje již výhradně v pásmu 5GHz. Hlavním důvodem volby tohoto pásma bylo větší množství volných nepřekrývajících se kanálů. Zařízení s tímto novým standardem jsou zpětně kompatibilní s předcházejícími standardy, dokonce i v pásmu 2,4GHz, kdy ale nebude možné využívat žádné z výhod, které tento nový standard přináší.

Teoretická rychlost u tohoto standardu by měla dosahovat hodnoty 1,3Gb/s. Reálně naměřená rychlost se pohybuje opět řádově v jiných číslech a to sice okolo 300Mb/s. Stejně jako tomu bylo u standardu 802.11n i tento standard využívá více antén, dokonce se maximální počet teoreticky použitelných antén vyšplhal na číslovku osm. Také šířka kanálu se zvedla na teoretickou hodnotu až 160MHz, přičemž běžně standard využívá šířku kanálu 80MHz. Hodnota 160MHz dokonce nemůže být v některých zemích použita kvůli omezené šířce pásma pro volné užívání - např. Čína.

Další novinkou u tohoto standardu je dělení komunikace na proudy (streamy). Počítá se s maximálním počtem až osmi proudů, přičemž pro komunikaci s jedním zařízením se budou využívat najednou maximálně tři proudy. Jediným háčkem prozatím je, že většina menších mobilních zařízení umí komunikovat pouze na jednom proudu, takže není možné tohoto potenciálu využít. I tak ale má více proudů na vysílači svůj význam a to díky další staré nově vylepšené technologii s názvem MU-

MIMO¹¹. Jak již název napovídá, tato technologie umožňuje komunikaci s několika zařízeními najednou. To řeší problém z minulosti, kdy bez ohledu na počet proudů mohl vysílač komunikovat vždy pouze s jedním zařízením. Pokud bylo zařízení více, musela se v komunikaci s vysílačem střídat. Nyní díky více proudům může na každém proudu komunikovat vysílač s jiným zařízením, přičemž může využít např. dva proudy pro komunikaci s laptopem a jeden proud pro komunikaci s mobilním telefonem.

Poslední nasazenou technologií, která se již objevovala i u některých zařízeních se standardem 802.11n, kde ale nebyla povinná, je tzv. Beamforming. Zjednodušeně řečeno je to technologie, která napomáhá formování signálu. Vysílací zařízení dokáže zmapovat prostředí včetně různých překážek a dle toho upraví vysílání signálu z jednotlivých antén tak, aby se v cíli sešel signál ze všech antén naráz, tedy ve fázi. Výsledkem je silnější signál i když je třeba poskládaný z odražených vln. Bez této technologie většinou signály z několika antén přijdou do cíle mimo fázi, a navzájem se tak vyruší. Tato technologie výrazně zlepšila kvalitu a dosah signálu přes různé překážky.



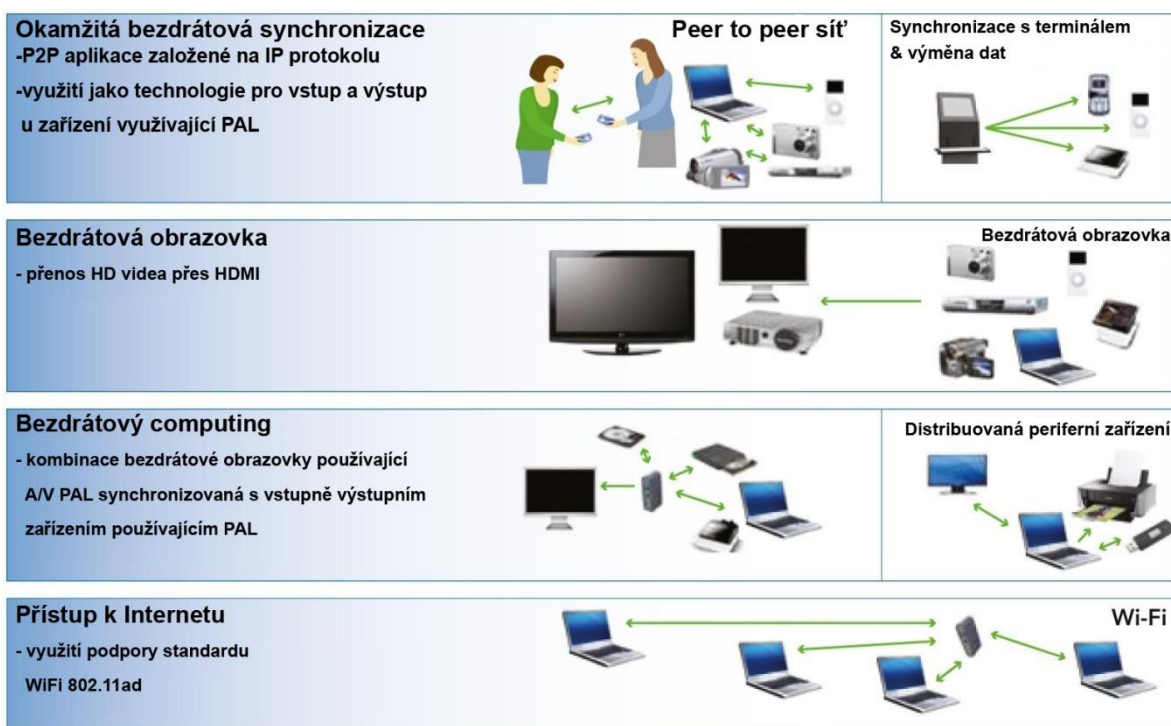
Obrázek 2.4 Ukázka Beamformingu (vlevo bez Beamformingu, vpravo s Beamformingem) [4]

2.1.6 IEEE 802.11ad

Tento standard není tak úplně typický pro označení jako WiFi, proto se také nazývá typ této sítě pojmem WiGig – název standardu, který zavedla Wireless Gigabit Alliance. Tento standard pracuje na rozdíl od všech ostatních na frekvenci 60GHz. To

¹¹ Multi User Multiple Input Multiple Output

mu umožňuje dosahovat rychlosti až 7Gb/s. Jak už to tak ale bývá, nic není zadarmo. Zvýšení přenosové rychlosti bylo dosaženo na úkor dosahu. Díky vysoké frekvenci se signál špatně ohýbá a odráží od překážek, a tudíž použití na vzdálenost větší než deset metrů je bez použití adaptivního beamformingu nemožné. To by ale nemělo být na závadu, jelikož hlavním účelem tohoto standardu by mělo být propojení zařízení s velkoplošnou obrazovkou či projektorem v rámci jedné místnosti. Mimo jiné by tento standard umožňoval streamování HD videa bez použití kabelového spojení. Většina směrovačů by měla umět i starší standardy, aby mohly komunikovat i se zařízeními, která nepodporují nový standard IEEE 802.11ad [8] [9].



Obrázek 2.5 Idea využití standardu IEEE 802.11ad [Upraveno dle 10]

2.2 Přenosové parametry

Už jsme si představily několik různých standardů, které slouží pro přenos signálu v bezdrátových sítích. Každý standard má svá specifika, díky nimž nabízí jak různé rychlosti přenosu dat, tak i kvalitativní vylepšení přenášeného signálu. Jelikož je v praxi zapotřebí nějakým způsobem určit, v jakém směru a pro jaké použití je signál více či méně kvalitní, existují tzv. přenosové parametry. Naměřené hodnoty každého

z následujících parametrů se vyhodnotí a určí se, v čem může být problém, či zdali je signál a přenosová rychlost dostatečná pro konkrétní službu např. hlasové hovory.

2.2.1 Koncové zpoždění

Delay, neboli česky koncové zpoždění či také latence, nám udává dobu, která je nezbytná na přenos paketu od zdroje k příjemci. Tento parametr může být ovlivňován velkým množstvím faktorů. Když pomíneme vnější síly, kterými jsou počasí, překážky a různé jiné rušení signálu, jsou zde i další faktory, které mají na zpoždění vliv. Mezi ně patří například použité kódování, příprava paketů na přenos kanálem, čekání paketů ve frontách přenosových zařízení, či dekódování signálu. Pokud koncové zpoždění přesáhne určitou hodnotu, ztratíme plynulost našeho hovoru či videokonference. U videokonference při takovém jevu nedojde ke ztrátě obrazu, ale sníží se FPS¹² neboli počet snímků za sekundu, což má za následek neplynulost tzv. „trhání“ obrazu. Pro sledovatelný obraz u videokonference potřebujeme alespoň 25 FPS. Co se týká hlasových hovorů, nemělo by jednosměrné koncové zpoždění přesáhnout hodnotu 180ms. Při vyšším koncovém zpoždění dochází ke zpoždění hovoru. Zatímco jedna strana už domluvila, druhá strana stále poslouchá zpožděnou zprávu. U přenosu dat není na tento parametr kladen takový důraz.

2.2.2 Kolísání zpoždění

Jitter, neboli česky kolísání zpoždění, nám udává rozdíl v časových intervalech mezi přijímanými pakety. Dochází k němu nejčastěji v místech, kde se slučuje několik zdrojů do jednoho výstupu. Opět je to velice důležitý parametr, zejména pro hlasové a obrazové služby. Dá se říci, že pro kvalitní hlasovou komunikaci je tento parametr ještě více důležitý, než samotné koncové zpoždění. Je totiž velice důležité, aby pakety s obsahem hlasové komunikace přicházely ve stejných časových úsecích. Pro plynulý hlasový hovor by hodnota kolísání zpoždění neměla přesáhnout hranici 30ms. To je ale v praxi velice těžko dosažitelné. Z tohoto důvodu nasazujeme nástroje QoS, které nám pomáhají u prioritních dat (např. hlasových hovorů či video hovorů) hodnotu kolísání zpoždění snížit. Ke snížení kolísání zpoždění se také využívá různých

¹² Frames Per Second

vyrovnávacích pamětí nebo bufferu, obsaženém v koncovém zařízení VoIP¹³. Tyto buffery v koncových zařízeních ale většinou způsobují zvětšení celkového zpoždění.

2.2.3 Ztrátovost paketů

Packet loss, neboli česky ztrátovost paketů, nám udává podíl přijatých a vyslaných paketů za jednotku času. Většinou se udává v procentech. Ke ztrátě paketů může dojít z několika možných příčin. V poslední době jsem velice často řešil problém, který je výhradou bezdrátových spojení mimo budovy, že za určitou dobu od montáže příslušného vysílače a přijímače se v cestě objevil nějaký nový porost, který tam před určitou dobou nebyl. Jelikož jeho větve zasahují jen z části do „vzdušné cesty“ mezi vysílačem a přijímačem, dochází jen k občasné ztrátovosti paketů, což může být občas při hledání problému matoucí. Další příčinou ztráty paketů může být vyčerpání zmíněné vyrovnávací paměti, či zahlcení procesoru některého ze zařízení. Pokud se podíváme na služby dle náročnosti na ztrátovost, bude tomu opačně, než jsme byli zvyklí u koncového zpoždění a kolísání zpoždění. Nejcitlivější na ztrátu paketů jsou data. U nich si nemůžeme dovolit vypustit žádný paket, jinak dostaneme data poškozená či neúplná. Proto se u přenosu dat často využívají různé algoritmy pro opětovné zaslání nedoručeného paketu, aby byla přenášená data opravdu kompletní. Na druhém místě je kupodivu hlasová služba. Pokud dojde k určité ztrátě paketů, dostaví se výpadek části naší konverzace. Bohužel zde nemůžeme využít stejných algoritmů pro znovu zaslání ztracených paketů, jelikož by to již nemělo smysl (sdělení by bylo již neaktuální). Pro kvalitní fungování hlasových služeb by se měla udržet ztrátovost paketů do 1%. Nejméně náchylné na ztrátu paketů je streamované video. Pokud dojde ke ztrátě některých paketů, dojde „pouze“ k jeho rozostření či krátkodobému výpadku, na který se ale opět naváže.

2.2.4 Šířka pásma

Bandwith, neboli česky šířka pásma, nám udává přenosovou kapacitu a propustnost daného kanálu. Každá služba má na šířku pásma jiné požadavky. Například data lze různě shlukovat a až poté přenášet. Naopak již zmiňované hlasové

¹³ Voice over Internet Protocol

služby si vystačí s užší šířkou pásma, ale za to konstantní, aby nedocházelo ke ztrátám. Šířka pásma závisí na několika faktorech, jako je rychlost vzorkování, typ použitého kodeku či režie na druhé vrstvě.

2.3 Režimy komunikace

Všechny popisované režimy komunikace nám definují, jak se chová kanál (frekvenční pásmo) při jeho sdílení mezi více koncovými uzly a přístupovým bodem (AP). Jelikož původní standard využíval pouze režimy, které neumožňovaly využití QoS, standard IEEE 802.11e zavedl rozšíření obou stávajících režimů přístupu k radiovému kanálu pro podporu QoS. Povinný DCF¹⁴ byl rozšířen na ECDF¹⁵ a volitelný PCF¹⁶ na rozšíření nazvané HCF¹⁷. Mimo jiné zajišťuje také zpětnou slučitelnost se zařízeními pracujícími se standardy IEEE 802.11a/b/g/n.

2.3.1 DCF

DCF je základní přístupovou metodou standardu IEEE 802.11, kterou implementují všechny stanice. Režim DCF je založen na metodě přístupu CSMA/CA¹⁸, v překladu mnohonásobný přístup s nasloucháním a vyvarováním se kolizím. Každá stanice musí před započítím vysílání nejprve naslouchat, zda nevysílá někdo jiný. Systém je podobný systému CSMA/CD¹⁹, který funguje na ethernetových sítích. Jelikož bezdrátové sítě podporují pouze half duplexní provoz (nejsou schopny zároveň vysílat a přijímat), není možné tento systém u nich použít. Mechanismus pro předcházení kolizím využívá dvě techniky. První technikou je IFS²⁰ tzv. vkládání mezery mezi vysílanými rámci. Druhou technikou je Backoff neboli odklad vysílání. Interval DIFS (DCF IFS) odpovídá době povinného čekání po zjištění volného vysílacího kanálu, než stanice bude moci sama začít vysílat. Pokud by v této době začala vysílat další jiná stanice, dojde k odkladu vysílání. Interval odkladu vysílání si náhodně volí sama

¹⁴ Distribution Coordination Function

¹⁵ Enhanced Distribution Coordination Function

¹⁶ Point Coordination Function

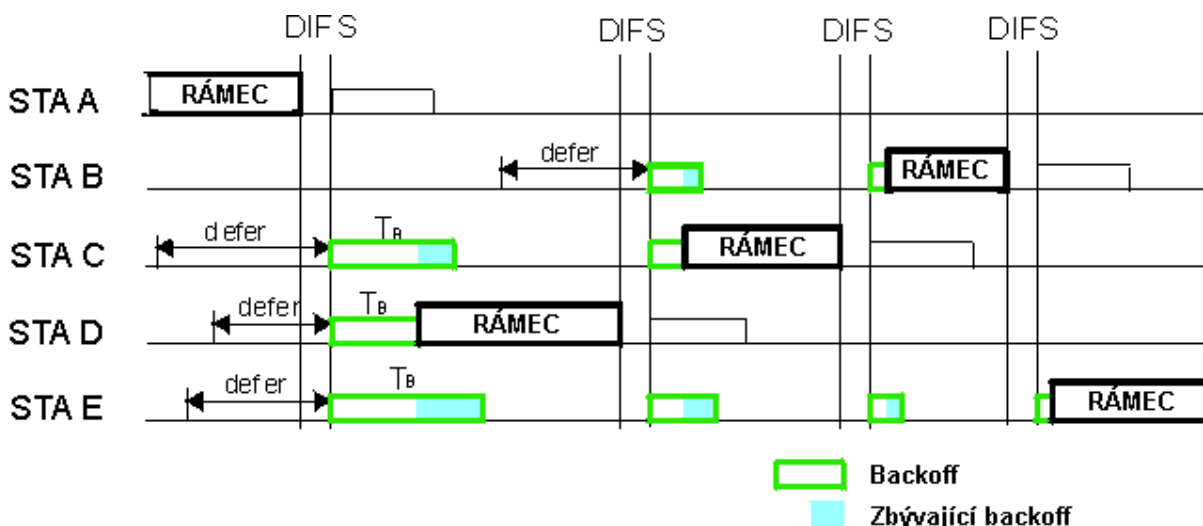
¹⁷ Hybrid Coordination Function

¹⁸ Carrier Sense Multiple Access with Collision Avoidance

¹⁹ Carrier Sense Multiple Access with Collision Detection

²⁰ Inter Frame Space

stanice a to sice z intervalu od nuly do velikosti CW²¹, česky nazýváno okno sváru. Ale i tak je možné, že může nastat kolize. K tomu dojde, pokud by se naráz začalo o vysílací kanál ucházet více stanic. Pokud dojde k další kolizi, velikost okna sváru se s každou kolizí zdvojnásobuje a dochází k tzv. Exponential Backoff. Po uplynutí tohoto intervalu odkladu a za podmínky, že je médium volné, může začít vysílání dat.[11]



Obrázek 2.6 Znárodnění režimu DCF v bezdrátové síti [Upraveno dle 24]

Jako další ochrana dat je zde ještě jeden mechanismus a to sice potvrzování o doručení. Pokud příjemce či přístupový bod obdrží paket, vyčká po dobu SIFS²², která je, jak již název napovídá, kratší než DIFS, a poté vyšle zpět potvrzení o přijetí paketu. Toto potvrzování je velice důležitou součástí obzvláště u WLAN²³, jelikož může dojít ke ztrátě či poškození dat, ať už v důsledku kolize, či pro nedostatečnou kvalitu kanálu.

Pokud dojde k tomu, že se vysílající stanice navzájem nevidí, znamená to, že přístupový bod musí řešit více kolizí, jelikož všechny stanice v okolí si mohou myslet, že se momentálně nacházejí v prostoru samy. V takovém případě umožňuje většina stanic zapnout mód RTS/CTS²⁴, ve kterém začínají stanice vysílat požadavkem – paketem RTS. Pokud je médium volné, stanice obdrží potvrzení od AP – paket CTS. Toto potvrzení říká stanici, že může po určitou stanovenou dobu vysílat. Na základě intervalu uvedeného v CTS paketu si ostatní stanice v okolí upraví alokační vektor

²¹ Contention Window

²² Short Inter Frame Space

²³ Wireless LAN

²⁴ Request to Send/Clear to Send

NAV²⁵, který obsahuje časový interval, během kterého se stanice nepokoušejí navázat spojení s AP. Mód RTS/CTS má ale velmi negativní dopad na propustnost systému, která může klesnout až na 20% deklarované kapacity.

2.3.2 PCF

Jelikož je režim PCF volitelný, nebývá nasazován zase tak často. Jedním z důvodů je, že je určen pouze pro synchronní datové přenosy a také se dá využít pouze v bezdrátové síti s infrastrukturou. Nasazení v síti typu Ad-hoc není možné. Přístupové body jsou totiž právě využívány k periodickému vysílání rámců typu beacon, kterými sdělují stanicím v síti aktuální specifické parametry pro identifikaci a management. Přístupový bod dělí mezi vysíláním těchto administrativních rámců dobu na dvě části. První je doba bez boje o médium tzv. contention-free, zatímco druhá je doba, kdy probíhá boj o médium tzv. contention. Pokud má nějaká stanice prioritní data k odeslání, může na základě výzvy obdržet povolení ke garantovanému vysílání po dobu, kdy nemusí s nikým jiným o médium bojovat. Jako už jsme si vysvětlili u režimu DCF interval DIFS i režim PCF má obdobný interval nazvaný PIFS – PCF IFS. Tento interval slouží k ohlášení stavu bez kolizí, aby mohly vysílat stanice s prioritním vysíláním. Ve srovnání s DIFS je PIFS o něco kratší ale zároveň o něco delší než SIFS.

2.3.3 EDCF

EDCF je prvním režimem upraveným dle normy IEEE 802.11e, který podporuje QoS. Tento režim rozlišuje provoz do čtyř kategorií, skládajících se z osmi prioritních tříd, rozdělených dle požadavků každého typu zátěže. Kategorie zabírají celé spektrum od nejnižší priority, která deklaruje pouze „Best effort“ QoS, až po nejvyšší prioritu, která se využívá u aplikací extrémně závislých na jakémkoliv zpoždění.

²⁵ Network Allocation Vector

Priorita (0 - 7)	Kategorie přístupu	Určeno pro
0	0	Best effort
1, 2	1	Pozadí
3, 4, 5	2	Video
6, 7	3	Hlas

Tabulka 2.7 Mapování priority na kategorii přístupu

Pokud je médium volné, může každá stanice začít vysílat. Má to ale ještě jednu podmínku a to sice, že musí uplynout interval čekání daný pro konkrétní kategorii provozu. Tento interval čekání AIFS²⁶ se prodlužuje se snižující se prioritou provozu. Mimo to se ještě k intervalu AIFS přičítá v případě kolize náhodný interval, který vygeneruje stanice při pokusu o přístup k médiu a detekování kolize. Tím se omezí počet kolizí s jinými stanicemi, které provozují EDCF ve stejné kategorii. Tímto vším je zajištěno, že stanice s vysokou prioritou provozu bude čekat kratší dobu na vysílání, než stanice s nízkou prioritou. Tím nám začíná fungovat právě QoS a provoz se stává řízeně neférový, kdy jsou upřednostňována data s vyšší prioritní třídou.

Režim EDCF tedy s vysokou pravděpodobností přidělí vyšší hodnotu šířky pásma kategorii s nižší prioritou při „boji“ o sdílené médium. Další ohromnou výhodou EDCF je jeho snadná implementovatelnost, díky níž je tato metoda často využívána.

2.3.4 HCF

HCF definuje stejně jako PCF dotazovací mechanismus. Jak už jsme od PCF zvyklí i zde jsou definované intervaly, které nám ohraničují „beacon“ rámce, jenž jsou rozděleny na dvě periody a to sice CFP a CP. V průběhu CFP tzv. hybridní koordinátor – většinou AP ovládá přístup k médiu. Během doby CP pracují všechny stanice v režimu EDCF. Zároveň také může během průběhu CP koordinátor převzít kontrolu nad přenosným médiem tím, že zašle CF-Poll paket všem stanicím. U HCF oproti PCF jsou nejvýznamnější následující rozdíly:

- HCF má definované již zmiňované třídy provozu – traffic classes. Díky nim může být uplatňováno QoS.

²⁶ Arbitration Interframe Space

- Stanice poskytují informace o délkách jejich front požadavků pro každou třídu provozu. Koordinátor tyto informace využívá pro upřednostňování určitých stanic před jinými.
- Stanice mají možnost využít TXOP²⁷, čímž se rozumí možnost zasílat několik paketů najednou v časovém intervalu určeném koordinátorem.

HCF je ze zmiňovaných metod nejpokročilejší. Pokud použijeme HCF, můžeme konfigurovat požadovanou kvalitu přenosu služeb s velkou precizností.

²⁷ Transmit Opportunity

3 Brána pro připojení k Internetu - Hotspot

V této kapitole představím Hotspoty a jejich typy a funkce. Následně naváží na typy řízení Hotspotů a velice důležitou část věnovanou zabezpečení. V rámci zabezpečení bude probrána i autentizace, autorizace a účtování řešené AAA²⁸ protokolem, který je pro náš bezdrátový Hotspot stěžejní. Proberu kvalitu služeb a následně představím několik platforem, na kterých se dá Hotspot provozovat, přičemž hlavní zaměření budu věnovat platformě Mikrotik. Závěrem této části provedu srovnání výhod a nevýhod jednotlivých platforem, jejich zhodnocení a provedu návrh na možnosti implementace platební brány pro Hotspot.

3.1 Popis Hotspotu

Jako Hotspot je obecně označována oblast, ve které je možné se bezdrátově za pomoci WiFi technologie připojit k síti či Internetu. Hotspot ale nemusí být zdaleka vždy provozován pouze na bezdrátových sítích, zrovna tak se dá aplikovat i na sítě metalické či optické, ale jeho využití v této sféře není tak hojné. V souvislosti s mojí prací je ale Hotspot chápán spíše jako služba, která nám po autentizaci uživatele umožní přístup do sítě či Internetu. Tato služba má hlavní výhodu v tom, že není zapotřebí, aby uživatel instaloval nějaký speciální software, či musel využívat jiné speciální vybavení k tomu, aby se připojil. Veškerá komunikace na straně uživatele probíhá přes rozhraní webového prohlížeče, tudíž jakékoliv zařízení, které je schopné využívat jednoduchý webový prohlížeč, má možnost se připojit na Hotspot. S Hotspotem se můžeme setkat jak v privátním, tak veřejném sektoru, přičemž druhá možnost je více pravděpodobná. Typická místa, kde se Hotspot využívá, jsou: letiště, kavárny, restaurace, nádraží či hotely. Hotspot v podstatě tvoří jakousi bránu do sítě, která nám zprostředkovává autentizaci, autorizaci a účtování připojovaných zařízení. Krom toho se dá ale využít i na další užitečné věci. Jak už bylo zmíněno, Hotspot využívá k přihlášení uživatele webovou stránku. Tato stránka se dá se základními znalostmi HTML a CSS snadno upravit do jakékoliv podoby a můžeme ji tak využít jako reklamní plochu. To se dá využít at' už k prezentování reklamy vlastní (např. v případě

²⁸ Authentication Authorization Accounting

restaurace či nějaké firmy), nebo reklamní plochy k pronájmu pro třetí subjekt, z čehož nám může plynout případně nějaký zisk.

Jako většina věcí má ovšem bezdrátový Hotspot i své nevýhody. Mezi ně se řadí hlavně omezený dosah signálu. Tato nevýhoda má řešení v podobě distribuovaného WiFi Hotspotu. Distribuovaný WiFi Hotspot je propojení několika bezdrátových bran pro připojení k Internetu, které se chovají, jako by to byl Hotspot jeden. Uživatel se tedy může během používání WiFi připojení pohybovat a přemísťovat se na různá místa, která jsou pokryta signálem z daného distribuovaného Hotspotu, aniž by ztratil připojení k Internetu.

Ve většině případů ale bývá Hotspot provozován na jednom zařízení. To ale není pravidlem. Hotspot může být zrovna tak provozován na složitější infrastruktuře, kdy je zapojeno několik vysílačů na různých místech. Pak už jen záleží na nasazené technologii a jak je daná infrastruktura postavená. Některá řešení nabízejí využití controlleru, což nám umožňuje řídit vše centrálně z jednoho místa. Takové řešení má většinou spousty výhod, jako například lepší roaming při přecházení mezi jedním vysílačem na druhý, ale ve většině případů si za taková řešení musíme dost zaplatit.

3.2 Funkce Hotspotu

Hotspot služba může poskytovat přístup do sítě či Internetu zdarma nebo za poplatek. Pokud se bavíme o Hotspotu, který poskytuje přístup zdarma, jedná se ve většině případů právě o restaurace nebo nějaká podobná zařízení, kde lidé své peníze utratí za jiné statky a Hotspot zde slouží jako dodatečná služba zákazníkovi. Zároveň, jak jsem již zmiňoval, může sloužit prostřednictvím přihlašovací obrazovky jako reklamní plocha. Mimo jiné může provozovatel takového Hotspotu hlídat, kdo se k Internetu připojí a kdo nikoliv. Většinou si zákazník musí v dané restauraci zažádat o tzv. voucher s přihlašovacím jménem a heslem, který mu právě umožní přístup do Internetu. Tím je možné eliminovat běžné „zloděje signálu“, kteří chodí do blízkosti dané restaurace využívat bezplatné WiFi připojení k Internetu, které má sloužit pouze pro zákazníky. Záleží jen na provozovateli, jaké vouchery pro zákazníky připraví, zdali neomezené nebo jak je tomu ve většině případů časově či datově omezené, které po vypršení dané kvóty uživatele automaticky odpojí. Pokud budeme hledat nějaký

veřejný Hotspot, který nabízí připojení zadarmo, můžeme si zkusit dopředu vyhledat místo, kde bude takové připojení možné pomocí různých serverů. Jedním takovým je například web www.wififreespot.com, kde můžeme dle lokality vyhledávat dostupné bezplatné Hotspoty. [32]

Pokud se budeme bavit o placené variantě Hotspotu, princip je obdobný. Rozdíl je v tom, že přihlašovací údaje zákazník obdrží až poté, co za ně nějakým způsobem zaplatí. Je více možností, jak platbu provést. První možností je stejně jako u výše zmíněného bezplatného Hotspotu vytvořit různé vouchery, které poté můžeme zákazníkovi prodávat. Pokud si ale představíme nějaký veřejný Hotspot například na letišti, náměstí, vlakovém nádraží a tak podobně, je nám jasné, že přístup pomocí voucheru je pro zákazníka značně nepohodlný. Obzvláště pokud se zákazník/uživatel nachází v cizím prostředí a neví, kde by si potřebný voucher zakoupil. Proto je tu druhá varianta a to sice zprostředkování platby prostřednictvím nějaké platební brány. Je to pohodlné, rychlé a nabízí to hned několik možností, jak může zákazník zaplatit za připojení k Internetu elektronickou cestou. V cizině jsou velice rozšířené platby prostřednictvím tzv. elektronických peněženek, kam si nabijete jednou za čas peníze a poté s ní můžete platit online za služby, které danou elektronickou peněženku podporují. U nás je spíše rozšířen způsob platby online pomocí platební karty a v poslední době stále více populární platba pomocí SMS zprávy z jakéhokoliv mobilního zařízení. Návrhu na nasazení platební brány a její problematice se budu věnovat v kapitole 3.9 této práce.

Hotspot nabízí ale i další funkcionalitu, která se dá perfektně využít k několika účelům. Jedná se o službu, kdy můžeme vymezit určitou adresu nebo i skupinu adres, na které může zákazník přistupovat a volně je procházet bez nutnosti přihlášení se k Hotspotu. Tato funkce se u Mikrotiku nazývá Walled Garden, v překladu něco jako oplocená zahrádka. V jádru to přesně vystihuje podstatu této funkce. Uživatel může procházet pouze povolené adresy zadané v sekci Walled Garden. K tomuto nastavení je možné použít i různé masky, pomocí kterých můžeme v adrese zastoupit jeden nebo více znaků a vložit tak pomocí jednoho záznamu více podstránek nebo sekcí určitého webu najednou. K zastoupení více znaků zde slouží symbol „*“ zatímco pro zastoupení jednoho znaku symbol „?“. Tato funkce se dá využít u obou variant Hotspotu, ať už je připojení zdarma nebo za poplatek. U zpoplatněné verze se dá opět využít Walled

Garden k reklamním účelům, kdy můžeme zpřístupnit bezplatně např. web naší firmy. U verze zdarma se dá naopak skvěle využít např. pro umožnění přístupu na web restaurace, kde si zákazník může prohlédnout denní menu, či stáhnout jídelní a nápojový lístek.

3.3 Typy řízení Hotspotu

[33] Při výstavbě složitější infrastruktury pro Hotspot bychom si měli nejprve zpracovat návrh dané infrastruktury. Podle něj se můžeme dále rozhodnout, jaký typ sítě pro nasazení Hotspotu zvolíme. Jsou dvě cesty stavby sítě, kterými se můžeme vydat. První možností je centralizovaná síť, tudíž síť s veškerým řízením v jednom centrálním bodě (na jednom zařízení). Druhou možností je stavba decentralizované sítě, kde je každý přístupový bod konfigurován samostatně.

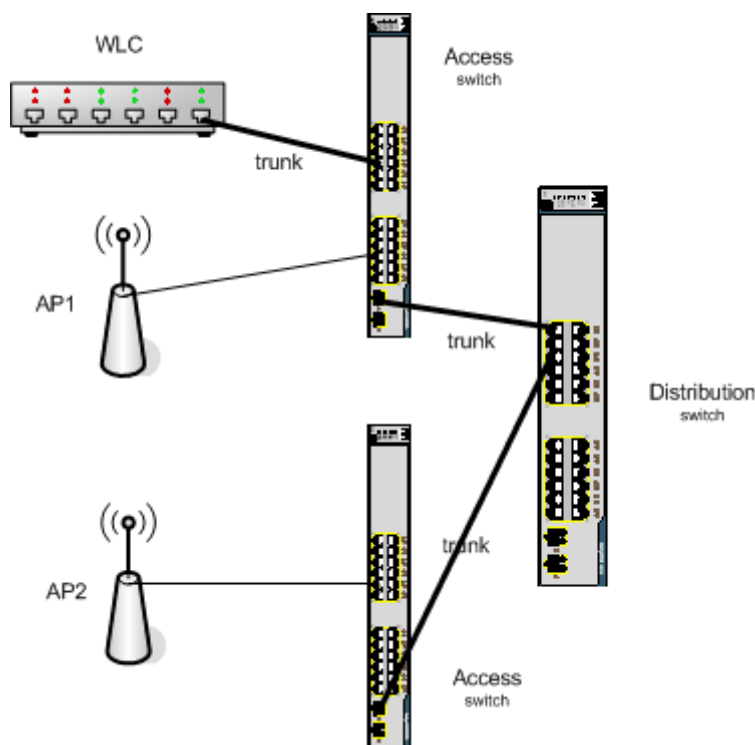
3.3.1 Samostatně spravované AP

U této varianty se chovají jednotlivé AP jako samostatná zařízení s vlastní samosprávou. Výhodou tohoto řešení je, že v případě výpadku či poruchy jednoho ze zařízení zůstávají ostatní AP plně funkční bez jakéhokoliv omezení. To platí v případě, že je infrastruktura dobře navržena tak, aby byly všechny síťové cesty ke všem zařízením duplikované, tudíž v případě výpadku jednoho zařízení může tok dat k ostatním zařízením pokračovat jinou datovou cestou. Na druhou stranu má toto řešení i značnou nevýhodu, která spočívá ve správě takovéto infrastruktury. Všechna zařízení mají svoji vlastní konfiguraci a chovají se jako samostatný člen infrastruktury, tudíž všechny požadavky zákazníka připojeného k danému zařízení se zpracovávají na tomto zařízení a až následně pokračuje komunikace s dalšími prvky v infrastruktuře. To je velice náročné na správu, nastavování a údržbu, jelikož každé zařízení musíme obstarávat zvlášť. Nápomocí nám může být jedině nějaký dodatečný software např. DUDE, který nám může s hromadnou správou více stejných zařízení najednou pomoci.

3.3.2 Centrálně řízený Hotspot

Tato varianta má také své výhody a nevýhody. Každopádně u rozlehlejší sítě o více přístupových bodech bych rozhodně doporučil využít právě centrálně řízený

Hotspot. Jeho hlavní výhodou je, že všechny požadavky se zpracovávají na jednom místě. V síti se nachází jedno zařízení, které se nazývá WLC²⁹, WLAN controller či WiFi controller a to slouží jako hlavní řídicí prvek. WiFi controller zpracovává jak veškeré požadavky týkající se zabezpečení a přístupu klientů do sítě, tak i centrální správu konfigurace. Všechna ostatní zařízení se totiž přepnou do režimu pouhých vysílačů, kdy tato zařízení pouze zprostředkovávají přenos signálu, ale veškeré požadavky přeposílají právě na WiFi controller.



Obrázek 3.1 Centrálně řízený Hotspot s využitím WLC [22]

Některé WiFi controllery dokonce umožňují kontrolovat všechna vysílající AP a rozdělovat dle pokrytí jejich vysílací výkon tak, aby docházelo k co nejideálnějšímu pokrytí s minimálním rušením. Také zprostředkovává roaming při přechodu připojeného zařízení z území jednoho vysílače do území jiného tak, aby nedošlo k žádnému výpadku např. při hlasovém hovoru, kdy by výpadek znamenal přerušování spojení. Pokud potřebujeme provést jakoukoliv změnu nastavení konfigurace, stačí ji provést právě pouze na WiFi controlleru. Nevýhodou je, že funkčnost celé sítě je životně závislá právě na WiFi controlleru a při jeho poruše či výpadku je naše síť zcela

²⁹ Wireless Lan Controller

nefunkční. Toto se dá řešit jedině záložním WiFi controllerem, který v případě výpadku původního nahradí jeho funkci.

Další výhody, které může WiFi controller nabízet:

- Možnost vysílání více virtuálních sítí – oddělení hostů
- WIDS³⁰ – systém pro odhalování a prevenci útoků na bezdrátovou síť
- PoE³¹ - porty pro přímé napájení AP po ethernetu

3.4 Zabezpečení Hotspotu

V této části se budu zabývat problematikou zabezpečení bezdrátového Hotspotu a vlastně obecně bezdrátových sítí – WiFi. Zabezpečení u těchto sítí je zpravidla daleko složitější, než u sítí metalických či optických, jelikož k přenosu dat dochází právě prostřednictvím radiových vln ve vzduchu. Tyto vlny jsou na rozdíl od metalických či optických sítí snadno přístupné komukoliv a odkudkoliv v dosahu vyzařování vysílacího WiFi zařízení. Jelikož každý přístupový bod (vysílací zařízení, přes které se klient připojuje do sítě) vysílá na nějakém kanále, který se v čase nemění, je odposlech dat z takovéto sítě ještě daleko snazší. Je pravda, že existují zařízení, která umožňují automaticky analyzovat a vyhodnocovat vytíženost daných kanálů (frekvencí) v té dané oblasti, kde se nachází, a podle toho zvolit kanál, který je nejméně vytížen. K tomu ovšem dojde pouze při restartu sítě, či zařízení, nikoliv v průběhu přenosu, či za běhu zařízení. Při změně kanálu by totiž došlo ke krátkodobému výpadku přenosu, což si většinou nemůžeme z technického hlediska dovolit. A jak z výše popsaných problémů již vyplývá, je odposlech nezabezpečeného WiFi signálu snadný asi jako poslech rádia, proto bylo vyvinuto několik standardů a metod pro zabezpečení těchto sítí. V následující části jednotlivé možnosti a jejich kombinace podrobně popíši a řeknu, k čemu se ta která technologie hodí či naopak nehodí.

³⁰ Wireless Intrusion Detection System

³¹ Power over Ethernet

3.4.1 Šifrování přenosu

Jednou z úplně základních ochran proti vniknutí do bezdrátové sítě je právě zašifrování přenášených dat. V následující části proberu, jaké jsou možnosti zabezpečit naši síť právě pomocí šifrování a jaké jsou výhody a nevýhody jednotlivých možností.

3.4.1.1 WEP

[27], [28] a [37] WEP³² je jednou z prvních rozšířenějších technologií, kterou lze použít na šifrování dat a autentizaci. Tato technologie se stala v roce 1997 standardem zabezpečení bezdrátových sítí 802.11. WEP funguje na linkové vrstvě, kde šifruje spojení pomocí šifry RC4. Při volbě WEP šifrování si můžeme vybrat z více verzí klíčů. Nejkratší 64bitový, delší 128bitový a v některých zařízeních dokonce 256bitový klíč. Například 64bitový klíč se skládá z 40bitového klíče, ke kterému je připojen 24 bitový inicializační vektor. Obdobně je tomu i u ostatních klíčů. Aby nedošlo k poškození dat, ověřuje WEP integritu přenesených dat pomocí kontrolních součtů CRC-32.

WEP podporuje, jak už bylo zmíněno, i autentizaci. Autentizace probíhá pomocí sdíleného klíče, kdy přístupový bod odešle klientovi text, klient jej zašifruje pomocí svého klíče a odešle zpět na přístupový bod. Ten se zprávu pokusí dešifrovat a porovnat s původní odeslanou. Na základě tohoto porovnání komunikaci buď povolí, nebo zamítne. Tato autentizace může být při využívání WEP vyřazena a používat pouze šifrování bez autentizace – tzv. Open system authentication. Pokud jste nuceni využívat zabezpečení přenosu pomocí WEP, doporučuje se autentizaci pomocí sdíleného klíče vypnout. Je to totiž snadný způsob pro útočníky, jak se nabourat do takovéto sítě. Při odposlechu přenosu autentizace se dá zjistit právě tento sdílený klíč. Jelikož WEP poté používá pro šifrování stejný sdílený klíč, jako byl použit pro autentizaci, je zabezpečení prolomeno snáze, nežli při vypnuté autentizaci. Tak jako tak je tato ochrana již slabá a neúčinná a doporučuji ji vyměnit za nějakou momentálně na trhu dostupnou účinnější ochranu.

V dnešní době je tato technologie již zastaralá a překonaná. Již od prvního prolomení v roce 2001 existují algoritmy a postupy, jak se dá tato ochrana během pár

³² Wired Equivalent Privacy

minut prolomit, a to dokonce i z mobilního zařízení. Přesto ji dnes ještě spousta uživatelů využívá, ať už z nevědomosti jejího snadného prolomení, či lenosti nastavit zařízení na jiný systém zabezpečení. Přesto, že je v dnešní době tato technologie již zastaralá, tak ji většina dnešních zařízení podporuje kvůli zpětné kompatibilitě se staršími zařízeními.

3.4.1.2 WPA

WPA³³ nastoupilo jako náhrada nebo lépe řečeno záplata za již prolomený WEP. WPA vycházelo z rozpracovaného návrhu standardu 802.11i (známého pod názvem WPA2). Jelikož se jednalo o rozpracovanou verzi, která měla překlenout období mezi prolomeným WEP a ještě nedodělaným WPA2, nesla si tato technologie hodně společného od předchozí technologie WEP.

Data přenášená pomocí WPA jsou opět šifrována pomocí proudové šifry RC4, stejně jako tomu bylo u WEP. Jedním z důvodů je, že bylo potřeba, aby bylo možno provozovat WPA na zařízeních která používala WEP pouhým updatem firmwaru daného zařízení. WPA používá 128bitový šifrovací klíč s 48bitovým inicializačním vektorem, tedy obměněný systém jako používal WEP, ale odolává o něco silnějším útokům. [27] K tomu, aby se tedy zvýšila bezpečnost oproti WEP ještě více, byl zaveden protokol TKIP³⁴, který měl odstranit problém s inicializačními vektory. TKIP protokol zavedl dynamickou správu šifrovacích klíčů, které jsou pomocí něj převáděny mezi klientem a přístupovým bodem, a to jak na začátku komunikace, tak na rozdíl od WEP i v průběhu komunikace. K tomu, aby mohl protokol fungovat, je nasazen na klientovi univerzální démon, tzv. suplikant, který zajišťuje autentizaci a šifrování klíčů pomocí TKIP. U WPA máme možnost volby dvojí autentizace. První možností je tzv. WPA-PSK(Pre Shared Key), v překladu sdílený klíč, což je možnost kterou jsme si již výše popsali. Druhá možnost, kterou WPA nabízí, je autentizace pomocí autentizačního serveru, např. RADIUS serveru, pomocí protokolu 802.1X.

³³ WiFi Protected Access

³⁴ Temporal Key Integrity Protocol

WPA má i vylepšenou metodu kontroly dat. Používá MIC³⁵, konkrétně algoritmus nazývaný Michael. Tato metoda zahrnuje počítadlo rámců, díky kterému chrání síť před napadením pomocí opakování předchozí odposlouchané komunikace.

3.4.1.3 WPA2 – 802.11i

[27] a [37] WPA2, známé také pod názvem standardu 802.11i, který splňuje, se stalo nástupcem předchozího protokolu WPA. Co se týče technologie jako takové, tak se oproti WPA nijak dramaticky nezměnila. Opět máme na výběr ze dvou variant a to sice WPA2-PSK (Pre Shared Key), či enterprise řešení v podobě využití autentizačního serveru, stejně jako tomu bylo u WPA. V případě volby PSK jsou opět přenášená data šifrována pomocí klíče, tentokrát o velikosti 256 bitů. Hlavní rozdíl nastal podporou nového druhu šifrování CCMP³⁶ založeného na AES³⁷, které mělo přinášet silné zabezpečení pro bezdrátové spojení. WPA2 je díky tomuto novému šifrování opět náročnější na hardware a tudíž už nebylo tak snadné jej implementovat pouze pomocí updatu firmware v přístupovém bodu, nýbrž bylo ve většině případů nutné zakoupit nová výkonnější zařízení. Většina zařízení umožňuje stále použití WPA2 se šifrováním TKIP. To ale není doporučeno hned ze dvou důvodů. Prvním důvodem je, že tento typ šifrování byl u WPA již prolomen. Druhým důvodem pak nemožnost využití protokolu 802.11n pro přenos dat v rychlostech větších než 54Mb/s. V dnešní době je WPA2 naprostým standardem a všechna nová zařízení jej musí podporovat.

3.4.2 AAA protokol

Zkratka AAA (Authentication, Authorization, Accounting) je v oblasti zabezpečení velmi často používána. Označuje nám tři základní úkony a to sice autentizaci, autorizaci a účtování. Tento protokol je využíván hlavně v infrastruktuře, kde je potřeba ověřovat uživatele přistupující do sítě a následně jim přidělovat či zakazovat přístup k různým prostředkům a nastavovat jim různá práva či oprávnění. Následně také díky účtování sledovat, které prostředky kdy a jak využívají.

Pro řízení přístupu do sítě se využívá zařízení nazývaného autentizační server. V praxi se dnes většinou využívá řešení pomocí tzv. AAA serveru, který kombinuje

³⁵ Message Integrity Code

³⁶ Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)

³⁷ Advanced Encryption Standard

všechny výše zmíněné funkce – autentizaci, autorizaci a účtování. Je to ideální centralizované řešení pro řízení přístupu, nastavení parametrů různých síťových služeb a tarifkaci. AAA server bychom měli vždy v naší infrastruktuře implementovat jako samostatné zařízení nikoliv jako součást některého síťového prvku. V současné době se využívá většinou jeden ze tří autentizačních protokolů. Prvním nejrozšířenějším protokolem je RADIUS³⁸, který vyvinula společnost Lucent. Druhým rozšířeným protokolem je TACACS+³⁹ vyvinutý firmou Cisco. Poslední protokol nese název Diameter (Diameter base protocol). Diameter vychází z protokolu RADIUS, ale má spoustu zásadních odlišností, díky kterým není s RADIUSem kompatibilní. V následující tabulce je porovnání těchto tří protokolů.

	RADIUS	TACACS+	Diameter
Protokol	UDP	UDP/TCP	TCP/SCTP
Porty	1812 (Autentizace, autorizace) 1813 (Účtování)	49	3868
Autentizace	Pomocí jména/hesla, EAP	Pomocí jména/ hesla, Kerberos	Pomocí jména/hesla EAP

³⁸ Remote Authentication Dial-in User Service

³⁹ Terminal Access Controller Access Control System Plus

Autorizace	Po úspěšné autentizaci může server přidat informaci o autorizovaných možnostech uživatele	Probíhá zcela odděleně	Po úspěšné autentizaci může server přidat informaci o autorizovaných možnostech uživatele
Účtování	Samostatné – lze zaznamenávat přístupy	Probíhá zcela odděleně	Samostatné – lze zaznamenávat přístupy
Bezpečnost	Sdílené heslo + MD5 haš	Sdílené heslo + MD5 haš	IPSec, TLS

Obrázek 3.2 Porovnání AAA protokolů [13]

3.4.2.1 Autentizace

[12] Autentizace v bezdrátových sítích je proces, při kterém dochází k ověření, zdali uživatel či zařízení žádající o přístup do sítě je oprávněným uživatelem dané sítě. Při autentizaci se ověřuje identita uživatele či zařízení a další údaje, kterými jsou např. heslo, token, digitální certifikát aj. Tyto údaje se porovnávají na autentizačním serveru s databází uživatelů a zařízení. Následně pak na základě vyhodnocení přístup do sítě schválí nebo zamítne.

3.4.2.1.1 Otevřený systém (Open system)

[37] Open system je úplně základní autentizační metoda, která je jako jediná vyžadována standardem IEEE 802.11 pro zajištění maximální kompatibility bezdrátových zařízení. Tato metoda ovšem, jak již název napovídá, neposkytuje žádné zabezpečení. Kterýkoliv uživatel či zařízení, které požádá o přístup k síti, je bez jakéhokoliv ověření do sítě připuštěno. Nasazení této metody je tedy vhodné zejména na veřejných místech jako jsou restaurace či kavárny, kde umožňuje snadný a rychlý

přístup k síti pro veřejnost. Další možnost nasazení je také při kombinaci s ověřováním na síťové vrstvě.

3.4.2.1.2 802.1x

[27] a [37] Protokol 802.1x zajišťuje zabezpečení fyzického přístupu do sítě a to jak přes ethernet rozhraní, tak i přes bezdrátový přístupový bod. Při připojení nového zařízení je okamžitě daný port blokován, tudíž není možný žádný přenos dat. Jediná povolená komunikace mezi novým klientem a přístupovým bodem či switchem je prostřednictvím EAP⁴⁰ autentizačního rámce. K tomu, aby mohl být nový klient autentizován, musí mít aktivní program, tzv. suplikant, který vyšle přes EAP protokol žádost o autentizaci na AP server. Tento suplikant je ve verzích Windows od verze XP již standardně nainstalován pro všechny adaptéry. Pokud využíváme starší verzi či jiný systém, kde by suplikant nebyl defaultně nainstalován, musíme využít software třetích stran např. SecureW2 802.1x client od firmy Juniper. Pokud obdrží switch či přístupový bod žádost o autentizaci, přepoše ji na autorizační server, většinou RADIUS server. RADIUS server nemusí být jen jeden, ale může jich být v celé topologii několik. Pokud je záznam o uživateli, který požaduje autentizaci, přítomen na lokálním RADIUS serveru, proběhne jeho ověření přímo zde na tomto serveru. Pokud se na lokálním serveru nenachází, přepoše se žádost přes strukturu RADIUS serverů až na server v jeho domovské síti, kde proběhne jeho ověření. Výsledek ověření, ať už schválení či zamítnutí, je odeslán zpět switchi či přístupovému bodu. Ten na základě tohoto ověření další komunikaci buď povolí, nebo zakáže.

Protokol 802.1x toho ale umí více, než jen autentizovat klienta. Na základě ověření umí přiřadit jednotlivému klientovi přístup do příslušných VLAN⁴¹ (autorizace), či nastavit politiku ohledně množství a rychlosti přenosu dat (úctování).

Už jsme zmínili, že pro požadavky na autentizaci se používá EAP. To je ale pouze autentizační rámec, který využívá pro autentizaci pomocí 802.1x několik různých EAP metod. Zde několik nejvyužívanějších z nich stručně popíšu:

- EAP-TLS (Transport Layer Security) – Tento typ EAP využívá kromě obecného hesla také privátního klíče, který je pro každého klienta jiný. Síla tohoto

⁴⁰ Extensible Authentication Protocol

⁴¹ Virtual LAN

zabezpečení je hlavně v tom, že pokud útočník odhalí heslo, tak se stejně nedokáže do sítě nabourat bez toho, aby vlastnil privátní klíč. Tento privátní klíč ještě může být uložen na čipovou kartu pro ještě vyšší bezpečnost. Toto zabezpečení je považováno za jedno z nejbezpečnějších, ale není už tak běžné jeho nasazení právě z důvodu potřeby privátních klíčů (nejčastěji ve formě certifikátů).

- PEAP (Protected Extensible Authentication Protocol) – Jednoduše řečeno je to chráněný EAP. PEAP zapouzdřuje EAP a používá šifrovaný TLS tunel pro přenos. Tím zvyšuje bezpečnost a nedostatky EAP, které předpokládá chráněné komunikační kanály.
 - EAP-MS-CHAP v2 – Jedna z nejpoužívanějších forem PEAP. Vnitřní autentizační protokol vychází z protokolu od Microsoftu, pod názvem „Microsoft’s Challenge Handshake Authentication Protocol“. Jedním z hlavních důvodů využití je podpora MS-CHAPv2 formátů včetně Active directory. Další předností je nutnost ověření CA⁴². Předtím, než klient odešle serveru svoje autentizační údaje, musí být server ověřen pomocí klientova certifikátu, který je ověřen CA.
- EAP-TTLS (Tunel Transport Layer Security) – Rozšířená verze TLS. Stejně jako TLS se považuje jako velmi bezpečný. Rozdíl oproti TLS spočívá v tom, že si může klient zaregistrovat svůj privátní klíč u nějaké certifikační autority. Tím se usnadní procedura instalace certifikátu u každého klienta. Při ověřování ověřuje certifikační autorita server a naopak klient je ověřen certifikátem u serveru. Pokud vše proběhne v pořádku, je vytvořen „tunel“ pro autentizaci klienta. Autentizace se provede pomocí ověřovacího protokolu přenosem přes tunel, kde je veškerý přenos šifrován.
- EAP-SIM (Subscriber Identity Module) – Slouží spíše pro ověřování v sítích GSM.
- LEAP (Light Extensible Authentication Protocol) – LEAP je proprietární metodou vytvořenou firmou Cisco. LEAP pro svou funkci používá dynamických WEP klíčů a vzájemného ověřování mezi klientem a autentizačním serverem.

⁴² Certification Authority

Toto ověřování se provádí dosti často, přičemž při každém ověření je přidělen nový WEP klíč. Síla této metody spočívá v tom, že by nemělo být snadné WEP klíč odhalit. LEAP nabízí také možnost využívat místo dynamických WEP šifrování TKIP.

3.4.2.2 Autorizace

Autorizace je proces, který následuje po dokončení procesu autentizace, za podmínky, že autentizace proběhla úspěšně. Během procesu autorizace jsou klientovi či zařízení přidělována jednotlivá práva a omezení pro přístup do sítě, jejích segmentů či využívání určitých síťových služeb včetně určení parametrů využívání té dané služby. Mimo to mohou být během autorizace zvažovány další faktory, jakými je třeba datum, čas, počet přenesených dat, zbývající kredit, místo připojení atd., které mohou rozhodnout o tom, zdali bude umožněn přístup k daným segmentům sítě a službám či nikoliv. Díky tomu může nastat i situace, že je uživatel či zařízení v pořádku autentizováno, ale během autorizace mu nebude povolen přístup k využívání daných služeb právě z důvodu nesplnění některého z nakonfigurovaných parametrů. Takové zařízení je tedy sice připojeno do sítě, ale nemůže využívat daných služeb, jelikož nebyly díky autorizaci umožněny.

Parametry, které mohou být nastaveny či přidělovány během autorizace:

- Přístup do určitých segmentů sítě
- Přidělení IP adresy z určitého rozsahu
- Nastavení přenosové rychlosti a QoS
- Délka využívání poskytnuté služby
- Limit na přenos dat

3.4.2.3 Účtování

Účtování je třetí částí AAA protokolu a pro aplikace našeho hotspotu je velice důležité. V rámci účtování je potřeba zaznamenat veškeré relace uživatelů či zařízení včetně jejich délek trvání. Tato data jsou pak využívána zejména k účtování zpoplatněných služeb, např. dle počtu přenesených dat či délky připojení. Mají ale i vedlejší účel. Můžeme díky tomu sledovat vytížení sítě či zvýšenou poptávku po určitých službách v určitou dobu a dle toho síť rozšiřovat či upravovat.

3.4.3 Další možnosti zvýšení zabezpečení

Kromě autentizace a šifrování je možné použít i další metody, které by měly ztížit útočnickovi přístup do naší sítě. Několik z nich podrobněji popíši.

3.4.3.1 MAC autentizace

[29] a [37] Každé zařízení, respektive každý síťový adaptér, ať už je to ethernetový adaptér či bezdrátový adaptér, má svoji unikátní MAC⁴³ adresu stanovenou od výrobce. Díky tomu se nabízí možnost zabezpečení připojení do sítě právě pomocí kontroly těchto MAC adres. Administrátor nastaví na přístupovém bodu seznam MAC adres všech zařízení, která budou mít povolení se k danému přístupovému bodu a následně i do sítě připojit. Každé zařízení, které se bude chtít připojit, bude zkontrolováno na existenci jeho MAC adresy v tabulce povolených adres a v případě shodného nálezu bude povoleno připojení do sítě. V opačném případě bude komunikace odmítnuta. Toto nastavení je také občas známo pod pojmem „Allow list“, což je právě jak překlad napovídá seznam či list adres, které budou mít povolen přístup. Naopak k tomu existuje ještě „Deny list“, který se používá pro blokování určitých adres pro přístup do naší sítě, ať už je to z důvodu potencionálního nebezpečí, či jiných důvodů.

Využitelnost této metody zabezpečení je ale téměř nulová. Pokud propočítáme časové náklady administrátora na nastavení tohoto zabezpečení, zadání všech adres do zmíněného „Allow listu“ a doby potřebné k prolomení této ochrany, dostaneme nemalou hodnotu. Jelikož tato ochrana řeší pouze zabezpečení připojení do sítě, nikoliv šifrování přenosu, je velice snadné odposlouchat z komunikace MAC adresy zařízení, které spolu již v dané síti komunikují a použít jednu z MAC adres na svém vlastním bezdrátovém adaptéru. Tomuto úkonu se říká klonování MAC adresy. Celý tento proces zabere méně než 1 minutu. Proto shledávám tuto ochranu za velmi slabou a nerentabilní na nasazení.

⁴³ Media Access Control

3.4.3.2 Skrytí SSID

SSID⁴⁴ je identifikátor každé vysílající bezdrátové sítě. Pokud se chceme připojit k nějakému přístupovému bodu, vyhledáme nejprve všechna dostupná zařízení, zobrazí se nám názvy (SSID) všech dostupných sítí a z nich si vybereme, ke které se chceme připojit.

[37] Jednou z možností, s kterou výrobci přišli, je možnost vypnutí broadcastu SSID. Jinými slovy, zakážeme vysílání informace o tom, že ten daný náš přístupový bod existuje. Pro klienta to znamená, že pokud se k dané síti chce připojit, musí znát SSID té dané sítě a ručně ho pro svůj adaptér nakonfigurovat k používání, což je pro uživatele laika již kolikrát nepřekonatelná překážka.

Pokud se na to podíváme ale z druhé strany, tedy v roli útočníka, je tato ochrana opět bezvýznamná, možná dalo by se říci i nebezpečná. Důvodem je, že každý přístupový bod vysílá broadcasty pomocí pěti mechanismů. Jedním z nich je broadcast SSID, který máme možnost vypnout. Úmysl byl takový, aby to znesnadnilo útočnickovi vyhledání či vůbec zjištění existence naší sítě bez znalosti jejího SSID. Skutečnost je ale jiná. Pokud zakážeme broadcast SSID, stále ale přístupový bod vysílá další čtyři typy broadcastů. A to sice: probe požadavky, probe odpovědi, požadavky na asociaci a požadavky na reasociaci. Tudíž jsme zakázali pouze jeden broadcast z pěti a zbylé čtyři broadcasty se dají i nadále vesele odposlouchávat. Navíc klient, který se připojuje k danému přístupovému bodu, odesílá SSID ve formě obyčejného textu bez jakéhokoliv šifrování – opět velmi snadné odposlechnout.

Shrnutím je tato ochrana spíše na škodu než pro užitek. Krom výše uvedených nebezpečí je ještě často příčinou problémů s WiFi roamingem při přechodu z jednoho přístupového bodu na jiný.

3.4.3.3 Deaktivace DHCP

Další z možností jak zabezpečit zařízení je deaktivování DHCP⁴⁵ protokolu. Pokud se klient připojí k síti, vyšle broadcast s dotazem na DHCP server v síti. Pokud nějaký DHCP server v síti existuje, odešle klientovi odpověď. Po potvrzení přijetí

⁴⁴ Service Set Identifier

⁴⁵ Dynamic Host Configuration Protocol

nabídky DHCP serveru na přidělení údajů klientovi, odešle DHCP server klientovi všechny potřebné údaje pro komunikaci v síti (IP adresu, masku podsítě, výchozí bránu a adresu DNS serveru/ů). DHCP server značně usnadňuje administrátorům práci s ruční konfigurací každého klienta. Nicméně už jsem slyšel nejednou radu, že pro zvýšení bezpečnosti by se měl DHCP server deaktivovat a vše nastavovat ručně. Mělo by se tím teoreticky ztížit útočnickovi nabourání do naší sítě.

Praxe je ale jiná. Ve skutečnosti přiděláme deaktivaci DHCP serveru jen spousty práce administrátorům, zatímco pro útočníka je obejití takovéto překážky otázkou jedné minuty. Při troše základního vzdělání v oblasti sítí není takový problém si zjistit do minuty schéma sítě a přidělit si nějakou IP adresu z rozsahu ručně. Tudíž tento postup považuji spíše za neúčinný nežli užitečný zejména, vezmeme-li v potaz čas investovaný do ručního nastavování všech klientů. Tak velké úsilí a časová náročnost se nám rozhodně neodrazí na kvalitě zabezpečení dané sítě.

3.5 Kvalita služeb - QoS

[14] a [36] Kvalita služeb bývá obvykle označovaná zkratkou QoS (Quality of Service). Jak už název napovídá, QoS nasazujeme všude tam, kde je zapotřebí zajistit nějakou stálou kvalitu určité služby nebo více služeb. Například některé aplikace vyžadují ke své správné funkčnosti nepřetržitý přísun dat dostatečnou rychlostí a bez většího omezení. Mezi takové aplikace můžeme zařadit například VoIP⁴⁶, video hovory, online realtime počítačové hry či přenosy velkého objemu dat. Pokud by se nám kupříkladu u VoIP nedostávalo dostatečně rychle potřebné množství dat, dojde k vypadávání hovoru, až k úplnému přerušení spojení, což je samozřejmě vysoce nežádoucí. Analogicky tomu je i u video hovoru či videokonference, která je na přenos dat ještě náročnější a při poklesu kvality spojení se okamžitě dostavuje „trhání“ obrazu, následně i přerušení spojení. Důležité je však ještě upozornit na fakt, že QoS nám nevyřeší problém pomalého připojení či špatného signálu z důvodu rušení. Pokud disponujeme nedostačující rychlostí linky pro daný počet uživatelů, poté bude docházet ke ztrátě kvality služeb ať už s aplikací nástrojů QoS či nikoliv. QoS nástroje nám pouze pomáhají řešit náhlé dočasné problémy se zahlcením linky či s rizikem jejího brzkého přetížení.

⁴⁶ Voice Over Internet Protocol

QoS se uplatňuje v mnoha různých odvětvích. Od GSM sítí přes sítě metalické, optické a jiné až po sítě bezdrátové, v našem případě WiFi. QoS pro bezdrátové sítě je částečně odlišné než QoS pro metalické či optické sítě. Musíme brát v potaz, že u bezdrátových sítí je přenosným médiem pouze vzduch a radiové vlnění, které je náchylné na rušení a šum způsobené všemožnými okolními vlivy. Ať už se budeme bavit o stálých omezeních, mezi které řadíme různé fyzické překážky, jako jsou budovy či porost, či o různých proměnlivých jevech, jako je počasí či elektrostatika ve vzduchu, to vše má na přenos signálu velký vliv.

3.5.1 Parametry využívané kvalitou služeb

K tomu, abychom dosáhli potřebné kvality služeb pro určité aplikace, nabízí QoS několik hlavních nástrojů, pomocí kterých se naše požadavky dají realizovat. QoS nástroje následně ovlivňují kvalitativní parametry přenosu. Seznam těchto parametrů je následující:

- Delay – koncové zpoždění
- Jitter – kolísání velikosti zpoždění
- Packet loss – ztrátovost paketů
- Bandwidth – šířka pásma

Princip činnosti těchto parametrů je popsán již v kapitole 2.2 zabývající se přenosovými parametry bezdrátových sítí.

3.5.2 Standard IEEE 802.11e

Původní specifikace IEEE 802.11 protokolu pro přístup k médiu (rádiovému kanálu) umožňovala pouze dva režimy komunikace a to sice DCF a PCF. Ani jeden z těchto režimů ale neumožňuje rozlišovat typy provozu, tzn. uplatňovat QoS.

Z tohoto důvodu byl v roce 2005 schválen IEEE 802.11e jako standard a nastoupil jako doplněk standardu 802.11. Tento standard definoval rozšíření pro umožnění zavedení QoS pro bezdrátové sítě a zařízení. Mezi uvedená rozšíření patřilo vylepšení MAC podvrstvy linkové vrstvy, což umožňovalo rozšíření podpory kvality služeb a také opravu chyb v téže podvrstvě. Tento standard byl navrhnout opravdu

robustně, aby pokryl veškeré požadavky na kvalitu služeb, ať už se jedná o velké firmy nebo pouze o domácnosti. Jelikož se v praxi ukázalo, že požadavky většiny klientů, které tvořily z valné hromady domácnosti, nevyužívá zdaleka všechn potenciál standardu IEEE 802.11e, byla zavedena již v roce 2004 určitá podmnožina QoS funkcionality nazvaná WMM⁴⁷. WMM je plně kompatibilní se standardem IEEE 802.11e, pouze byla omezena na funkce potřebné pro nejčastěji žádané aplikace bezdrátových sítí. Nejčastěji využívanými aplikacemi, jak už jsem se zmiňoval, jsou VoIP, video hovory, streamované video, hudba, online počítačové hry a další.

3.5.3 Základní architektury QoS

3.5.3.1 Best-effort services

Best-effort services by se dalo přeložit jako metoda nejlepší snahy poskytnout služby. Přesně tak tato metoda i funguje. Vždy se snaží doručit všechny pakety ze zdroje k cíli bez ohledu na to, jaký obsah dané pakety přenáší – video, hlas, data a jiné. Dá se tedy říci, že všechny pakety mají stejnou prioritu a není tedy nijak rozlišováno, zdali se jedná o hlasový hovor se šéfem či streamování videa z webu. Toto nastavení tedy neřeší vůbec žádnou kvalitu služby. Pokud dojde k zahlcení sítě, dojde po vyčerpání kapacity bufferu k zahazování paketů. Chceme-li v síti s nastavenou architekturou best-effort services řešit problém zahlcené sítě, máme dvě možnosti. Jednou z nich je odpojování klientů, kteří síť nadměrně vytěžují neustálým stahováním velkých objemů dat např. přes P2P síť. Takové řešení se ale jen stěží dá realizovat, jelikož dané stanice by byly odpojeny úplně, a tudíž by nemohly využívat ani jinou komunikaci, kterou potřebují jejich uživatelé např. ke svému zaměstnání. Druhou možností je rozšíření šířky pásma. Takové řešení je sice fajn, ale jeho hlavní nevýhodou je finanční náročnost. Není možné neustále rozšiřovat šířku pásma kvůli narůstajícímu počtu uživatelů nadměrně vytěžujících síť stahováním velkých objemů dat. Jedinou výhodou této architektury je snadné nasazení, jelikož nevyžaduje použití žádných nástrojů QoS.

⁴⁷ WiFi Multi Media

3.5.3.2 Integrated services

Architektura integrated services využívá nástroje, které definují signalizační proces. Pomocí něj mohou jednotlivé datové toky požadovat rezervaci přenosového pásma a požadovaného zpoždění. Tato signalizace probíhá od zdroje až k cíli a zajišťuje tedy rezervaci po celé cestě. Aby bylo možné garantovat šířku pásma a požadované zpoždění, musí tato architektura zajišťovat minimálně dvě funkce. První funkcí je Resource reservation (rezervace zdrojů) a druhou je Admission control (řízení přístupu). Resource reservation slouží k signalizaci pro jednotlivé komponenty, kolik pásma a jaké zpoždění je potřeba rezervovat, zatímco Admission control následně rozhoduje, zdali tyto požadavky přijme či zamítne. Tato architektura má ale i své nevýhody, mezi které patří problematická škálovatelnost, kdy rezervace jsou prováděny pro jednotlivý datový tok a pro ten jsou též zasílány periodické obnovovací rezervační zprávy. Řešením je nasazení výkonných zařízení nebo slučování několika zpráv do jedné.

3.5.3.3 Differentiated services

Třetí architekturou a zároveň nejvíce využívanou je differentiated services, která je z hlediska vývoje následníkem architektury integrated services. Tato architektura funguje na principu kategorizace provozu do jednotlivých tříd CoS⁴⁸. Těmto třídám jsou pak následně pomocí nástrojů QoS zajištěny kvalitativní parametry přenosu. Tato architektura je tedy postavena na myšlence preferování určitého provozu před jiným. Z vlastní zkušenosti vím, že je velice užitečné při rozdělování provozu do tříd vyčlenit jednu třídu na tzv. nežádoucí provoz. Mezi takový řadím například stahování přes P2P aplikace. Této třídě přidělím pouze velice omezenou rychlost, aby nedocházelo k nadměrnému vytěžování linky. Tento způsob je daleko efektivnější než úplné zakázání takové třídy, jelikož pak mají uživatelé snahu nějakým způsobem tento zákaz obcházet v podobě nějakého tunelu.

3.6 Platforma Mikrotik

V současné době je na trhu nespočet různých firem, které nabízejí svá síťová zařízení. Jednou z nich je právě lotyšská firma Mikrotik založená v roce 1995 v Rize,

⁴⁸ Class of Service

kteřá se rozhodla jít kompletně svojí cestou. Vybudovala postupně kompletní řešení jak po hardwarové stránce, tak i po softwarové. V současnosti tvoří hardware pro platformu Mikrotik tzv. RouterBOARD, který byl vyvinut v roce 2002, zatímco software, který byl dopracován v roce 1997, se skrývá pod názvem RouterOS. V této kombinaci dohromady tvoří ideální řešení. Síťový operační systém RouterOS, který je vytvořený z hodně modifikované distribuce Linuxu, je šitý na míru pro využití hardwaru RouterBOARDu. Jináč je možné používat RouterOS i na platformě x86, což opět rozšiřuje možnosti jeho využití. Zde ale musíme počítat s tím, že využití hardwaru nebude tak efektivní jako při kombinaci s RouterBOARDem. [15] a [35]

Mikrotik nabývá stále větší popularity i proto, že nabízí velké množství RouterBOARDů, takže se dá najít ideální produkt jak pro menší firmu, tak pro velké poskytovatele Internetu. Hardware RouterBOARDů je snadno modifikovatelný pro dosažení potřeb konkrétního zákazníka. Obdobné je to i se systémem RouterOS, který se dá relativně snadno upgradovat na verzi s rozšířenou novou funkcionalitou. Zároveň nabízí ideální poměr cena/výkon, kdy je v konkurenci o značný krok vpředu.

3.6.1 Obecné představení RouterBOARDů

Platforma Mikrotik nabízí velké množství všech možných RouterBOARDů. Jednotlivé produkty se liší zejména architekturou a také množstvím různých slotů a rozhraní, kterými jsou vybaveny. Následujícími komponentami disponuje většina RouterBOARDů:

- Procesor: většinou Atheros, výjimečně Power PC, MPC, MIPS
- Paměť RAM, nyní většinou typu DDR
- Ethernet porty (Fast nebo Gigabit Ethernet), samostatně konfigurovatelné
- Většina RouterBOARDů nabízí PoE na jednom z portů
- Mini PCI slot, některé jich mají více
- NAND či Flash paměť o různé velikosti
- CF slot
- Napájecí konektor, obvykle s velkým rozsahem napájecího napětí
- Sériový port
- USB porty

Díky různým rozhraním, které RouterBOARDy nabízejí, je možné je rozšířit o další funkcionality např.: WiFi rozhraní, GSM, 3G, ADSL a další. Právě díky těmto modifikacím lze ze zařízení udělat téměř cokoliv, co zákazník potřebuje. Poskytovatelé Internetu využívají hlavně rozšíření pomocí mini PCI slotů, kam se dají vložit různé WiFi karty.

RouterBOARDy jsou prodávány pod různým označením. Většinou se jedná o zkratku skládající se z písmen RB (RouterBOARD) a čísla, za kterým v některých případech následují ještě písmena. Číslice nám určují řadu a konkrétní typ RouterBOARDu, zatímco písmenka nám odlišují rozdíly u modelů, které mají více verzí. Význam jednotlivých písmen je popsán v následující tabulce:

A	Více paměti
H	Vyšší výkon procesoru
G	Gigabit ethernet
U	USB porty
R	Integrovaná bezdrátová karta
N	Podpora standardu 802.11n

Tabulka 3.3 Legenda písmen v označení modelů RouterBOARDů [16]

3.6.1.1 Mini PCI WiFi karty

Na trhu existuje celkem větší množství miniPCI WiFi karet. Přímo Mikrotik má v prodeji okolo 8 typů. Je dobré volit WiFi karty přímo právě od Mikrotiku, vyhneme se tím případným problémům s kompatibilitou. V současné době Mikrotik nabízí modely obsažené v následující tabulce 3.4.

Typ	Obecná specifikace	Čipset	Vysílací výkon	Anténní konektor
R52	802.11 a/b/g	Atheros AR5414	Až 19dBm (80mW)	2x U.FL
R52H	802.11 a/b/g vysoký výkon	Atheros AR5414	Až 25dBm (320mW)	2x U.FL
R5H	802.11a vysoký výkon	Atheros AR5414A	Až 25dBm (320mW)	1x MMCX
R52N	802.11 a/b/g/n	Atheros AR9220	Až 25dBm (320mW)	2x U-FL
R2N	802.11 b/g/n	Atheros AR9223	Až 25dBm (320mW)	2x U-FL
R52Hn	802.11 a/b/g/n vysoký výkon	Atheros AR9220	Až 25dBm (320mW)	2x MMCX
R5nH	802.11 a/n vysoký výkon	Atheros AR9220	Až 23dBm	1x MMCX
R52n-M	802.11 a/b/g/n	Atheros AR9220	Až 23dBm	2x MMCX

Tabulka 3.4 Modely miniPCI WiFi karet Mikrotik [16]

Jak můžeme vidět v tabulce výše, jsou si tyto karty dosti podobné. I tak mezi nimi rozdíly jsou a je třeba dát pozor při výběru na správnou volbu.

3.6.2 Operační systém RouterOS

[34] Jak už jsem zmiňoval, RouterOS je síťový operační systém založený na linuxovém jádře, který je speciálně vyvinutý pro využití hardwaru RouterBOARDu, přičemž ho lze ale provozovat i na platformě x86. Funkcionalita, kterou RouterOS nabízí, je velice široká a dobře konfigurovatelná. Možnost využití či omezení jednotlivých funkcí je určena zakoupenou licencí RouterOS. Mikrotik poskytuje i licenci na vyzkoušení, která je zdarma a také demo licenci. Licence na vyzkoušení má veškerou funkcionalitu, ale její užívání je omezeno na pouhých 24 hodin. Demo verze žádné časové omezení nemá, ale nabídka funkcí, kterými disponuje je značně omezená. Licence jsou rozděleny do tzv. levelů. V současnosti existuje celkem 6 levelů, přičemž level 0 je právě zmiňovaná zkušební licence a level 1 demo licence. Rozdíl mezi jednotlivými licencemi je popsán v následující tabulce 3.5:

Číslo Levelu	0 (zkušební)	1 (Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Podpora při první konfiguraci	-	-	-	15 dnů	30 dnů	30 dnů
Možný upgrade	-	-	ROS v4.x	ROS v4.x	ROS v5.x	ROS v5.x
Bezdrátové AP	24h limit	-	-	Ano	Ano	Ano
Bezdrátový klient a bridge	24h limit	-	Ano	Ano	Ano	ano
RIP, OSPF, BGP protokoly	24h limit	-	Ano *	Ano	Ano	Ano
EoIP tunely	24h limit	1	Neomezeně	Neomezeně	Neomezeně	Neomezeně

PPPoE tunely	24h limit		200	200	500	Neomezeně
PPTP tunely	24h limit	1	200	200	500	Neomezeně
L2TP tunely	24h limit	1	200	200	500	Neomezeně
OVPN tunely	24h limit	1	200	200	Neomezeně	Neomezeně
VLAN rozhraní	24h limit	1	Neomezeně	Neomezeně	Neomezeně	Neomezeně
Aktivní uživatelé HotSpotu	24h limit	1	1	200	500	Neomezeně
RADIUS klient	24h limit	-	Ano	Ano	Ano	Ano
Fronty	24h limit	1	Neomezeně	Neomezeně	Neomezeně	neomezeně
Web proxy	24h limit	-	Ano	Ano	Ano	Ano
Synchronní rozhraní	24h limit	-	-	Ano	Ano	Ano
Aktivní relace user manageru	24h limit	1	10	20	50	neomezeně

Tabulka 3.5 Srovnání licencí Mikrotik RouterOS upraveno dle [16]

3.6.2.1 Management RouterOS

RouterOS je možno spravovat několika různými způsoby. Jako uživatel máme možnost volby ze tří rozhraní a 4 způsobů, přes která se dá RouterOS spravovat. Jedním z primárních rozhraní je připojení přes linkovou vrstvu pomocí MAC adresy. Využívá se hlavně při prvotním nastavení, kdy ještě není nastavena žádná IP komunikace nebo v případě nějaké kolize na třetí vrstvě. V opačném případě je lepší využít jiné způsoby. Pokud máme v síti více zařízení tohoto typu, stává se tento způsob

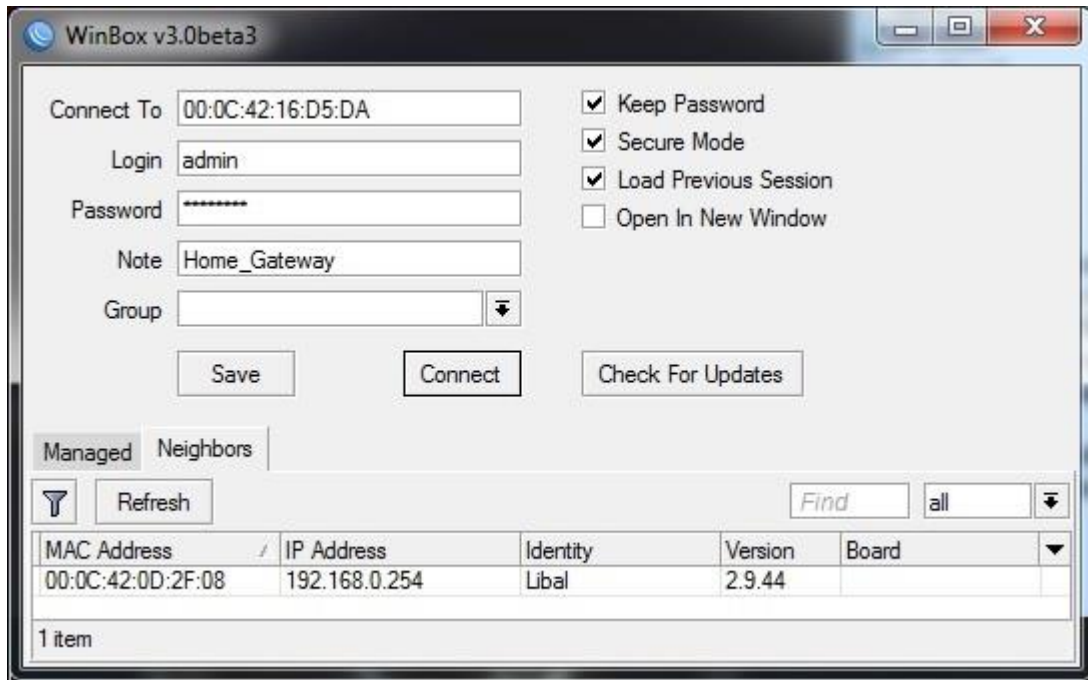
nespolehlivý a komunikace z mé zkušenosti dost často „padá“. Dalšími způsoby, jak se připojit, je přes protokol TCP/IP, HTTP nebo pomocí sériové linky, kterou je většina RouterBOARDů vybavena. K tomu můžeme využít klienta Telnet nebo šifrovaného SSH⁴⁹. Další možností je využití rozhraní jakéhokoliv webového prohlížeče, což nám umožní snadný přístup bez jakékoliv instalace či využití dalších podpůrných prostředků. Pro toto připojení je ale nutná funkční komunikace na třetí vrstvě a přidělená IP adresa k danému rozhraní RouterBOARDu. Poslední možností, která se mi jeví jako nejlepší, je využití grafické konzole WinBox.

3.6.2.1.1 WinBox

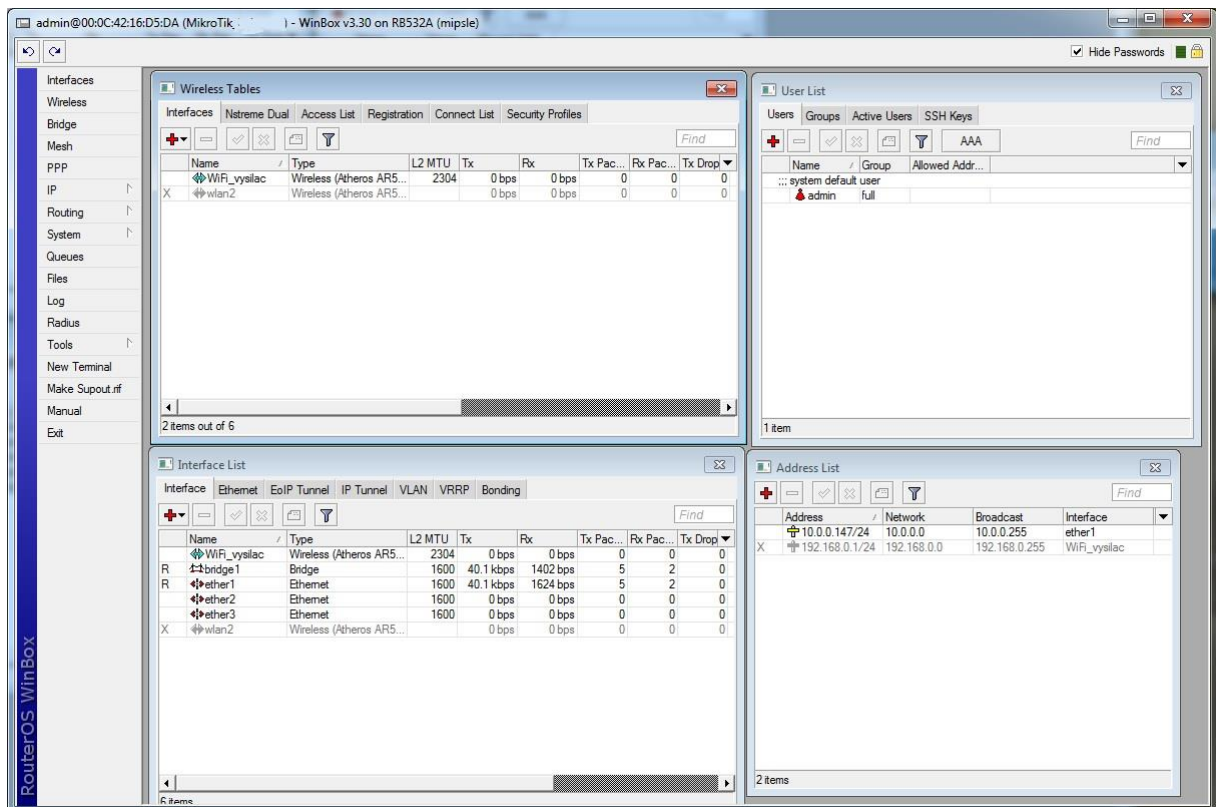
Jelikož, jak už jsem zmínil, WinBox patří mezi nejlepší nástroje, kterými se dá RouterOS spravovat, chtěl bych ho trochu více představit. [34] WinBox patří mezi grafické uživatelské rozhraní, které si svoji oblíbenost vysloužilo jednoznačně svou přehledností. Jedná se o MDI (Multiple Document Interface)⁵⁰ rozhraní, které nám umožňuje nastavovat a ovládat veškeré parametry RouterOS. Vše má svoji hierarchickou strukturu učeněnou do přehledného menu, skrze které je snadné najít rychle a přesně to, co hledáme. Ve stejné hierarchické struktuře se nacházejí i textové příkazy, které vlastně kopírují funkcionalitu jednotlivých položek grafického rozhraní WinBoxu. WinBox umožňuje připojení přes linkovou vrstvu pomocí MAC adresy nebo pomocí protokolu TCP/IP.

⁴⁹ Secure Shell

⁵⁰ V okně aplikace je možné mít otevřených více podoken, přičemž v každém můžeme mít zobrazena jiná data týkající se dané aplikace, v tomto případě konfigurace a stav RouterOS



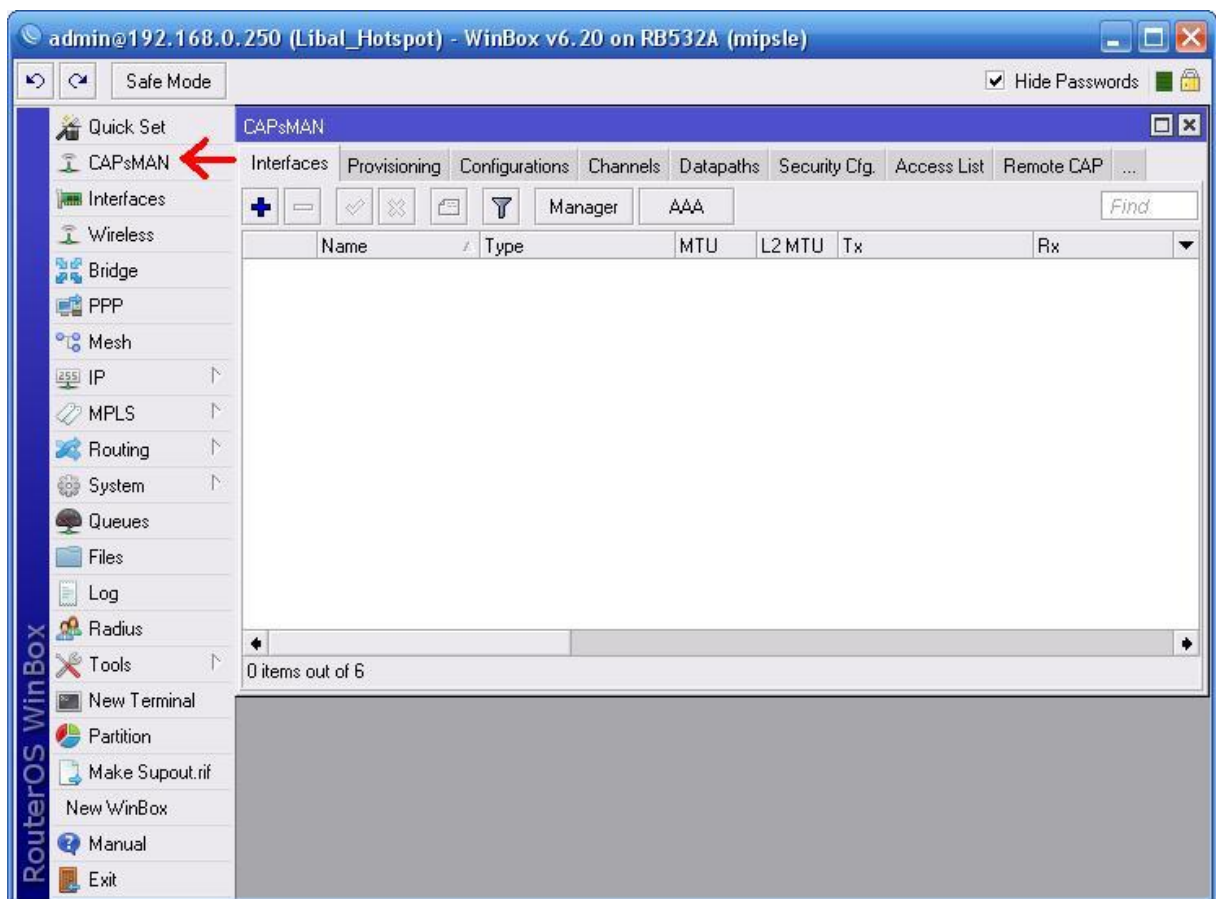
Obrázek 3.6 Přihlášení do WinBox



Obrázek 3.7 Prostředí WinBoxu

3.6.3 Centrálně kontrolované přístupové body - CAPsMAN

CAPsMAN⁵¹ slouží k vytvoření centrálně řízené sítě na platformě Mikrotik. Po instalaci a nastavení CAPsMANu je veškerá konfigurace AP či autentizace uživatelů řízena právě CAPsMANem. Výhodou oproti jiným platformám je, že CAPsMANem, který plní jakousi funkci controlleru, může být jakýkoliv RouterBOARD. Není tedy potřeba kupovat speciální sofistikované zařízení, které by sloužilo extra pouze pro účel controlleru. Jedinou podmínkou, kterou musí RouterBOARD splňovat, aby se mohl stát CAPsMANem je, že musí mít instalovaný RouterOS verze 6.11 nebo vyšší.



Obrázek 3.8 Správa CAPsMANu v RouterOS

⁵¹ Controlled AP System Manager

V momentě kdy určíme, které zařízení bude CAPsMAN, nastavíme ostatní zařízení jako tzv. CAP⁵². CAP pouze zprostředkovává bezdrátovou konektivitu pro uživatele a šifrování či dešifrování bezdrátového přenosu na linkové vrstvě. CAPs mohou komunikovat s CAPsMANem na linkové vrstvě pomocí MAC nebo na síťové vrstvě pomocí IP protokolu. Pokud zvolíme možnost propojení pomocí MAC, nepotřebujeme provádět žádnou IP konfiguraci na CAPs. Podmínkou ale je, že všechna zařízení musejí být ve stejném segmentu linkové vrstvy (nezáleží, zdali ve fyzickém nebo virtuálním za pomoci tunelů). Pokud zvolíme druhou možnost propojení na třetí vrstvě, musí být jednotlivá zařízení dosažitelná prostřednictvím IP protokolu. V tomto režimu může projít komunikace NATem, je-li to zapotřebí. Pokud nejsou CAPs a CAPsMAN ve stejném segmentu linkové vrstvy, pak musí být v CAPu nastavena IP adresa CAPsMANa.

Pozor si musíme dát i na to, že ve výchozím nastavení nejsou data klienta na připojení přeposílána CAPsMANovi nijak zabezpečena. Pokud chceme toto spojení zabezpečit, musíme nastavit použití IPSec⁵³ nebo šifrovaného tunelu.

3.7 Další platformy

Hotspot můžeme provozovat na několika různých platformách. Na rozdíl od jiných funkcí, funkci Hotspotu ale nenabízejí téměř žádné domácí směrovače, musíme tedy zabrousit mezi nějaká inteligentnější a dražší zařízení. Vybral jsem některé platformy, které nabízejí možnost provozování Hotspotu a porovnám jejich výhody a nevýhody oproti platformě Mikrotik.

3.7.1 Platforma Cisco

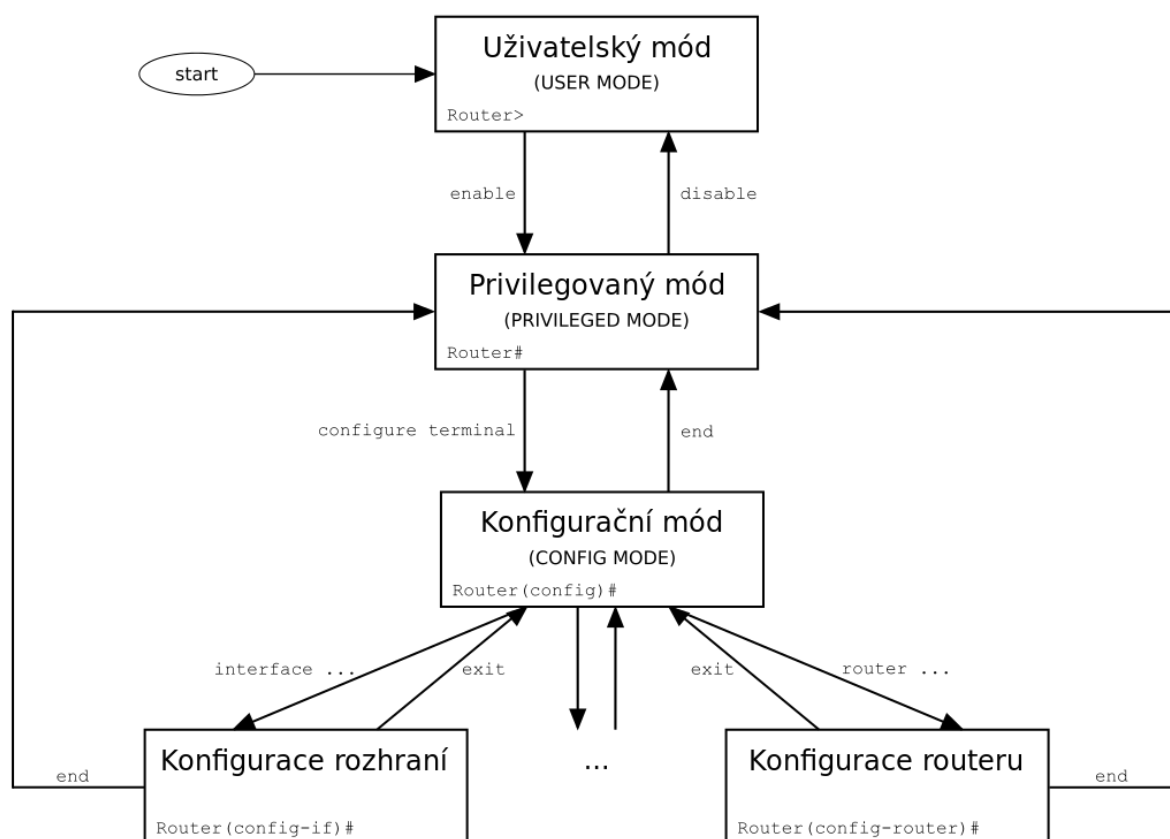
Cisco je jednou z největších firem prodávajících síťové prvky a dokonce celá komplexní řešení infrastruktury pro malé, střední i velké korporace. Jelikož mají ohromné zastoupení na trhu a solidní podporu se svým vlastním školicím systémem, stojí za to provést srovnání, jaké technologie nám nabízí oproti konkurenci.

⁵² Controlled Access Point

⁵³ IP Security – bezpečnostní rozšíření IP protokolu založené na autentizaci a šifrování každého IP datagramu.

3.7.1.1 Cisco IOS

IOS⁵⁴ je operační systém používaný na směrovačích, přepínačích a dalších zařízeních firmy Cisco. Stejně jako je RouterOS stavěný na míru pro RouterBOARD, tak i IOS je stavěný na míru pro Cisco zařízení. Je to velice propracovaný systém, který umožňuje veškeré nastavení zařízení. Konfigurace zařízení se provádí hlavně prostřednictvím CLI⁵⁵ rozhraní. Cisco sice nabízí nástroj GUI⁵⁶ pro zjednodušenou správu základních funkcí zařízení, ale tato aplikace není zdaleka tak propracovaná jako např. WinBox u Mikrotiku. Veškerá nastavení se tedy provádějí přes CLI. Pokud se ale do CLI rozhraní IOSu trochu vžijete, jeho ovládání je velice intuitivní. Příkazy jsou rozděleny do několika uživatelských módů, kde v každém módu máme k dispozici jiné příkazy týkající se daného módu a s tím spojená i určitá oprávnění, co a kde můžeme měnit.



Obrázek 3.9 Módy CLI rozhraní IOSu [21]

⁵⁴ Internetwork Operating System

⁵⁵ Command Line Interface

⁵⁶ Graphic User Interface

Cisco zařízení mají více typů paměti a odlišný systém aplikování příkazů. Zatímco Mikrotik RouterOS ukládá provedené změny okamžitě do konfigurace, která je platná i po restartu zařízení, Cisco IOS se chová úplně jinak. Veškeré příkazy, které administrátor zadá, jsou sice ihned aplikovány, ale pouze do tzv. „running config“, což je soubor s aktuální konfigurací nahraný v paměti RAM. Do této paměti se kopíruje při každém startu zařízení ze souboru zvaného „startup config“ uloženého v trvalé paměti. Pokud tedy provedeme jakoukoliv změnu a chceme ji zachovat i po restartu zařízení, musíme provést jednoduchým příkazem zkopírování aktuální konfigurace z paměti RAM do trvalé konfigurace.

3.7.1.2 Cisco WLC

Cisco WLC⁵⁷ je zařízení, pomocí kterého můžeme vytvořit centrálně řízený typ bezdrátové sítě pro náš Hotspot. WLC plně přebírá veškerou funkcionalitu, která za normálního stavu probíhá na AP. AP se stanou pouhými vysílači, které jsou ovládány WLC a veškeré požadavky mu přeposílají. Zároveň WLC může monitorovat okolí všech AP a upravovat jejich kanály, výkon a další parametry tak, aby bylo pokrytí signálem co nejideálnější s co nejmenším rušením. Cisco WLC také umožňuje další funkce. Zmínil bych např. možnost napájet prostřednictvím portů připojené AP přes ethernet nebo také automatické udržování verze IOS na všech AP.

3.7.1.2.1 Benefity Cisco WLC

Kromě standardních funkcí, které WLC většinou nabízí, má Cisco ještě některé funkce navíc. Podrobnější popis funkcí vztahujících se k našemu Hotspotu následuje níže.

Cisco HA (High Availability)

High Availability je služba Cisca, která nám umožňuje vložit do infrastruktury dva WLC, přičemž jeden z nich bude v záložním módu nazývaném „Standby“ mód. Standby WLC synchronizuje pravidelně s hlavním WLC počet licencí AP, AP roamingové klíče a status CAPWAP⁵⁸ protokolu. V případě jakéhokoliv výpadku či selhání hlavního WLC ihned převezme jeho funkci a síť funguje plynule dál.

⁵⁷ Wireless LAN Controller

⁵⁸ Control and Provisioning of Wireless Access Points

Cisco AVC (Application Visibility and Control)

Cisco AVC je sada služeb, které dokáží monitorovat a klasifikovat data na aplikační vrstvě. Díky tomu je schopný WLC identifikovat a následně oklasifikovat přes 1000 aplikací. Rozpoznané aplikace, které spadají do naléhavých pracovních aplikací, jsou pak upřednostňovány před aplikacemi ostatními. Krom toho také umožňuje nastavit různé priority QoS pro jednotlivé aplikace či měnit dynamicky síťové cesty v infrastruktuře na základě vytížení jednotlivých cest.

Cisco Bonjour Services Directory

Cisco WLC umožňuje využití mDNS⁵⁹ na druhé vrstvě napříč mezi WLAN, LAN a WAN sítěmi pro funkčnost aplikací Apple.

Cisco CleanAir

V dnešní době se vyskytuje stále více a více WiFi zařízení, ať už se bavíme o velkých vysílačích ISP či malých domácích směrovačích. Mimo WiFi jsou ale i další zařízení, která nějakým způsobem ke své funkčnosti využívají spektrum radiových vln podobné spektru, které využívají WiFi sítě. Tím vzrůstá šance, že bude v některém místě docházet k interferenci vlnění a signál z našeho AP bude narušen. V tu chvíli může dojít v nejhorším případě i k výpadku určitých zařízení připojených k tomuto narušenému AP a technik musí tuto situaci řešit. Problém je, že taková zařízení, která mohou svým fungováním rušit signál našeho AP, nejsou stálá. Neustále se objevují nová a jiná starší naopak zase zanikají. Je proto pro efektivní provoz potřeba monitorovat okolí 24 hodin a reagovat na situaci okamžitě jak nastane. To je přesně to s čím Cisco přišlo pod názvem CleanAir. CleanAir je nová technologie nasazená na Cisco Aironet 3600 a 2600, Cisco WLC, Cisco Prime Infrastructure a Cisco Mobility Services Engine. Tato technologie monitoruje okolní síť 24 hodin 7 dnů v týdnu a detekuje nejen cizí WiFi sítě, ale i zařízení jako jsou mikrovlnné trouby, bezdrátové telefony, rušičky signálu, detektory pohybu, bezdrátové bezpečnostní kamery a další. Objevené zdroje rušení ihned zavádí do interní databáze a určuje jejich lokaci na mapě. Následně podle toho upraví vysílací výkon a parametry AP, které do dané oblasti zasahují tak, aby nedocházelo k interferenci vlnění.[18]

⁵⁹ Multicast Domain Name System

Cisco ClientLink

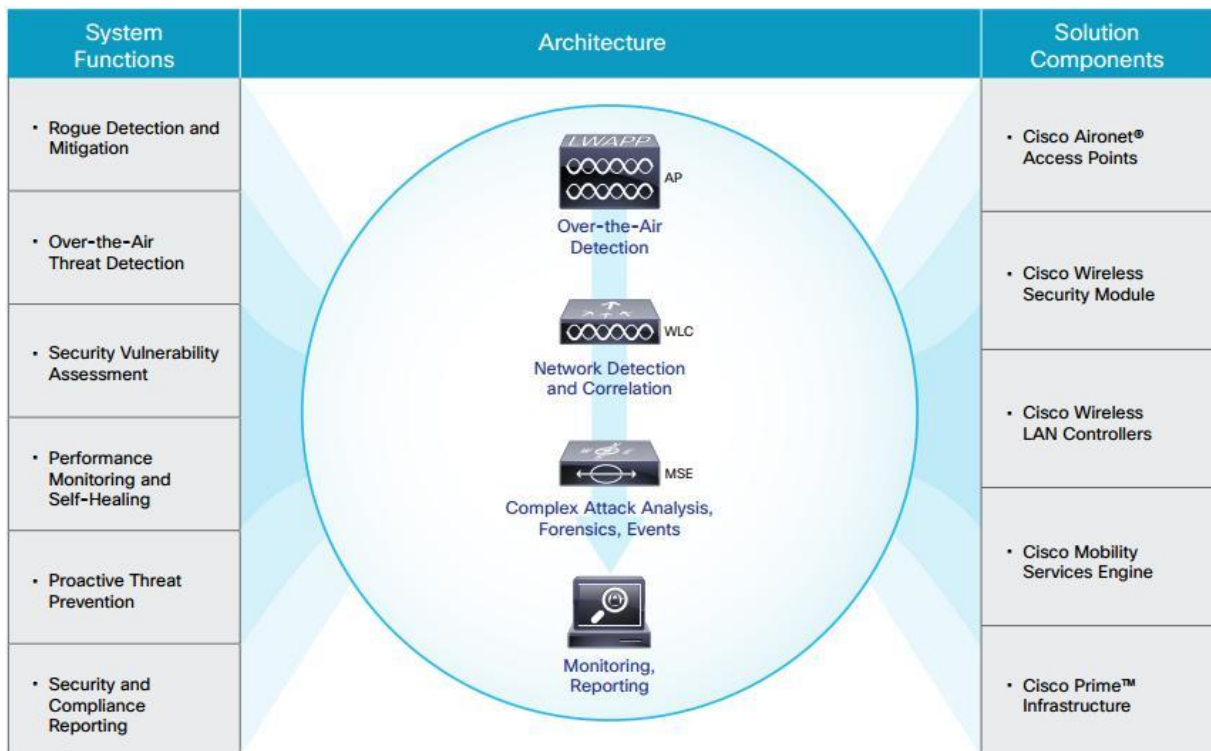
S nástupem standardu 802.11n a novějších nastal problém týkající se vyvážení propustnosti mezi zařízeními s tímto novým standardem a zařízeními se standardy 802.11a/g. V praxi se totiž stává zřídka kdy, že by firma migrovala naráz všechna zařízení na novější standard, tudíž dochází skoro vždy k postupnému obnovování hardwaru kus po kusu. ClientLink je tedy technologie aplikovaná právě v mixovaných sítích standardů 802.11a/g a novějších.

Novější standardy nabízejí daleko větší propustnost oproti starším a tím pádem se stávají starší prvky v síti značnou brzdou celé infrastruktury. Je to dáno mimo jiné i podporou MIMO technologie, která u starších standardů není podporována. Aby tento velký rozdíl byl nějakým způsobem minimalizován, vyvinulo Cisco technologii ClientLink. Tato technologie využívá potenciálu další vysílací cesty směrem ke klientovi se standardem 802.11a/g, která je za normálního stavu nevyužitá. Tyto pokročilé techniky zpracování signálu využívající více „vysílacích cest“ směrem ke klientovi umožňují optimalizovat signál přijímaný klientem při stahování dat bez zpětné vazby. Právě to je hlavní rozdíl oproti standardní MIMO technologii, kde je právě zpětná vazba využita. Díky tomu je možné tuto technologii aplikovat právě pro všechna klientská zařízení se standardem 802.11a/g. Jelikož je tato technologie implementována hardwarově, nesnižuje nijak výpočetní výkon zařízení, a tudíž nedochází k žádnému snížení přenosové rychlosti.[19]

Cisco Adaptive WIPS (Wireless Intrusion Prevention System)

Tato technologie poskytuje pokročilé zabezpečení sítě. Spočívá ve specializovaném monitorování a detekování anomálií vyskytujících se v bezdrátové síti, hlídání neautorizovaného přístupu a jiných RF⁶⁰ útoků. Jelikož monitoring probíhá neustále a je po nějakou dobu zaznamenávána i historie, může podle ní být určena jakákoliv abnormalita, která se v infrastruktuře vyskytne. Systém na tento jev upozorní administrátora a pokud je to možné, tak automaticky aplikuje některé kroky pro zamezení detekovaného útoku. Systém se skládá z mnoha komponent, které navzájem spolupracují a vytvářejí společně velice robustní ochranný systém.[20]

⁶⁰ Radio Frequency



Obrázek 3.10 Funkce a komponenty Cisco WIPS [20]

3.7.2 Platforma Linux

Další platformou, kterou jsem se rozhodl zařadit mezi moje srovnání, je platforma Linux. Důvodem k tomuto rozhodnutí bylo představit jednu z platform, které nabízí bezplatné zprovoznění Hotspotu. Linux je volně šiřitelný operační systém pod GNU GPL⁶¹. To umožňuje pokročilejším administrátorům tento Hotspot různě modifikovat či upravovat k obrazu svému. Na straně druhé zde ale není žádná podpora a vše má v rukou sám administrátor.

Pro zprovoznění Hotspotu na platformě Linux se můžeme vydat několika cestami. První možností je naprogramovat si vše od píky až do konce. Taková varianta nám sice umožní postavit si vlastní Hotspot přesně na míru dle našich představ, na druhou stranu za touto možností stojí velké množství práce a úsilí, které by se dalo minimalizovat pomocí dalších možností. Druhou možností je využít již připravené komponenty a pomocí nich sepsat obslužný program pro Hotspot, který bude tyto jednotlivé komponenty využívat. Toto řešení je střední cesta mezi první a třetí

⁶¹ General Public License

možností. Má své výhody i nevýhody. Mezi výhody patří škálovatelnost a upravitelnost dle našich představ. Je zde ale i značná nevýhoda, která se projevuje zejména při updatu některé z použitých komponent. Např. pokud použijeme některý z nabízených RADIUS serverů jako je FREE RADIUS a dojde k jeho aktualizaci, může dojít k nějaké změně, která způsobí nefunkčnost našeho Hotspotu. Následně je nutný zásah administrátora do naší aplikace a upravit ji tak, aby opět fungovala s novou updatovanou verzí. Třetí variantou je využití již komplexního balíku Hotspotu, který již zahrnuje propojení jednotlivých komponent a napojení na nějaké uživatelské rozhraní. Tato varianta je samozřejmě nejjednodušší a zároveň čas a práci šetřící. Shledávám také výhody této varianty v tom, že pokud dojde ke změně nebo updatu některé z používaných komponent, je následně také updatována tato aplikace. Nabízí již zpracované uživatelské rozhraní, které lze v případě potřeby různě modifikovat.

3.7.2.1 GRASE Hotspot

GRASE je kompletní řešení Hotspotu pro platformu Linux. Projekt je šířen pod licencí GNU GPLv3, a tudíž může být různě modifikován a upravován pro vlastní specifické potřeby. V současné době je oficiálně podporována distribuce Linuxu Ubuntu a Debian.

GRASE Hotspot je vlastně, jak už jsme si řekli, takovým pomyslným lepidlem mezi všemi komponentami s přidaným uživatelským webovým rozhraním. GRASE Hotspot využívá následující komponenty:

MySQL

MySQL je využito jako free databáze, kam jsou ukládána veškerá potřebná data, jako jsou záznamy uživatelů, různých profilů pro účtování atd.

CoovaChilli

CoovaChilli je založeno na populárním, ale již nefunkčním projektu ChilliSpot. Jedná se o softwarový přístupový controller s rozsáhlými možnostmi. Poskytuje

funkce jako captive portal⁶² či walled garden. Pro funkce autentizace přístupu a účtování využívá buď RADIUS server nebo http protokol.

FreeRadius


FreeRadius je jedním z nejrozšířenějších a nejvíce využívaných RADIUS serverů pro platformu Linux na světě. Často se nasazuje i pro komerční využití, jelikož je šířen také pod licencí GNU GPL. Mimo jiné je právě využíván mnoha poskytovateli Internetu a jeho nasazení najdeme i na akademické půdě. Funguje na něm totiž i síť eduroam. FreeRadius je velice rychlý, nabízí spoustu vlastností a je lehce modifikovatelný a rozšiřitelný o další funkcionalitu.

3.7.2.1.1 Rozhraní a funkcionalita GRASE Hotspotu

Jak už jsem zmiňoval, GRASE nabízí webové administrátorské rozhraní. To nám umožňuje upravovat a nastavovat konfiguraci z jakéhokoliv zařízení bez ohledu na operační systém, postačí přítomnost jakéhokoliv webového prohlížeče.

⁶² Captive portal je speciální webová stránka, na kterou je uživatel přesměrován před zobrazením jakékoliv jiné stránky. Většinou se jedná o přihlašovací stránku Hotspotu.

Default - GRASE (v3.7.7.11.306.gc0ceb9b)



Logged in as **guest**

- Status
- Users
- New User
- Batch Users
- Computer Account

- Monitor Sessions
- Reports
- DHCP Leases

- Settings
- Site Logo
- Network Settings
- Coova Chilli Settings
- Portal Customisation
- Ticket Print Settings
- Groups

- Admin Users
- Admin Log

- Logoff

Create User

Username
 Choose a username

Password
 Choose a secure password for the user Average - 57

Group
 Choose the users group (Expiry is based on the user group)

Comment


A comment about the user

When either limit is reached, the user will be cut off. (i.e. after 1hour even if they still have data left)
 A limit of 0 does not mean unlimited, it will immediately lock the user out. To have an unlimited user, the user must be created without any limits.
If a limit is not set here, but is defined for the group, then the group limit will apply

Data Limit (MiB)
 OR Choose a Data
Limit OR Type your own value

Time Limit (Minutes)
 OR Choose a Time
Limit OR Type your own value

[Help Page](#) | [GRASE Hotspot Project](#) | [My Account](#) | [Admin](#)
 © 2014 Timothy White
 Page generated in 0.11 seconds on F4dca06a09a4 using 6.75 MiB mem



Obrázek 3.11 Webové rozhraní administrace GRASE Hotspotu

Administrátorské rozhraní trochu připomíná User Manager od Mikrotiku kombinovaný s některými funkcemi v RouterOS. Nabízí nám jak přidávání jednotlivých uživatelů, tak i jako tvorbu až tisíce uživatelů najednou pomocí dávky. Každému uživateli může být přidělena různá kvóta limitující odběr dat či časový limit připojení. Pokud nechceme nastavovat každého uživatele zvlášť, je zde možnost nastavení skupin, které fungují obdobně jako profily v User Manageru od Mikrotiku. Stačí nastavit limity pro nějakou skupinu, a poté již jen tvoříme uživatele, kteří dědí

parametry námi stanovené skupiny. Jako malá vychytávka je možnost přidání fyzické MAC adresy zařízení, která je ověřována automaticky bez nutnosti přihlašování.

Mezi dalšími možnostmi nastavení GRASE Hotspotu je úprava přihlašovací obrazovky, kde je možné skrýt či zobrazit určité části, či je jinak modifikovat. Dále disponuje také funkcí pro tisk voucherů dočasných uživatelských účtů, kterým se dá nastavit jakákoliv doba vypršení. Po jejím uplynutí je již účet nefunkční. V neposlední řadě je zde jednoduché síťové nastavení, které je potřeba pro chod celého Hotspotu. Zde nastavíme adresy DNS serverů, výchozí brány a také rozhraní přes které přistupují uživatelé (LAN) a rozhraní do sítě Internet (WAN). Nakonec bych ještě podotkl, že je možné vytvořit více administrátorských účtů, pomocí kterých je možné Hotspot přes toto webové rozhraní spravovat.

3.8 Porovnání platforem

V předchozí části jsme si představili zástupce tří pomyslných kategorií bezdrátových sítí pro Hotspot. Tyto kategorie bych popsal následovně:

1. Malé provozovny

Tato kategorie by měla představovat místa, která bude možné pokrýt pokud možno signálem z jednoho až dvou vysílačů a nebude tedy potřeba žádná složitá infrastruktura o více AP. Takovými místy může být třeba malá kavárnička, menší podnik či nějaký menší penzion. Pro nasazení Hotspotu do takovýchto prostor se ideálně hodí finančně nenáročná varianta, která nabídne jednoduchou obsluhu a dokáže obsloužit několik desítek až stovek zákazníků. Zabezpečení se předpokládá na nižší až střední úrovni bez podpory jakýchkoliv rafinovaných monitorovacích prostředků.

2. Středně velké provozovny, větší veřejné Hotspoty

Tato kategorie bude asi zahrnovat většinu případů. Jedná se sice o Hotspoty, které jsou určeny do středně velkých provozoven, jako jsou restaurace, rozlehlé bary, nákupní centra, středně velké firmy, větší hotelový komplex nebo i veřejný Hotspot pokrývající náměstí, letiště a jiná větší veřejná místa. Předpokládá se už v případě nutnosti většího počtu zařízení možnost centrálního řízení a střední stupeň

zabezpečení. Mělo by se jednat o zlatou střední cestu co se výkonu a finančních nákladů týče.

3. Velké korporace, městské Hotspoty

V této kategorii bude poměrem asi nejméně případů. Jedná se totiž o velké firmy většinou s více budovami či odlehlými pracovišti. Mnohokrát se jednotlivá pracoviště nacházejí i v různých zemích a při tom vše musí být perfektně funkční a chovat se pro uživatele transparentně jako jedna síť. Další možností je pokrytí velkých veřejných ploch, např. veřejný Hotspot, který bude pokrývat celé město či obdobně rozsáhlé projekty. U takovýchto sítí se samozřejmě vyžaduje vysoký výkon zařízení, aby bylo možné zpracovávat ohromné množství připojených klientů a i tak poskytovat dostatečnou rychlost připojení a kvalitu služeb. Zabezpečení musí být rovněž na vysoké úrovni, jelikož ve firemním prostředí se jedná o mnoho míst, kde by bylo možné se do sítě nabourat a odcizit tak velmi cenná a důležitá data. Samozřejmostí je předpoklad centrálního řízení s maximální možností kontroly a update jednotlivých AP. Přesto, že do této skupiny bude spadat poměrem asi nejméně zákazníků v porovnání s ostatními skupinami, je jich i tak dost a svým rozměrem a potřebou velkého množství zařízení kolikrát překonají mnoho menších zákazníků dohromady.

	Kategorie 1 Linux GRASE	Kategorie 2 Mikrotik	Kategorie 3 Cisco
Centrální řízení	NE	ANO	ANO
Počet uživatelů	>10000	Dle licence – Level 6 neomezeně	Dle zařízení – 8500 series až 64000
Počet AP	-	Až 2007	Dle zařízení – 8500 series až 6000
Bezpečnost (váha 1-10)	1	5	10
Automatický upgrade firmware AP	-	NE	ANO
Pokročilé monitorování sítě	NE	NE	ANO
Rozšiřitelnost (váha 1-10)	1	7	10
Cenová hladina	Minimální – pouze HW	Střední	Velmi vysoká

Tabulka 3.12 Porovnání několika kritérií u různých platform

Výše uvedená tabulka poskytuje pouze některé základní aspekty pro zevrubné srovnání. Je ale velice náročné, řekl bych až nemožné, udělat do jedné tabulky komplexní srovnání produktů z různých kategorií. Proto chci tabulku doplnit ještě o toto slovní zhodnocení.

Zástupce první kategorie na Linuxové platformě, kterým byl zvolen GRASE Hotspot, je základní variantou, která kromě základní znalosti operačního systému Linux nepotřebuje žádné pokročilé znalosti pro její užívání. Znalost Linuxu je nutná pouze pro instalaci a základní konfigurace, poté se již vše provádí přes již zmíněné webové rozhraní, kde to zvládne i pokročilejší uživatel. Veškerý software je zdarma, a tudíž i náklady na zřízení takového Hotspotu jsou minimální a skládají se v podstatě jen z ceny Hardwaru, na kterém Hotspot poběží. Ten samozřejmě budeme volit dle

náročnosti využití Hotspotu a našich nároků. Na to, že je Hotspot SW zdarma, nabízí plnou základní funkcionalitu Hotspotu s autentizací proti RADIUS serveru. Bohužel nepodporuje centrální řízení.

Zástupcem druhé kategorie je Mikrotik. Mikrotik je v poslední době velice oblíbená platforma a její nasazení stále narůstá. Důvodem je velice dobrá škálovatelnost a možnost upravit jakékoliv zařízení téměř pro jakýkoliv účel. Zároveň je šikovně vymyšlený i systém licencování, kdy v případě, že již vlastníme Hotspot a zjistíme, že nám nestačí počet uživatelů nebo nám schází nějaká jiná funkcionalita, stačí zakoupit vyšší level licence a HW nám může zůstat stejný. Mikrotik nabízí většinu moderních protokolů a služeb a je plně konfigurovatelný jak přes textové rozhraní, tak přes GUI pomocí zmiňovaného WinBoxu. Ke správě Mikrotiku je ale již zapotřebí určitých síťářských znalostí a naučit se pracovat s RouterOS. Mikrotik podporuje centrální řízení, které je možno aktivovat na jakémkoliv zařízení s RouterOS verze 6.11 a vyšší. Není tedy potřeba zakupovat specializované zařízení pro funkci WLC. Cenou Mikrotik dosahuje některými modely k cenám obyčejných domácích směrovačů, které nenabízí zdaleka takovou funkcionalitu jako platforma Mikrotik. Za vyšší modely si musíme sice trochu připlatit, ale i tak se pohybujeme v řádech tisíců korun. Mikrotik je v současné době asi jednou z nejlepších platform v poměru cena/výkon.

Zástupcem třetí kategorie je velmi známé Cisco. Jedná se o světovou jedničku v prodeji síťových prvků a veškerého síťářského vybavení. Jejich zařízení mají již dlouholetou tradici a jejich technologie prošly mnoholetým vývojem. Cisco nabízí řešení pro jakékoliv potřeby. Zároveň nabízí mnoho funkcí a technologií, které u konkurence nenajdeme - viz.: platforma Cisco 3.7.1. Tyto technologie posouvají tato zařízení na úplně jiný level a nabízí opravdu high tech řešení pro velké firmy a korporace, kde je zapotřebí špičková technologie. Dalším faktem Cisca je, že se musíte již dopředu pevně rozhodnout, co a jak budete stavět. Některá cisco zařízení jsou sice modulární, ale i tak již slouží k nějakému určitému účelu. Samozřejmostí je podpora centrálního řízení, kdy je ale zapotřebí zakoupit některý z WLC, které má Cisco v nabídce. Opět se jednotlivé modely liší parametry a mimo jiné i počtem AP a uživatelů, které je možno obsloužit. To vše si ale musíme zaplatit nemalou částkou, která se pohybuje v desítkách až stovkách tisíc korun.

3.9 Návrh platební brány

Jelikož je v dnešní době Internet dá se říci nezbytností, poptávka po připojení stále stoupá. V domácnostech je Internet téměř samozřejmostí a postupně se rozšiřuje i na veřejná místa. Hodně provozovatelů restauračních a tomu podobných zařízení nabízí přístup k Internetu zdarma jako nadstandardní službu svého podniku. Stále ale ještě jsou místa, kde Internet není a lidé by ho velice rádi využili. Mezi taková patří zejména veřejná místa, jako jsou letiště, nádraží, náměstí atd. Zde ale většinou zřizovatel bezdrátového Hotspotu zamýšlí svůj projekt s vidinou zisku, a tudíž není připojení poskytováno zdarma. Otázkou je, jak vyřešit zpoplatnění připojení k Internetu, které by bylo limitované na určitou dobu. A právě tento problém řeší platební brána.

Platební brána je vlastně jakýsi prostředník mezi databází uživatelů Hotspotu, která je většinou spravována nějakým RADIUS serverem a nějakou institucí zprostředkovávající bezhotovostní platby. Celý systém pak funguje tak, že zákazník si vybere z nabídnutých možností cenu, za kterou si chce zakoupit určitý počet dat či časový limit připojení k Internetu. Poté zvolí variantu platby a zašle požadavek na provedení platby zvolenému subjektu. Pokud subjekt potvrdí provedení platby, je vytvořen účet uživatele na RADIUS serveru a jemu nastaveny patřičné parametry dle typu zvolené varianty při platbě. Následně je uživatel informován o provedení transakce a jsou mu poskytnuty přihlašovací údaje. S nimi se již může uživatel připojit do sítě a využívat služeb, které si zaplatil.

3.9.1 Typy platebních bran

V současné době se naskýtají tři možnosti, jak může zákazník bezhotovostně zaplatit za využití služeb našeho Hotspotu. Postupně rozeberu jednotlivé varianty.

3.9.1.1 Elektronická peněženka

První varianta je velice oblíbená v zahraničí a považuje se i za jednu z nejrychlejších a nejpohodlnějších metod platby. Jedná se o takzvanou elektronickou peněženku. Elektronická peněženka je vlastně taková vaše virtuální peněženka online, do které si např. bankovním převodem pošlete nějaké finance, kterými můžete

následně z této elektronické peněženky platit. Problém v současné době nastává v tom, že je již velké množství provozovatelů elektronických peněženek. Mezi známými elektronickými peněženkami můžeme jmenovat PayPal, PaySec, MoneyBookers nebo nyní PayU využívanou portálem Aukro.cz. K tomu, abychom mohli z dané elektronické peněženky za naše služby zaplatit, musí provozovatel Hotspotu nabízet možnost platby právě danou elektronickou peněženkou. Platba touto metodou je velice rychlá a dá se říci, že i bezpečnější, jelikož nemusíme nikam uvádět údaje o svých platebních kartách od bankovního účtu.

3.9.1.2 Online platební karta

Druhá varianta je platba online platební kartou. V takovém případě musí mít provozovatel Hotspotu sepsanou smlouvu na používání online platebního terminálu. Tato metoda je u nás více populární než elektronické peněženky. Stačí pouze vyplnit číslo platební karty, datum platnosti platební karty a cvc kód a platba může být provedena. Pokud je platba autorizována, opět bude vytvořen účet na RADIUS serveru a uživatel bude informován o provedení platby. Následně mu budou zaslány přihlašovací údaje.

Třetí variantou je možnost platby prostřednictvím SMS zprávy z jakéhokoliv mobilního zařízení. Tato varianta je velice praktická, jelikož dnes téměř každý vlastní mobilní telefon a umí napsat a odeslat textovou zprávu SMS. Jelikož ale existuje několik různých operátorů poskytujících mobilní služby, není možné, pokud chceme zachovat nějaké jednotné telefonní číslo pro platby, navázat kontakt pouze s jedním z nich. Ke zprovoznění této varianty plateb je zapotřebí navázat spolupráci se zástupcem některého z SMS agregátorů, který následně spolupracuje se všemi mobilními operátory. To nám umožní využívat jednotná telefonní čísla pro platby za připojení.

3.9.1.3 SMS platby

Většina SMS agregátorů nabízí dvě varianty SMS plateb. První z nich je označována zkratkou MO⁶³, zatímco druhá možnost se skrývá pod zkratkou MT⁶⁴.

⁶³ Mobile Originated

⁶⁴ Mobile Terminated

První možnost – MO funguje tak, že je započata, jak již název říká, na mobilním zařízení. Po odeslání SMS zprávy je ihned příslušná částka odečtena. Hodnotu SMS můžeme vyčíst z posledního dvojčíslí telefonního čísla, na které SMS zprávu odesíláme. Tato cena je konečná včetně DPH. Pokud bychom chtěli nechávat zákazníkovi zasílat zpětnou SMS s potvrzením o zaplacení, bude cena této SMS účtována provozovateli této služby. Cena této potvrzující SMS se pohybuje v průměru od 1 do 3 Kč.

Druhá možnost – MT funguje naopak tak, že je na mobilním telefonu zakončena. Nejprve zašleme bez ohledu na částku SMS na uvedené telefonní číslo. Po provedení veškeré autorizace je nám zaslána potvrzující SMS. Platba je stržena až v momentě, kdy je nám doručena právě tato SMS, přičemž náklady obou SMS zpráv platí uživatel. Výhoda této metody je v tom, že při jakémkoliv výpadku v komunikaci mezi SMS agregátorem a našim Hotspot systémem nemusíme řešit žádná dodatečná storna odečtené částky, jelikož platba je provedena až po platné autorizaci. Jako bonus je u této metody větší podíl z částky připadající poskytovateli služby.

Celkově se ale moc platba pomocí SMS poskytovateli služby Hotspotu moc nevyplatí, jelikož z důvodu mnoha článků v platebním řetězci je podíl z celkové částky SMS zprávy velice malý.

3.9.2 Návrh na implementaci 1


















Na trhu existuje několik různých poskytovatelů zprostředkování plateb pro náš Hotspot. Po průzkumu několika z nich jsem se rozhodl pro představení jednoho z nich. Je to firma HOTSPOTSYSTEM.COM, která nabízí různé metody Hotspotů a účtování. Mimo jiné dokonce nabízí nějaké varianty free Hotspotů a Hotspotů na vyzkoušení, což ale není náš případ.

HOTSPOTSYSTEM.COM nabízí platbu mnoha různými prostředky a propojení s většinou platforem včetně platformy Mikrotik. Pro implementaci této platební brány nastavíme Hotspot službu na našem Mikrotik zařízení obdobným způsobem, jaký je popsán v praktické části této práce. Rozdílný postup bude následovat v nastavení RADIUS serveru, kde musíme nastavit IP adresy RADIUS serverů provozovatele HOTSPOTSYSTEM.COM. Dále musíme nastavit v sekci Walled Garden adresy serverů, které budou zprostředkovávat platby, aby bylo možné na ně přistupovat i bez

přihlášení k Hotspotu. Posledním krokem je upravení login obrazovky pro možnosti výběru platby za připojení k Internetu. Poskytovatel této platební brány poskytuje značnou podporu a umožňuje také navýšit náš profit z obrátů s narůstajícím počtem uživatelů. Jedná se o skvělé komplexní řešení platební brány, které lze implementovat na spoustu různých platforem za minimální ceny.[23]

3.9.3 Návrh na implementaci 2

[25]Další možností, jak se dá realizovat platební brána pro Hotspot, je upravení a nasazení vcelku nové platební brány s názvem PayU. PayU pronikla na český trh zhruba před 3-4 lety, kdy její rozmach v ČR byl podpořen dražebním portálem Aukro.cz, který začal tuto platební bránu využívat jako jednu z možností online plateb za vydražené předměty či další služby. Tato brána nyní nabízí spolupráci s většinou českých bank a nabízí online platby v reálném čase u většiny z nich. Mimo to samozřejmě podporuje i standardní platbu bankovním převodem, která ovšem není provedena v reálném čase.

Rychlý převod z České spořitelny prostřednictvím Servisu 24			zpracování v reálném čase
Rychlý převod z Komerční banky prostřednictvím internetbankingu			zpracování v reálném čase
Rychlý převod z ČSOB nebo ERA prostřednictvím internetbankingu		ČSOB/ERA	zpracování v reálném čase
Rychlý převod z UniCredit Bank prostřednictvím internetbankingu		UniCredit Bank	PŘIPRAVUJEME
Rychlý převod z GE Money bank prostřednictvím internetbankingu		GE Money Bank	zpracování v reálném čase
Rychlý převod z mBank přes internetové bankovníctví		mPeníze	zpracování v reálném čase
Rychlý převod z Raiffeisenbank přes internetové bankovníctví		ePlatby	zpracování v reálném čase
Rychlý převod z Sberbank přes internetové bankovníctví		Sberbank	zpracování v reálném čase
Rychlý převod z Fio banky		Fio banka	zpracování v reálném čase
Platba kartou prostřednictvím platební brány ČSOB		VISA, MasterCard	zpracování v reálném čase
Platba kartou prostřednictvím platební brány ČSOB		Diners Club	zpracování v reálném čase
Platební řešení PaySec		PaySec	zpracování v reálném čase
Běžný bankovní převod		pro ostatní bankovní ústavy	při odeslání platby do 15:00 prostředky připsány následující den
Platba poštovní poukázkou		složenka	poukázaná peněžní částka je vyplacena zpravidla do tří pracovních dnů ode dne podání
Digitální peněženka pro jednoduché a bezpečné placení - bez hotovosti a platební karty		MasterCard Mobile	zpracování v reálném čase

Obrázek 3.13 Nabídka plateb platební brány PayU

Platební bránu PayU již v dnešní době implementuje spousta elektronických obchodů, které díky ní umožňují zákazníkovi pohodlnější a rychlejší možnost nákupu. Po nastudování implementační dokumentace, kterou PayU na svých stránkách nabízí volně ke stažení [26], se dá PayU implementovat také pro náš Hotspot. Vše je velice pěkně připravené a se základní znalostí nějakého programovacího jazyku není implementace nikterak složitá. Bohužel nebylo možné implementaci v praxi provést,

jelikož PayU nenabízí žádnou zkušební variantu. Za implementaci se platí poplatek ve výši 3900Kč.

3.9.4 Návrh na implementaci 3

Třetí možností, na kterou bych chtěl poukázat, je implementace platební brány za pomoci nástroje User manager na platformě Mikrotik. Jeho podrobnější popis a implementace je rozepsána v kapitole 4.3.1.1. User manager nabízí možnost propojení s platební bránou PayPal. Je nutné mít založený u PayPal účet, který poté použijeme pro naši platební bránu. Uživatelé poté budou moci zaplatit za připojení k Internetu prostřednictvím služby PayPal, kdy po úspěšně autorizované platbě bude odeslán pokyn našemu User manageru pro vygenerování uživatele a přidělení přístupu k Internetu danému uživateli. Tato metoda je velice praktická a ne velmi náročná na implementaci, nicméně omezuje možnost plateb pouze na nabídku PayPal. PayPal ale v současné době nabízí široké množství způsobů, jak zprostředkovat online platbu včetně využití online platebních karet. Jelikož v dnešní době většina lidí vlastní platební kartu, která umožňuje online platby, považuji nasazení této platební brány jako za jednu ze solidních možností.

4 Realizace Hotspotu na platformě Mikrotik

Po teoretickém úvodu a zasvěcení do dané problematiky nadešel čas na aplikování uvedených znalostí do praxe. V následující části se pokusím nastavit hotspotový systém na platformě Mikrotik a propojení s RADIUS serverem, na kterém bude probíhat ověřování uživatelů připojujících se k Hotspotu a nastavení různých kritérií připojení, kterými jsou např.: omezená doba připojení, počet přenesených dat či omezení přenosové rychlosti. Vše budu nastavovat na testovací konfiguraci, která by měla simulovat obdobné nasazení v reálném provozu.

Nejprve představím návrh sítí a popis topologií, které budu implementovat a popíši, kde a jak se taková řešení dají využít. Následně představím jednotlivé hardwarové vybavení, které jsem pro simulaci a konfiguraci Hotspotu využil. Na to naváže kapitola, kde popíši konfiguraci a nastavení na jednotlivých zařízeních a také implementaci s několika různými RADIUS servery. Závěrem otestuji implementované řešení, představím nějaké utility pro testování a porovnáím jednotlivé varianty RADIUS serverů, u nichž shrnu jejich výhody a nevýhody.

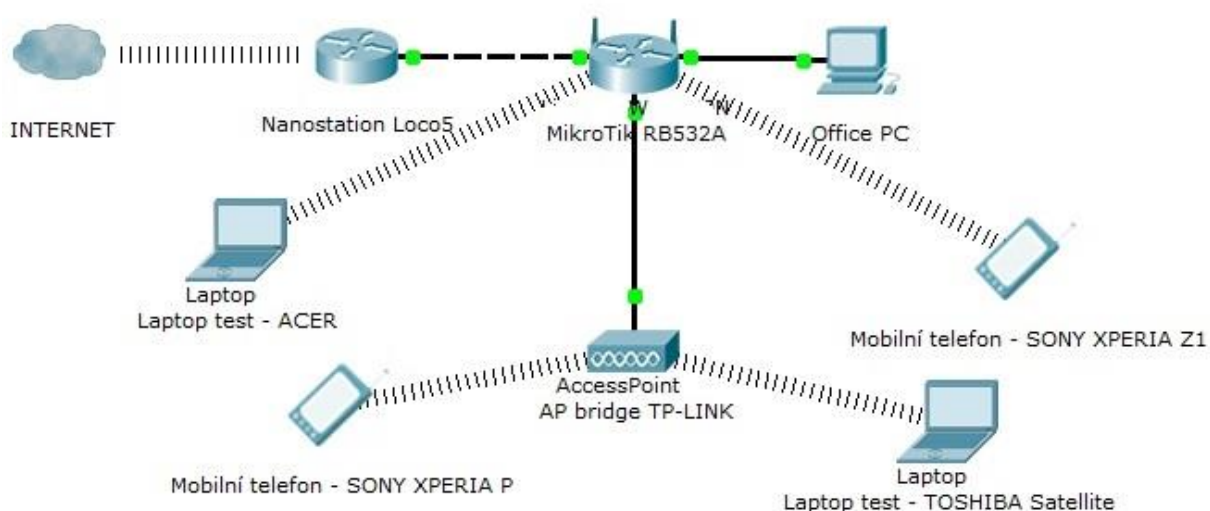
4.1 Návrh sítí

Síť pro implementaci Hotspotu může mít různou velikost. Od malé jednoduché sítě o jednom aktivním prvku až po rozsáhlé komplexní sítě o několika desítkách aktivních prvků. Takové již většinou využívají systém centrálního řízení, aby byl management jednotlivých prvků pro administrátory ulehčen.

Já jsem se rozhodl implementovat celkem dvě hotspotová řešení. První řešení představuje menší hotspotovou síť, kterou jsem vytvářel na zakázku pro restauraci. U druhého řešení jsem zvolil zlatou střední cestu, na které se dá odzkoušet více možností jako například funkce centrálně řízeného Hotspotu. Takto nabrané zkušenosti je možno využít v praxi jak na malé síti, tak na síti velké.

První topologie je tedy navržena pro provoz Hotspotu v restauraci. V současné době má restaurace pouze bezdrátové připojení k Internetu od svého poskytovatele pomocí LocoStation 5 od Ubiquinti. Na tuto stanici je v současné době připojen jeden

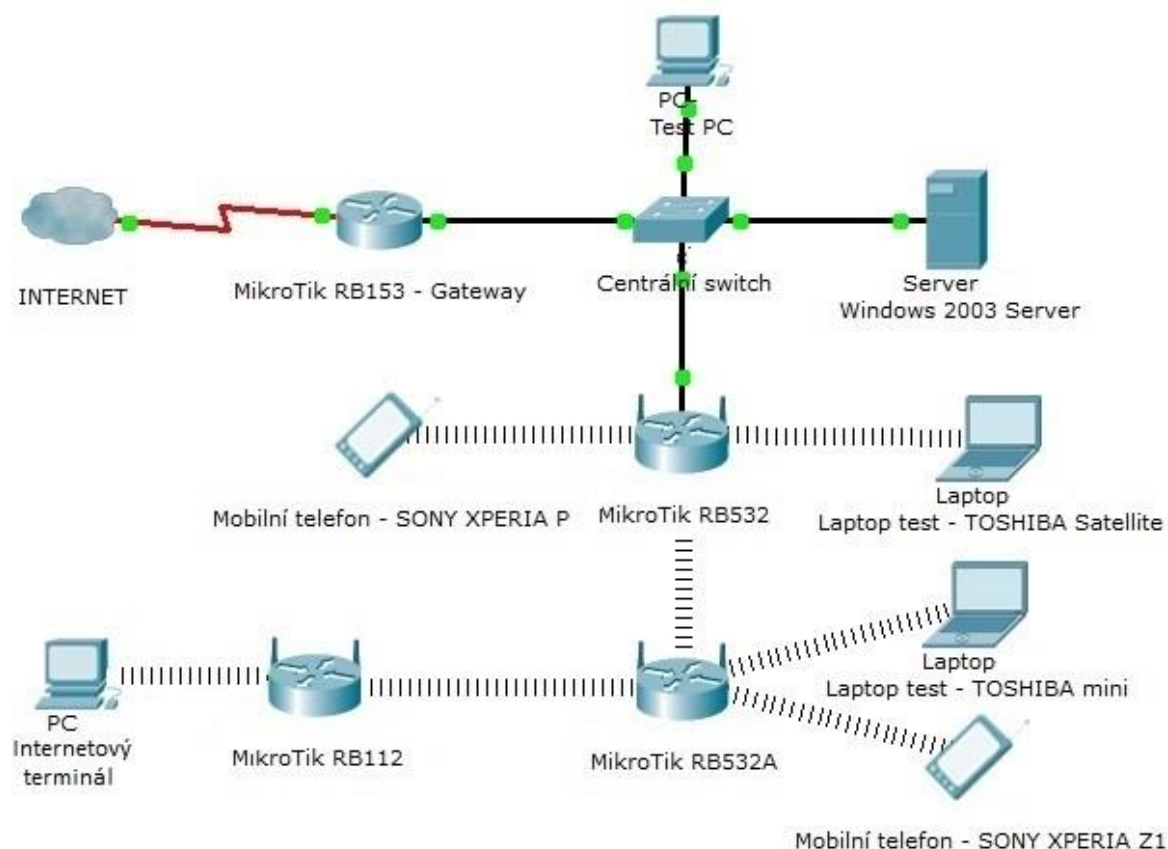
stolní počítač, který slouží pro kancelářské účely restaurace a také jeden přístupový bod TP-LINK, který vysílá v prostoru restaurace a umožňuje návštěvníkův volné a nekontrolované připojení k Internetu prostřednictvím WiFi. Požadavek restaurace byl právě na zavedení Hotspotu, kterým bude připojení kontrolováno. Zároveň si přeje možnost vydávání voucherů, které budou časově či datově omezené. Tyto vouchery budou poté dávat svým zákazníkům v případě dotazu na WiFi připojení. Tímto krokem se omezí možnost případného připojení lidí v okolí, kteří nejsou současnými návštěvníky restaurace a pouze „kradou“ WiFi signál pro své účely.



Obrázek 4.1 Topologie implementované hotspotové sítě pro restauraci

Jak vidíme na obrázku výše, znázorňujícím novou topologii, bude stávající síť rozšířena o MikroTik RouterBOARD RB532A, který nám bude poskytovat veškeré nastavení a funkcionality potřebnou pro zprovoznění Hotspotu. Stávající vybavení se zachová a současně využívaný TP-LINK se použije jako další přístupový bod Hotspotu pro lepší příjem signálu v salóncu. Laptopy a mobilní telefony slouží pro simulaci připojení k Hotspotu zákazníkem a testování ostrého provozu.

Druhá topologie byla zpracována jako návrh na implementaci hotspotové sítě pro poskytovatele Internetu ve městě Trutnov, který chtěl rozšířit své služby zákazníkům o poskytnutí Internetu na několika veřejných místech s velkou koncentrací lidí.



Obrázek 4.2 Topologie implementované hotspotové sítě pro poskytovatele Internetu

Topologie se skládá z celkem čtyř RouterBOARDů Mikrotik, serverového PC, PC pro internetový terminál, dvou laptopů a dvou mobilních zařízení, která slouží zejména pro testovací účely. Celý koncept je vymyšlený tak, aby pokryl tři hlavní části města s velkou koncentrací lidí. Připojení do sítě Internet je řešeno přes výchozí bránu zkonfigurovanou na RouterBOARDu RB153, který bude umístěn v sídle poskytovatele Internetu nacházejícího se téměř u náměstí. Zde bude rovněž umístěn centrální přepínač (switch), ke kterému bude připojen náš testovací počítač, server, případně několik kancelářských PC pro práci zaměstnanců a hlavně přípojka pro spojení s dalším RouterBOARDem RB532. Ten bude umístěn na náměstí a bude sloužit jako jeden z přístupových Hotspot bodů a zároveň také jako převaděč neboli opakovač (repeater) pro přenos signálu do dalšího RouterBOARDU RB532A. Ten bude umístěn v oblasti u autobusového nádraží, kde bude pokrývat nejen samotný terminál a nástupiště, ale i kulturní centrum UFFO a přilehlé budovy soudu, obecního úřadu a banky. Posledním RouterBOARDem je model RB112, který bude umístěn na vlakovém nádraží. Připojen do naší sítě bude prostřednictvím RouterBOARDu RB532A

umístěného na autobusovém nádraží pomocí bezdrátového přenosu. K tomuto RouterBOARDu RB112 bude připojen Internetový terminál, který bude umožňovat uživatelům využití Internetu pro případné vyhledání vlakového spojení či jakékoliv jiné potřeby. Kromě umístěného terminálu samozřejmě nabízí rovněž připojení uživatelů s vlastními zařízeními, která podporují WiFi. V diagramu jsou znázorněna jako koncová mobilní zařízení, která budou simulovat reálný provoz uživatelů a nám budou sloužit jako zařízení testovací.

4.2 Použitý hardware

V této části popíšu jednotlivé komponenty a zařízení, které jsem při implementaci obou topologií použil. Na rozdíl od teoretické části, kde byly uvedeny pouze obecné informace o jednotlivých částech, zde uvedu již konkrétní specifikaci RouterBOARDů, které jsem použil.

4.2.1 RouterBOARD

Dá se říci, že takový hlavní základ druhé topologie tvoří dva celkem výkonné Mikrotik RouterBOARDy s označením RB532, přičemž jeden z nich je v lepší verzi RB532A. Tento typ je rovněž využit v topologii první, kde má hlavní funkci. Jedná se o střední třídu směrovačů z řad Mikrotiku. Specifikace modelu RB532A jsou následující:

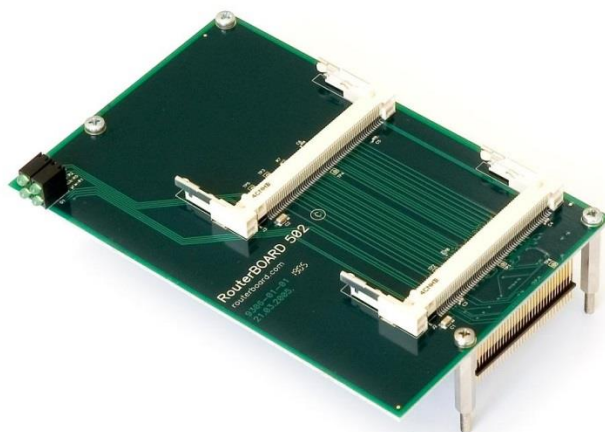
CPU	MIPS32 4Kc based 266MHz (400MHz optional) embedded processor
Memory	64MB DDR onboard memory chip
Boot loader	RouterBOOT, 1Mbit Flash chip
Data storage	64MB/128MB onboard NAND memory chip CompactFlash type I/II slot (also supports IBM/Hitachi Microdrive)
Ethernet	One IDT Korina 10/100 Mbit/s Fast Ethernet port supporting Auto-MDI/X Two VIA VT6105 10/100 Mbit/s Fast Ethernet ports supporting Auto-MDI/X
MiniPCI slot	Two MiniPCI Type IIIA/IIIB slots
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, 2 LED pairs for MiniPCI slots, 1 user LED
Watchdog	IDT internal SoC hardware watchdog timer
Power options	IEEE802.3af Power over Ethernet: 12V or 48V DC mode Power jack/header 6..22V or 25..56V DC jumper selectable

Tabulka 4.3 Specifikace RouterBOARDu RB532A [17]



Obrázek 4.4 RouterBoard RB532A

Tento RouterBoard mimo jiné disponuje také konektorem na základní desce, který slouží k připojení přídatného modulu tzv. daughterboardu. Mikrotik nabízí k tomuto modelu výběr z následujících tří modulů: RB502, RB564 a RB604. Přičemž modul RB502 rozšiřuje RouterBoard o 2 miniPCI sloty, modul RB564 o 4 miniPCI sloty a 6 ethernet portů a modul RB604 o 4 miniPCI sloty. Já jsem pro naše potřeby použil modul RB502, který osadím bezdrátovými kartami, které budou následně napojeny na antény směřující do různých zeměpisných stran.



Obrázek 4.5 Daughterboard RB502

RouterBOARD RB532A s připojeným daughterboardem RB502 dosahuje docela velkých rozměrů, proto jsem byl nucen na něj vyrobit ochrannou krabičku vlastní výroby. Na její výrobu jsem využil starý zdroj ze stolního PC. Case má dobré ochranné vlastnosti a zároveň vysoký stupeň ventilace pro dobré chlazení.



Obrázek 4.6 Ochranný case na RouterBOARD RB532A s daughterboardem RB502

Třetím RouterBOARDem, který představím, je RB112. Ve stručnosti je to méně výkonná varianta RB532, která se také ale prodává s RouterOS licencí level 4. Nabízí jeden fast ethernet port a dva miniPCI sloty pro bezdrátové karty. Je založený stejně jako RB532 na procesoru MIPS32 4Kc s tím rozdílem, že je taktován pouze na 175MHz. Dále disponuje 16MB paměti RAM a 64MB NAND paměti. Je to dostačující zařízení pro AP, opakovač či koncovou stanici.

4.2.2 MiniPCI WiFi karty

Jak už bylo zmíněno v kapitole 3.6.1.1 pojednávající o obecném přehledu miniPCI karet pro platformu Mikrotik, je jich celá škála. Já jsem pro tuto testovací sestavu využil karty typu R52, na které jsou připojeny propojovací pigtaily RG178U – RSMA female. Tyto karty jsou dobrou volbou, pokud bychom chtěli využívat v budoucnu místo pásma 2,4GHz pásmo 5GHz.

4.2.3 Server PC

Mimo samotných směrovačů a jiného síťového vybavení byl využit i jeden starší stolní počítač, který byl využit jako server. Jako operační systém byl nainstalován Windows 2003 Server Enterprise edition. Windows Server platforma byla zvolena hlavně z důvodu využití této platformy u mnoha firem, poskytovatelů Internetu a dalších subjektů, kdy využívají mimo jiné zejména služby Active Directory pro správu svých zákazníků či zaměstnanců.

4.3 Hotspot v RouterOS

V rámci mé praktické části jsem se rozhodl zpracovat, jak už bylo zmíněno, celkem dvě hotspotová řešení. Jako první se budu zabývat jednodušší variantou pro Hotspot v restauraci. Některá základní nastavení budou pro obě topologie obdobné, takže z nich bude malá část využita i ve druhé složitější variantě.

4.3.1 Hotspotové řešení 1 - restaurace

Pro zprovoznění Hotspotu v RouterOS musíme nejprve provést základní konfiguraci rozhraní, která se odvíjí od toho, jak jsme připojeni do sítě Internet (WAN) a jak budeme chtít nakonfigurovat naši LAN síť pro Hotspot.

V našem případě je směrovač RB532A připojen k Internetu ethernetovým portem *eth1*, který je propojen s LocoStation 5. Ta slouží jako brána do Internetu. Hotspot bude vysílat prostřednictvím bezdrátových rozhraní *wlan1* a *wlan2* nacházejících se přímo na Mikrotik RouterBOARDu a dále prostřednictvím bezdrátového rozhraní směrovače TP-LINK, který bude připojen k Mikrotik RouterBOARDu pomocí ethernetu.

V současné době je spuštěn na LocoStation 5 DHCP server, který přiděluje IP adresy všem připojeným zařízením. Rovněž na směrovači TP-LINK je spuštěn druhý DHCP server a překlad adres NAT⁶⁵, který přiděluje IP adresy všem bezdrátově připojeným zařízením k tomuto směrovači. Jelikož nemáme od poskytovatele Internetu do LocoStation přístup, jsme nuceni DHCP server zde běžící ponechat. Druhý

⁶⁵ Net Address Translation

DHCP server bude zrušen a nahrazen DHCP serverem novým spuštěným na našem Mikrotiku RB532A. Z TP-LINKu bude vytvořen pouze bridge, který bude rozšiřovat signál do další části restaurace, kde se nachází salonek.

Konfigurace RB532A

Nejprve nastavím ethernetová rozhraní. Rozhraní *ether1* budu používat jako rozhraní pro připojení k Internetu a propojím ho tedy s LocoStation 5. Jelikož na LocoStation 5 běží DHCP server, nastavím na rozhraní *ether1* DHCP client, tedy aby se chovalo jako obyčejný klient a nechalo si přidělat IP adresu od DHCP serveru. Automaticky se mi samozřejmě přidělí i maska podsítě a výchozí brána včetně IP adres DNS serverů. Na ostatní porty, jak ethernetové tak bezdrátové, nastavím DHCP server, který mi bude přidělovat IP adresy pro místní síť. Veškerou komunikaci mezi Internetem a místní sítí budu překládat pomocí NAT. Dalším požadavkem je, aby jeden z ethernetových portů zůstal „vyjmutý“ z Hotspotu a mohl na něj být připojen firemní počítač pro kancelářskou práci restaurace. Pro tento účel ponechávám port *ether3*. Zbylý port *ether2* a všechna bezdrátová rozhraní sloučím do jednoho bridge. Port *ether3* bude mít nastavenou svou adresaci a svůj dhcp server pro přidělování IP adres, aby byl celkově oddělen od sítě pro Hotspot. Adresu Hotspot serveru musíme nastavit na adresu našeho bridge a také jako interface zvolíme též náš bridge, jinak nám Hotspot nebude fungovat. Login metody Hotspotu pro naše účely nastavíme na HTTP PAP a HTTP CHAP. Doporučuji zrušit možnost cookie, která slouží k zapamatování si přihlášení v prohlížeči. Podrobný postup je ukázán v následující konfiguraci:

```
/system identity> set name="Restaurace_Salamandr"  
/interface bridge> add name="Hotspot_bridge"  
/interface bridge port> add bridge="Hotspot_bridge" interface=ether2  
/interface bridge port> add bridge="Hotspot_bridge" interface=wlan1  
/interface bridge port> add bridge="Hotspot_bridge" interface=wlan2  
/ip dhcp-client> add add-default-route=yes disabled=no interface=ether1 use-peer-dns=yes  
/ip address> add address=192.168.1.1 interface=Hotspot_bridge netmask=255.255.255.0  
/ip address> add address=192.168.2.1 interface=ether3 netmask=255.255.255.0  
/ip pool> add name="Dhcp_pool_hotspot" ranges=192.168.1.10-192.168.1.254
```

```

/ip pool> add name="Dhcp_pool_ether3" ranges=192.168.2.10-192.168.2.254
/ip dhcp-server> add address-pool=Dhcp_pool_hotspot disabled=no interface=Hotspot_bri
dge name="Dhcp_hotspot
/ip dhcp-server> add address-pool=Dhcp_pool_ether3 disabled=no interface=ether3
name="Dhcp_ether3"
/ip firewall nat> add action=masquerade chain=srcnat out-interface=ether1
/ip firewall nat> add src-address=192.168.2.0/24 chain=srcnat action=masquerade out-
interface=ether1
/ip dns> set allow-remote-requests=yes
/ip hotspot profile> add name="Hotspot_profil_manager" hotspot-address=192.168.1.1
login-by=http-chap,http-pap
/ip hotspot> add name="Hotspot_server" profile=Hotspot_profil_manager
interface=Hotspot_bridge disabled=no

```

Nyní máme RouterBOARD RB532A částečně připravený, ale v tuto chvíli bude fungovat Hotspot pouze na rozhraní ether2. Nicméně rozhraní ether3 by již mělo být plně funkční pro připojení firemního počítače pro kancelářské účely. Zbývá nám tedy ještě nastavit bezdrátová rozhraní a také vytvořit jednoho či dva uživatele pro otestování funkčnosti našeho Hotspotu.

```

/interface wireless security-profiles> add name="zabezpec hotspot" mode=dynamic-keys
authentication-types=wpa-psk,wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-
ccm wpa-pre-shared-key="SalamAnDr1980" wpa2-pre-shared-key="SalamAnDr1980"
/interface wireless> set wlan1 ssid="Salamandr Internet" band=2ghz-b/g channel-
width=20mhz frequency=2412 mode=ap-bridge security-profile="zabezpec hotspot"
name="WiFi Hotspot Ant1" disabled=no
/interface wireless> set wlan2 ssid="Salamandr Internet" band=2ghz-b/g channel-
width=20mhz frequency=2412 mode=ap-bridge security-profile="zabezpec hotspot"
name="WiFi Hotspot Ant2" disabled=no
/ip hotspot user> add name=admin password=admin server=Hotspot_server disabled=no
/ip hotspot user> add name=user1 password=heslo server=Hotspot_server disabled=no

```

V tuto chvíli můžeme RouterBOARD zapojit a odzkoušet všechna rozhraní, zdali fungují tak, jak mají. Pokud jste postupovali přesně jako já, měl by být na portu ether3

přístupný Internet, přičemž IP adresa by vám měla být přidělena DHCP serverem z rozsahu 192.168.2.10-192.168.2.254. Na portu *ether2* a na obou bezdrátových rozhraních by vám měl též přiřadit IP adresu DHCP server a to sice z rozsahu 192.168.1.10 – 192.168.1.254, přičemž bude po otevření prohlížeče nutné se přihlásit. K přihlášení použijeme předem vytvořené testovací účty *admin* s heslem *admin* nebo *user1* s heslem *heslo*.

Dalším krokem je zprovoznit ověřování pomocí lokálního RADIUS serveru, který nám nabízí platforma Mikrotik. K tomu, abychom mohli ověřování pomocí RADIUS serveru začít využívat, musíme ještě udělat v našem nastavení několik změn. Tou hlavní je přidání RADIUS serveru, kde zvolíme, že bude využíván pro Hotspot, vyplníme jeho IP adresu a heslo v kolonce *secret*, které je využíváno pro komunikaci s RADIUS serverem. Jelikož se chystáme využívat User manager od Mikrotiku, vyplníme IP adresu našeho bridge. Poté už jen změníme u našeho již nastaveného Hotspot profilu typ ověřování na RADIUS a aktivujeme funkci *accounting*.

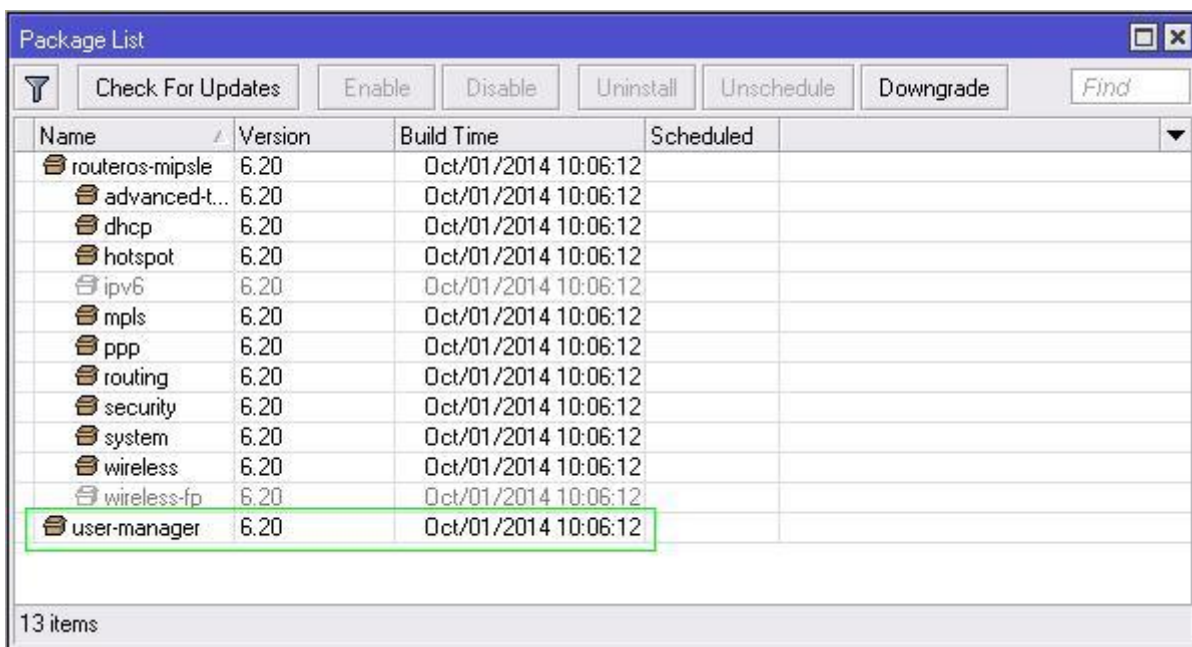
```
/radius> add address=192.168.1.1 disabled=no secret=s3cr3t1980 service=hotspot  
/ip hotspot profile> set Hotspot_profil_manager use-radius=yes radius-accounting=yes
```

Nyní ještě před nastavením User manageru zkonfiguruji a připojím přístupový bod TP-LINK. Nastavím ho do módu ap-bridge, v kterém bude do WiFi vysílat to co mu přijde na ethernetový port. Nebude zde aktivován žádný DHCP server, vše bude využíváno z RouterBOARDu RB532A. Jediné co uznávám za vhodné udělat je přidělení IP adresy tomuto TP-LINKu ze stejného rozsahu naší sítě, aby bylo později možné do něho snadno přistoupit přes webové rozhraní. Přidělím mu tedy adresu z našeho rozmezí 192.168.1.2. Tato adresa je volná a nemůže být přidělena žádnému uživateli DHCP serverem, jelikož rozsah přidělování adres začíná až adresou 192.168.1.10. Tímto je po fyzické stránce celá síť kompletní a zbývá pouze nastavit User manager.

4.3.1.1 User Manager

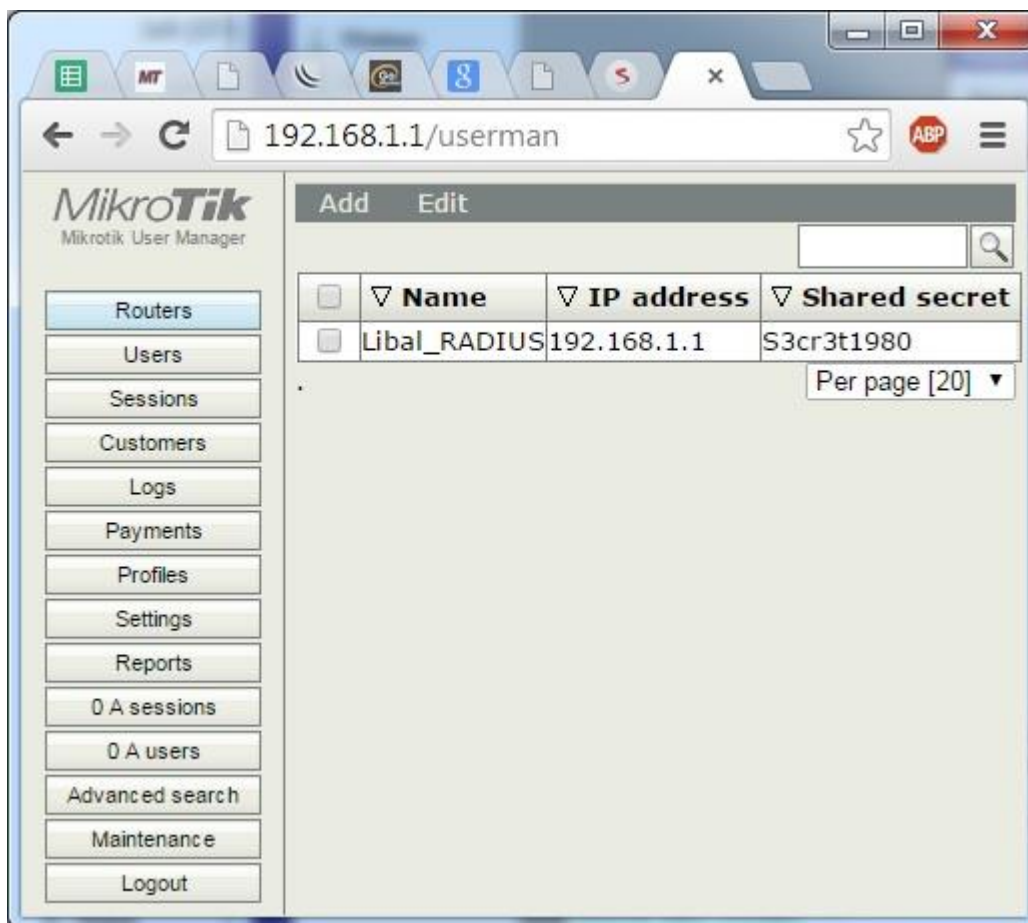
Jak již bylo zmíněno, nejvíce nabízející se variantou je využití RADIUS serveru přímo za pomoci samotného Mikrotiku. Mikrotik totiž nabízí dodatečný balíček s názvem User Manager, který umožní provozovat na daném RouterOS RADIUS server a zároveň spravovat databázi uživatelů včetně dalších nastavení. User Manager ale

není standardně nainstalován se základním RouterOS, tudíž je ve většině případů potřeba jej doinstalovat. Dodatečné balíčky si můžeme stáhnout ze stránek Mikrotiku [15], ale je opět potřeba zkontrolovat si verzi RouterOS, kterou máme a stáhnout balíček pro stejnou verzi (v našem případě verzi 6.20). Různé verze nejsou totiž u Mikrotiku navzájem kompatibilní. Ve stažené složce balíčků najdeme balíček s názvem user-manager-6.20-mipsle.npk a zkopírujeme jej do položky „Files“ ve WinBoxu. Stejně jako u upgrade RouterOS je důležité nahrát balíček přímo do kořenového adresáře. Poté následuje restart RouterBOARDu a balíček by měl být po naběhnutí doinstalován. Zkontrolovat si to můžeme opět ve WinBoxu v položce System->Packages.



Obrázek 4.7 Nainstalované balíčky ve WinBoxu

Pokud zde vidíme nainstalovaný balíček user-manager ve verzi 6.20, máme vyhráno a můžeme se do něj přihlásit. Přihlášení provedeme přes jakýkoliv webový prohlížeč, do kterého napíšeme v adresním řádku <http://<ip-address-mikrotik>/userman>, kde <ip-address-mikrotik> reprezentuje adresu IP, kterou jsme si nastavili na WAN rozhraní našeho Mikrotiku. Pro přihlášení použijeme výchozí nastavení. User *admin* a heslo ponecháme prázdné. V případě úspěchu se dostaneme do nastavení našeho User manageru.



Obrázek 4.8 Webové rozhraní Mikrotik User Manageru

Nejprve si musíme do našeho User Manageru přidat směrovače, s kterými budeme chtít User Manager používat. To provedeme přes Routers->Add->New. V novém okně vyplníme název, pod kterým bude náš směrovač přidán (viz. obrázek 4.8 výše), dále IP adresu směrovače nastavenou pro WAN rozhraní, heslo nastavené v RouterOS pro použití s RADIUS serverem (pole secret) a zaškrtnout použití CoA⁶⁶ portu jehož hodnotu nastavíme na 1700. Tím je směrovač přidán.

V dalším kroku zabezpečíme v položce „Customers“ účet admina tak, že mu nastavíme nějaké heslo a případně vyplníme další informace. Můžeme si přidat i další účty, přičemž každý účet může mít přednastavenou např. svoji šablonu pro vouchery, ale to popíši podrobněji v následující části.

⁶⁶ CoA (Change of Authorization) slouží ke změně některých atributů na základě žádosti RADIUS serveru bez nutnosti odpojení uživatele

Posledním krokem nutným ke zprovoznění User manageru, aby fungoval jako RADIUS server, je přidání uživatelů. To provedeme v položce „Users“. Můžeme buď pomocí volby „Add“ přidávat uživatele ručně po jednom nebo pomocí volby „Batch“ vygenerovat libovolné množství uživatelů najednou. K přidání uživatele stačí vyplnit jeho uživatelské jméno a heslo. Ostatní informace jsou nepovinné. Každý uživatel ve výchozím nastavení má neomezený přístup co se času i přenesených dat týče. Kupravení těchto parametrů slouží takzvané profily, které se přidělují nově vytvářeným uživatelům. Při hromadném generování více uživatelů najednou stačí zadat délku generovaného uživatelského jména a hesla, případně nějaký prefix, který bude u uživatelského jména použit, navolit profil, který jim bude přidělen a generování může začít. Toto se hodí zejména pro vytváření uživatelských účtů, které se budou později využívat na vouchery, o tom ale později. Pokud máme přidávaného alespoň jednoho uživatele, můžeme přejít k testování. Při připojení na WiFi Hotspot by nám měla naběhnout po spuštění webového prohlížeče nám již známá úvodní stránka Mikrotik Hotspotu, přes kterou se pokusíme na nově vytvořeného uživatele v User Manageru přihlásit. Po ověření uživatele RADIUS serverem již máme umožněný přístup do Internetu.

4.3.1.1.1 User Manager – Vouchery

Jak jsem již zmiňoval, User Manager umožňuje tvorbu tzv. voucherů, což jsou v podstatě poukazy, které slouží pro přístup k Internetu prostřednictvím našeho Hotspotu. V jádru je možné rozdělit tyto vouchery na dva základní typy. První typ voucheru poskytuje uživateli neomezený přenos dat, ale je limitován časovým intervalem, po jehož vypršení dojde k automatickému přerušení spojení a odpojení uživatele. Druhým typem je naopak časově neomezený přístup, ale uživatel má k dispozici pouze omezený počet dat, která může přenést. Většinou se volí jedna z těchto dvou možností, ale je možné je i vzájemně zkombinovat. Např. přístup na 2 hodiny s omezením přenosu 200MB dat. Mimo toto základní rozdělení se dále dají nastavovat další parametry, jako je přenosová rychlost, různé omezení IP adres, portů a dalších věcí.

Vytvořím dva demonstrační profily. Jako první vytvořím profil pro vouchery s limitem stažených dat o velikosti 200MB. Druhý profil bude naopak bez limitu stažených dat ale omezený dobou připojení na 2 hodiny. Právě ten se bude později

využívat v praxi pro provoz v restauraci. Nastavení provedeme v položce „Profiles“ a záložce „Limitations“, kde přidáme novou limitaci kliknutím na Add->New. Zvolíme název např. „200MB“ a vyplníme pole „Download“ hodnotou 200M. Pokud chceme, můžeme ještě v části Rate limits nastavit omezenou rychlost stahování včetně nastavení Burst rate⁶⁷, Burst threshold⁶⁸ a Burst time⁶⁹. Přidání dokončíme tlačítkem „Add“. Obdobným způsobem přidáme ještě jednu limitaci s názvem „2 hours“ a v položce „Uptime“ vyplníme hodnotu 120m. Opět přidáme tlačítkem „Add“.

Nyní máme předpřipravené dvě různé limitace, které použijeme pro vytvoření již zmíněných profilů. V záložce „Profiles“ přidáme nový profil zvolením tlačítka „+“ a vyplníme název profilu např. „Quota 200MB“. Dále zde určíme cenu tohoto voucheru v položce „Price“ a platnost voucheru v řádu dnů. Platnost se počítá dle nastavení v poli „Starts“ buď od vytvoření tohoto profilu nebo od prvního přihlášení daného uživatele. Po vyplnění přejdeme tlačítkem „Add new limitation“ do další části, kde zvolíme náš předpřipravený limit 200MB a potvrdíme tlačítkem „Add“. Mimo to se zde dá ještě nastavit restrikce na určité dny a čas, v který je možno se pomocí tohoto profilu připojit. Analogickým způsobem přidáme i druhý profil pod názvem „Limit 200MB“, kde přidáme naši předpřipravenou limitaci 200MB. Tímto jsou připraveny profily zákazníka *admin* pro vytváření nových uživatelů. Každý zákazník může mít vytvořené různé profily pro tvorbu uživatelů.

4.3.2 Hotspotové řešení 2 – Poskytovatel Internetu

Tato topologie je oproti první variantě složitější a budu na ni demonstrovat praktické využití centrálně řízeného Hotspotu. U platformy Mikrotik se tato funkce nazývá CAPsMAN. CAPsMAN slouží zároveň také pro označení hlavního řídicího směrovače – tzv. controlleru, který spravuje bezdrátová rozhraní ostatních směrovačů nazývaných CAPs.

⁶⁷ Burst rate udává maximální hodnotu downloadu a uploadu při aktivní funkci Burst

⁶⁸ Burst threshold udává hodnotu průměrné rychlosti přenosu dat, při jejímž překročení se deaktivuje Burst rate

⁶⁹ Burst time je čas udaný v sekundách, po který se vypočítává průměrná rychlost přenosu dat

Pokud budu popisovat topologie od páteřní linky, kde je připojena celá síť k Internetu, narazím jako první na zařízení Mikrotik RB153. Jedná se o starší kousek, který zde plní funkci brány do Internetu. Jeho funkce je čistě o překladu adres NAT a připojení několika periferních zařízení v sídle firmy. Toto nastavení není z hlediska mojí práce důležité, proto jej nebudu podrobněji rozebírat. Dalším aktivním prvkem v této topologii je centrální přepínač (switch). K němu je připojeno jedno testovací PC, které slouží pro různé účely techniků poskytovatele Internetu, dále server s operačním systémem Windows server 2003 Enterprise edition a nejdůležitější prvek této topologie směrovač Mikrotik RB532. Právě tento směrovač RB532 bude sloužit jako controller této hotspotové sítě a nastavím ho tedy jako CAPsMAN. Kromě toho, že zaujímá řídicí funkci ostatních vysílačů naší hotspotové sítě, sám je také jedním z vysílačů a sice pokrývá prostory náměstí. Dalším prvkem v síti je RouterBOARD RB532A, který bude pokrývat největší území, co se bezdrátového vysílání týče. Tento RouterBOARD je připojen k RB532 pomocí bezdrátového rozhraní. RB532A pokrývá svým signálem území v okolí autobusového nádraží a také slouží jako bezdrátový opakovač pro připojení posledního aktivního prvku naší topologie a to sice RouterBOARDu RB112. Ten se bude nacházet v prostorách vlakového nádraží, kde bude zprostředkovávat připojení veřejného PC terminálu pro přístup k Internetu prostřednictvím WiFi. Ostatní bezdrátová zařízení zahrnující laptopy, tablety a mobilní zařízení slouží pro simulaci uživatelů a k testovacím účelům nastavení sítě.

Konfigurace RB532

Jak už jsem zmiňoval, tento RouterBoard bude takovým jádrem této topologie. Začnu opět nastavením ethernetu. Budu využívat pouze jedno ethernetové rozhraní a to sice *ether1*, které bude spojovat tento RouterBoard s centrálním switchem a tudíž s celou lokální sítí. Jelikož chci mít hotspotovou síť oddělenou od sítě lokální, zavedu pro ni adresaci s jinou podsítí. Zároveň nastavím nový DHCP server, který bude všem uživatelům hotspotové sítě přidělovat IP adresy. Pro dobrou správu si vytvořím dva bridge. První z nich bude obsahovat všechna ethernetová rozhraní a jedno bezdrátové rozhraní, které bude sloužit pro komunikaci s RouterBOARDem RB532A. Druhý bude sloužit pro všechna bezdrátová rozhraní, která budou centrálně řízena a budou sloužit právě pro přístup do Internetu přes Hotspot systém. Mezi místní sítí a sítí pro Hotspot

bude probíhat překlad adres NAT. U Mikrotiku se tento proces překladu nazývá *masquerade*. Bezdrátové rozhraní pro komunikaci s RB532A nastavíme do režimu AP bridge a nastavíme šifrování přenosu WPA2. Také skryji vysílání SSID, jelikož tento spoj bude sloužit pouze jako tunel mezi oběma Mikrotiky a neslouží k připojování uživatelů. Nyní zbývá nastavit samotný Hotspot, pro nějž vytvoříme patřičný profil a přidělíme mu interface bridge vytvořeného pro Hotspot. Hlavní je nastavení RADIUS serveru a jeho konfigurace, která je popsána podrobněji v následující kapitole 4.3.2.1, která se zabývá právě konfigurací RADIUS serveru ve Windows 2003 serveru a jeho napojení na RouterOS pro ověřování uživatelů z Active Directory. Konfigurace RouterBOARDu RB532 je následující:

```
/system identity> set name="CAPsMAN"  
/interface bridge> add name="Hotspot_bridge"  
/interface bridge> add name="Local_bridge"  
/interface bridge port> add bridge="Hotspot_bridge" interface=cap1  
/interface bridge port> add bridge="Hotspot_bridge" interface=cap2  
/interface bridge port> add bridge="Hotspot_bridge" interface=cap3  
/interface bridge port> add bridge="Hotspot_bridge" interface=cap4  
/interface bridge port> add bridge="Local_bridge" interface=ether1  
/interface bridge port> add bridge="Local_bridge" interface=ether2  
/interface bridge port> add bridge="Local_bridge" interface=ether3  
/interface bridge port> add bridge="Local_bridge" interface=wlan2  
/ip address> add address=192.168.1.1 interface=Hotspot_bridge netmask=255.255.255.0  
/ip address> add address=192.168.0.250 interface=Local_bridge netmask=255.255.255.0  
/ip pool> add name="Dhcp_pool_hotspot" ranges=192.168.1.2-192.168.1.254  
/ip dhcp-server> add address-pool=Dhcp_pool_hotspot disabled=no  
interface=Hotspot_bridge name="Dhcp_hotspot"  
/ip dns> set servers 8.8.8.8  
/ip dns> set allow-remote-requests=yes  
/ip firewall nat> add action=masquerade chain=srcnat src-address=192.168.1.0/24  
/ip route> add dst-address=0.0.0.0 gateway=Local_bridge
```

```
/interface wireless security-profiles> add name="prenos_wpa2" mode=dynamic-keys authentication-types=wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-ccm wpa2-pre-shared-key="s3cr3t1980"
```

```
/interface wireless> set wlan2 ssid="CAPsMAN_prenos" band=5ghz-a channel-width=20mhz frequency=5180 mode=ap-bridge security-profile="prenos_wpa2" hide-ssid=yes disabled=no
```

```
/radius> add address=192.168.0.107 disabled=no secret=W2k3serverRADIUS service=hotspot
```

```
/ip hotspot profile> add name="Hotspot_AD" hotspot-address=192.168.1.1 login-by=http-pap use-radius=yes radius-accounting=yes
```

```
/ip hotspot> add name="Hotspot_server" profile=Hotspot_AD interface=Hotspot_bridge address-pool=Dhcp_pool_hotspot disabled=no
```

Nyní je nastaven základ pro fungování Hotspotu a ověřování proti RADIUS serveru na Windows serveru běžícím na IP adrese 192.168.0.107. Konfiguraci a propojení tohoto serveru s naší Mikrotik platformou proberu v další kapitole 4.3.2.1. Nyní ale musíme ještě zkonfigurovat funkci CAPsMAN, která nám právě umožní řízení ostatních RouterBOARDů v síti pomocí tohoto RouterBOARDu. Konfigurace je následující:

```
/caps-man channel> add name=kanal_hotspot frequency=2422 width=20 band=2ghz-b/g
```

```
/caps-man configuration> add name=config_hotspot mode=ap ssid="Verejny Internet Hotspot" channel=kanal_hotspot
```

```
/caps-man provisioning> add radio-mac=00:80:48:4A:EB:8B action=create-dynamic-enabled master-configuration=config_hotspot
```

```
/caps-man manager> set enabled=yes
```

```
/interface wireless cap> set enabled=yes interfaces=wlan1 caps-man-addresses=192.168.0.250
```

Pro funkčnost CAPsMANu je potřeba přednastavit základní profil konfigurace, který pak bude použit pro přidělené „CAPs“. V tomto profilu nastavíme, že bezdrátová rozhraní budou vysílat v režimu „ap“ v pásmu 2,4GHz na určené frekvenci a se stejnou šířkou pásma. Díky tomu, že tyto parametry budou vzhledem k této centrální správě na všech „CAPs“ stejné, budou se moci již jednou autorizovaná a připojená zařízení

automaticky připojit kdekoliv, kde bude signál z kteréhokoliv vysílače naší hotspotové sítě. Takto by měla být ve stručnosti konfigurace RouterBOARDU RB532 kompletní.

Konfigurace RB532A

Tento Mikrotik je v naší topologii takový dá se říci převaděč. Přijímá signál pomocí WiFi z RouterBOARDu RB532 CAPsMAN, který dál distribuuje RouterBOARDu RB112. Kromě toho také slouží jako vysílač pro náš veřejný Hotspot. Bude pokrývat okolí autobusového nádraží včetně přilehlé oblasti kulturního centra UFFO, budovy soudu a obecního úřadu. Rozhraní, která jsou používána k přenosu dat mezi RouterBOARDy budou ponechána v lokální síti, zatímco rozhraní, která budou vysílat signál pro veřejnost, budou součástí hotspotového bridge, který spadá do jiné podsítě. Společně s hotspotovými rozhraními RouterBOARDU RB532 budou řízena CAPsMANem a tudíž veškeré jejich nastavení a konfigurace bude sdílána právě od něj. Tento RouterBOARD nebude využívat v současnosti žádná ethernetová rozhraní, zato bude využívat hned čtyři rozhraní bezdrátová. Dvě slouží na komunikaci s ostatními prvky v síti a druhá dvě budou právě sloužit k vysílání hotspotové sítě do dvou různých zeměpisných směrů, tak aby pokryly popsané území. Konfigurace je následující:

```
/system identity> set name="CAP_RB532A_autobusak"  
/interface bridge> add name="Local_bridge"  
/interface bridge port> add bridge="Local_bridge" interface=ether1  
/interface bridge port> add bridge="Local_bridge" interface=ether2  
/interface bridge port> add bridge="Local_bridge" interface=ether3  
/interface bridge port> add bridge="Local_bridge" interface=wlan1  
/interface bridge port> add bridge="Local_bridge" interface=wlan2  
/ip address> add address=192.168.0.249 interface=Local_bridge netmask=255.255.255.0  
/ip route> add dst-address=0.0.0.0 gateway=Local_bridge  
/interface wireless security-profiles> add name="prenos_wpa2" mode=dynamic-keys  
authentication-types=wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-ccm wpa2-  
pre-shared-key="s3cr3t1980"
```

```
/interface wireless> set wlan1 ssid="CAPsMAN_prenos" band=5ghz-a channel-  
width=20mhz frequency=5180 mode=station-pseudobridge security-  
profile="prenos_wpa2" disabled=no
```

```
/interface wireless> set wlan2 ssid="CAPsMAN_prenos_vlakac" band=5ghz-a channel-  
width=20mhz frequency=5200 mode=ap-bridge security-profile="prenos_wpa2" hide-  
ssid=yes disabled=no
```

```
/interface wireless cap> set enabled=yes interfaces=wlan3,wlan4 caps-man-  
addresses=192.168.0.250
```

Po této konfiguraci již naváže RB532A komunikaci s RB532 a CAPsMAN začne řídit nově přidělená bezdrátová rozhraní. Zároveň je připraveno jedno bezdrátové rozhraní pro připojení posledního RouterBOARDu RB112, umístěného na vlakovém nádraží.

Konfigurace RB112

Poslední Mikrotik, který nám zbývá nakonfigurovat v naší topologii, je RB112. Je to starší model a už nedisponuje takovým výkonem jako např. použité RB532, nicméně pro naše nasazení plně dostačuje. Jeho hlavní účel je pokrytí WiFi signálem s naší hotspotovou sítí v prostorách vlakového nádraží a připojení bezdrátového terminálu pro umožnění přístupu k Internetu uživatelům, kteří nemají žádné své mobilní zařízení podporující WiFi. Tento RouterBOARD disponuje právě dvěma bezdrátovými rozhraními, přičemž jedno slouží jako přijímací pro spojení s RB532A a druhé bude řízené CAPsMANem a slouží k vysílání naší hotspotové sítě. Přenos mezi jednotlivými RouterBOARDy bude šifrován a vysílání SSID mezi oběma RouterBOARDy je skryto. Konfigurace je následující:

```
/system identity> set name="CAP_RB112_vlakac"
```

```
/ip address> add address=192.168.0.249 interface=wlan2 netmask=255.255.255.0
```

```
/ip route> add dst-address=0.0.0.0 gateway=wlan2
```

```
/interface wireless security-profiles> add name="prenos_wpa2" mode=dynamic-keys  
authentication-types=wpa2-psk unicast-ciphers=aes-ccm group-ciphers=aes-ccm wpa2-  
pre-shared-key="s3cr3t1980"
```

```
/interface wireless> set wlan2 ssid="CAPsMAN_prenos_vlakac" band=5ghz-a channel-  
width=20mhz frequency=5200 mode=station-bridge security-profile="prenos_wpa2"  
disabled=no
```



```
/interface wireless cap> set enabled=yes interfaces=wlan1 caps-man-  
addresses=192.168.0.250
```

U všech RouterBOARDů je samozřejmě potřeba nastavit k účtu, který bude používán na přihlašování administrátora do směrovačů, nějaké heslo, aby nemohly být RouterBOARDy a jejich konfigurace tak snadno napadeny nepovolanými osobami.

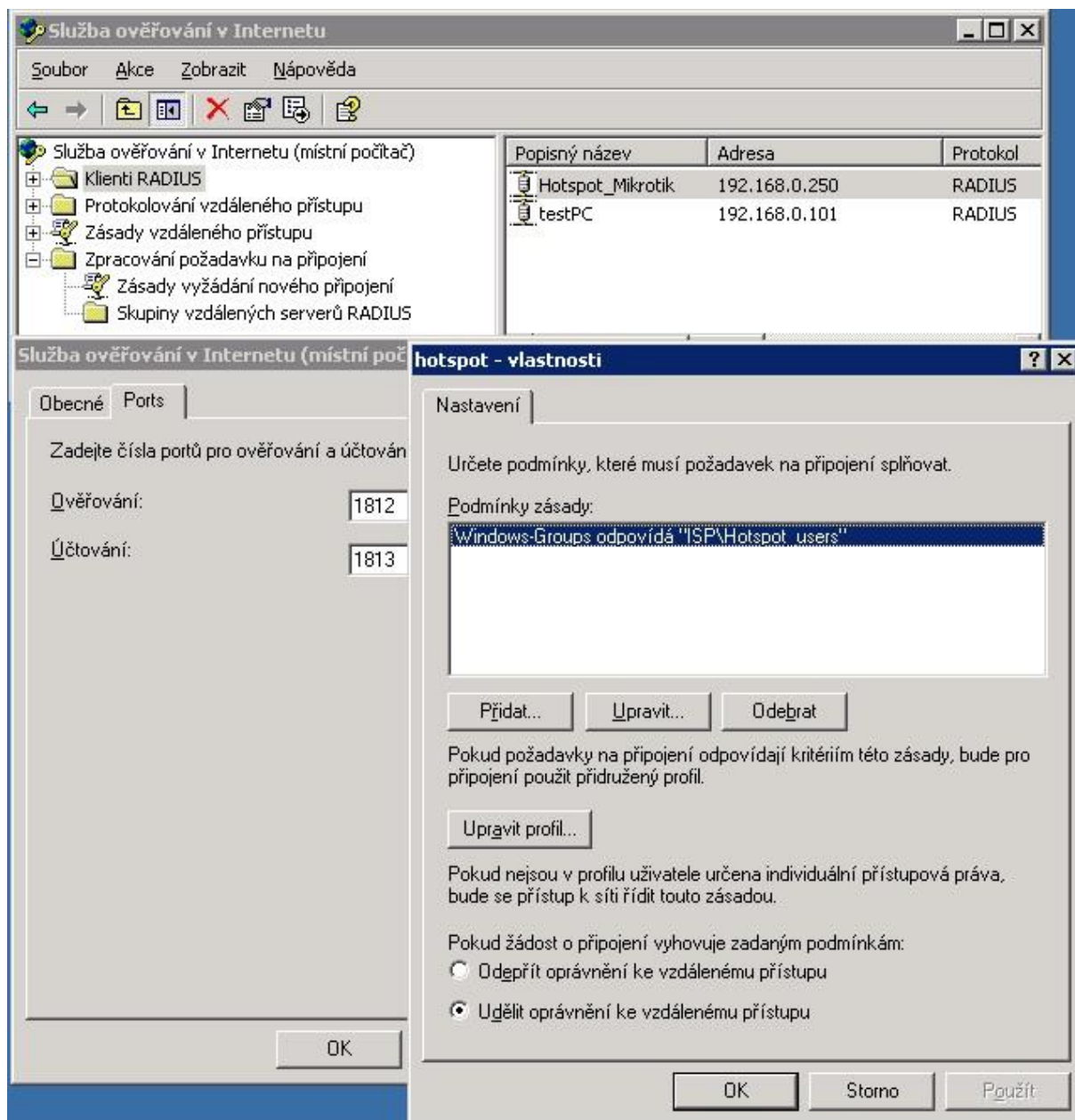
4.3.2.1 Windows Server RADIUS a Active directory

Jak už jsem zmiňoval, hodně firem i poskytovatelů Internetu používá síťový operační systém od firmy Microsoft s názvem Windows Server pro správu svých uživatelů. V takovém případě se naskýtá skvělá možnost propojit Windows server s naší Mikrotik platformou a zároveň využít Windows server jako RADIUS server pro náš Mikrotik. Praktické využití této varianty v sektoru poskytovatelů Internetu je hlavně v možnosti umožnit svým zákazníkům, kteří využívají jejich připojení v domácnosti i připojení na veřejných místech, kde daný poskytovatel Internetu poskytuje Hotspotová přípojná místa.

4.3.2.1.1 Konfigurace Windows 2003 Serveru

Nejprve je zapotřebí doinstalovat službu Internetové autentizace. Tu následně zaregistrujeme do Active Directory, abychom mohli později využívat ověření uživatelů právě z Active Directory. Ve vlastnostech Internetové autentizační služby nastavíme libovolný název a čísla portů, které budeme používat pro autentizaci a účtování. Já jsem nastavil autentizační port na hodnotu 1812 a účtovací port na 1813. Následně v položce „Klienti RADIUS“ vytvoříme nového klienta – náš Mikrotik. Nazveme si ho např. Hotspot_Mikrotik, vložíme IP adresu Mikrotiku a secret heslo pro komunikaci. V poli „Klient-dodavatel“ ponecháme RADIUS Standard, jelikož Mikrotik se v daném seznamu nenachází. Dále je nutné vytvořit politiku pro vzdálený přístup. Ve vlastnostech našeho Hotspotu pod položkou „Podmínky zásady“ přidáme podmínku „Windows-Groups odpovídá ISP\Hotspot_users“ a zaškrtneme „Udělit oprávnění ke vzdálenému přístupu“. Hotspot_users je mnou předem připravená skupina v Active Directory, do níž budu zařazovat uživatele, kteří budou mít možnost připojení na Hotspot. Před potvrzením ještě rozklikneme „Upravit profil“ a v záložce „Ověřování“ zaškrtneme „MS-CHAP v2“, „MS-CHAP“, „CHAP“, a „PAP, SPAP“. V záložce „Šifrování“

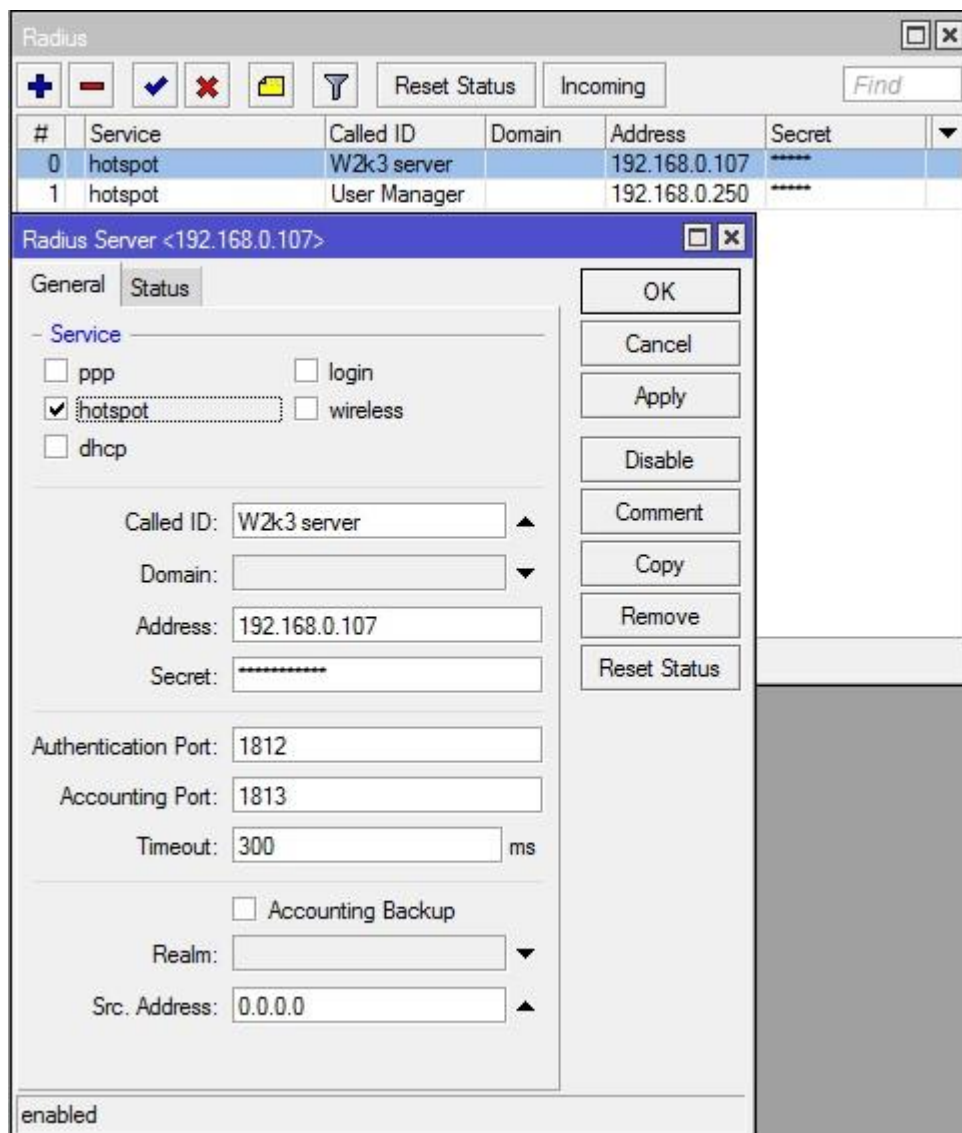
zaškrtneme všechny úrovně šifrování a vše potvrdíme. Tím je naše autentizační služba (RADIUS server) připravena k použití.



Obrázek 4.9 Nastavení autentizační služby na Windows 2003 serveru

Nyní je potřeba upravit také nastavení Mikrotiku tak, aby s naším novým RADIUS serverem komunikoval. To je vcelku jednoduché. V položce Radius vytvoříme nový RADIUS server pro Hotspot, vyplníme IP adresu PC, kde běží Windows Server s naší autentizační službou a secret heslo pro komunikaci. Autentizační port nastavíme stejně jako ve Windows serveru na 1812 a účtovací port na 1813. Tím by už mělo být

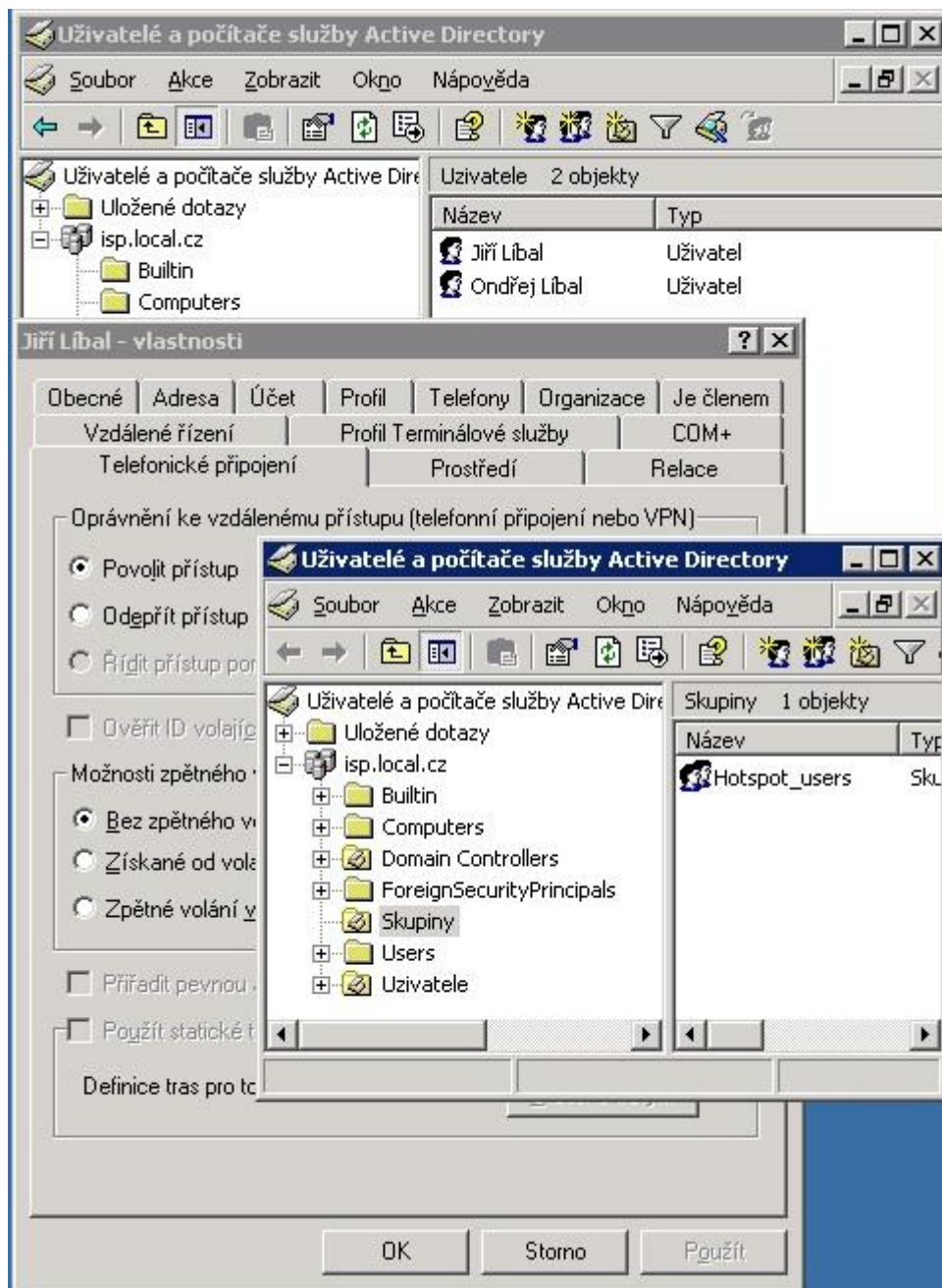
možné navázat spojení s RADIUS serverem. Můžeme to otestovat pomocí nástroje NTRadPing Test Utility více viz. Kapitola 4.6 o testování Hotspotu.



Obrázek 4.10 Nastavení RouterOS pro spolupráci s Window RADIUS serverem

Posledním krokem je nastavení uživatelů v Active Directory. Vyhledáme si skupinu uživatelů, kterým chceme umožnit přístup (v mém případě Hotspot_users) na náš Hotspot a otevřeme si její vlastnosti. V záložce „Je členem“ nastavíme, aby tato skupina byla členem skupiny „RAS and IAS Servers“. Nyní už zbývá jen vytvořit uživatele, u kterých musíme nastavit, aby byli členy naší skupiny „Hotspot_users“. Nesmíme zapomenout ve vlastnostech uživatelů v záložce „Telefonické připojení“ přepnout tlačítko v sekci „Oprávnění ke vzdálenému přístupu“ na volbu „Povolit přístup“. Na to pozor, protože bez této volby i když se vše jeví správně, vám nebude

autentizace uživatelů fungovat. Vše potvrdíme a můžeme vyzkoušet. Náš Hotspot by měl být plně funkční s ověřováním uživatelů pomocí RADIUS serveru běžícího na Windows 2003 serveru s Active Directory.

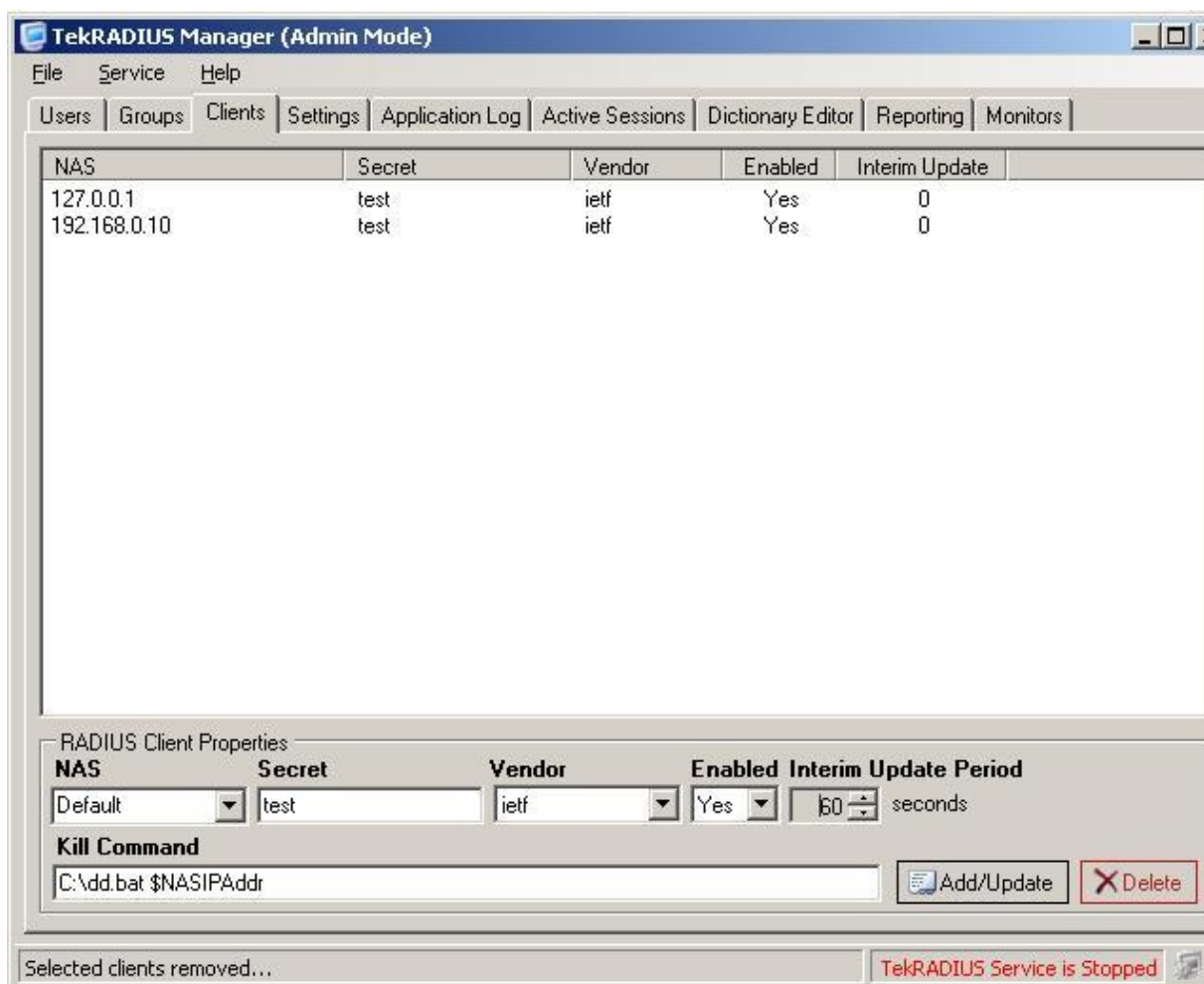


Obrázek 4.11 Skupiny, uživatelé a nastavení vzdáleného přístupu ve Windows 2003 serveru

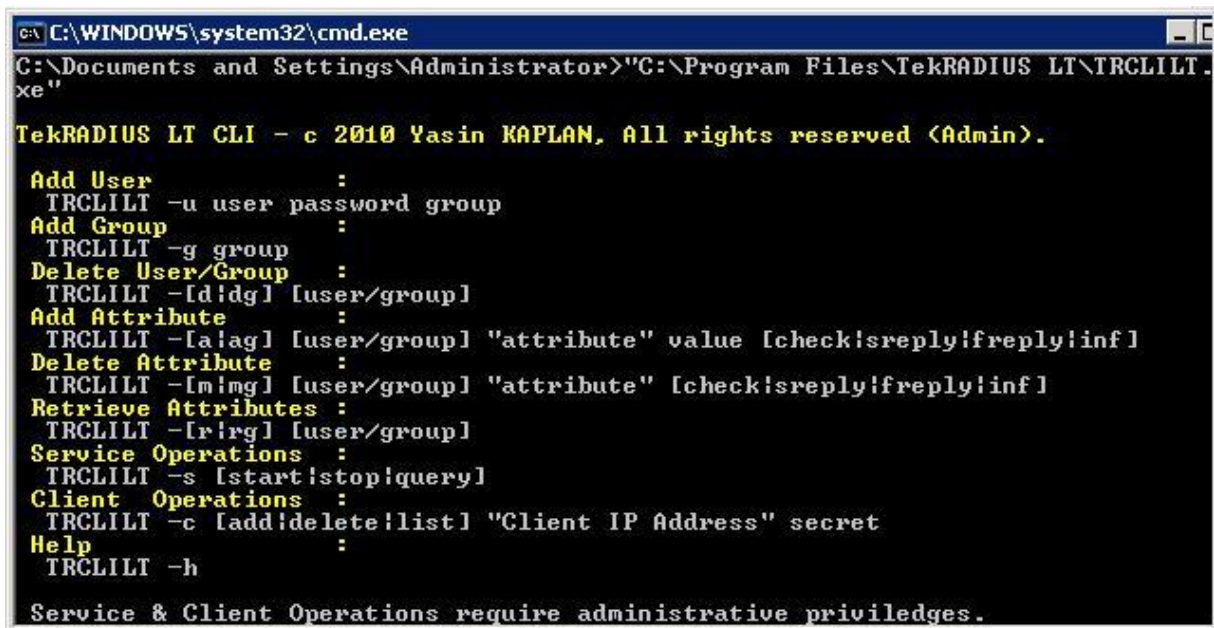
4.4 TekRadius server

Pro porovnání jsem se rozhodl vyzkoušet ještě jednu možnost, jak zprovoznit RADIUS server, který nám umožní snadné ověřování uživatelů. TekRADIUS je

v určitém rozsahu freeware Windows RADIUS server aplikace, která nám umožní rychle a snadno spustit autentizaci uživatelů pro náš Hotspot na jakékoliv platformě Windows. Tuto variantu jsem vybral z více důvodů. Prvním z nich je, že nabízí rychlou a snadnou implementaci. Druhým důvodem je, že je zdarma a pracuje na platformě Windows. Třetí důvod je možnost správy. TekRADIUS totiž umožňuje správu jak přes GUI rozhraní, kdy můžeme pohodlně vše nastavovat a přidávat uživatele pomocí velice uživatelsky přívětivého prostředí, tak i pomocí CLI. To se hodí zejména, pokud bychom chtěli psát vlastní skripty. Díky tomu by bylo možné navázat funkcionalitu tohoto RADIUS serveru s nějakou jinou aplikací, např. platební bránou, která by nám vkládala do databáze nové uživatele na základě určitých požadavků.



Obrázek 4.12 TekRADIUS GUI



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>"C:\Program Files\TekRADIUS LT\TRCLILT.exe"

TekRADIUS LT CLI - c 2010 Yasin KAPLAN, All rights reserved (Admin).

Add User          :
TRCLILT -u user password group
Add Group         :
TRCLILT -g group
Delete User/Group :
TRCLILT -[d|dg] [user/group]
Add Attribute     :
TRCLILT -[a|ag] [user/group] "attribute" value [check!reply!reply!inf]
Delete Attribute  :
TRCLILT -[m|mg] [user/group] "attribute" [check!reply!reply!inf]
Retrieve Attributes :
TRCLILT -[r|rg] [user/group]
Service Operations :
TRCLILT -s [start!stop!query]
Client Operations :
TRCLILT -c [add!delete!list] "Client IP Address" secret
Help             :
TRCLILT -h

Service & Client Operations require administrative privileges.
```

Obrázek 4.13 TekRADIUS CLI

4.5 Porovnání RADIUS serverů

Představil jsem celkem tři možnosti RADIUS serverů. První možnost přímo nabízená platformou Mikrotik se jménem User Manager je dostačující zejména, pokud chceme využívat Hotspot v nějaké restauraci či jiné menší provozovně. User manager nám může zajistit ověřování stálých uživatelů, ale zároveň se dá také využít pro tvorbu dočasných uživatelů a tisk voucherů pro krátkodobé či jinak omezené přístupy. Této možnosti často využívají různé restaurace či menší hotely.

Druhou možností je RADIUS server implementovaný přímo ve Windows serveru. Tato možnost se samozřejmě nabízí v případě, že v dané firmě již používají Windows server a aktivně využívají Active directory pro správu uživatelů. V tu chvíli je to nejlepší řešení, jak využít vzájemné spolupráce těchto dvou platform. Na druhou stranu, v případě že žádný Windows server v naší síti nevlastníme, je vcelku zbytečné jej implementovat pouze kvůli využití RADIUS služby, kterou nabízí. Nicméně stojí za zvážení, jaké další funkce, které tento mocný server nabízí, bychom mohli v naší síti případně využít.

Poslední možností je dedikovaný RADIUS server prostřednictvím samostatné Windows aplikace. Obecně se dá říci, že tuto možnost se dá aplikovat na cokoliv, kam se nehodí předchozí dvě varianty. Víceméně tato aplikace nám poskytuje vše nutné, co

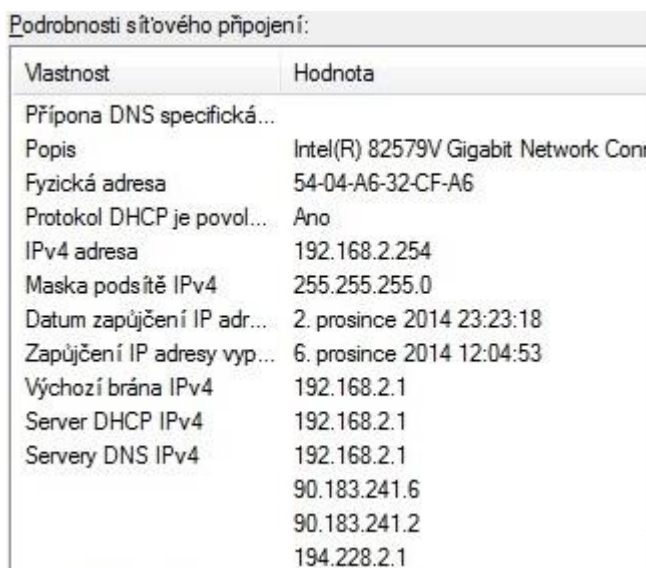
potřebujeme pro autentizaci uživatelů s možností textového rozhraní, a tudíž i skriptování. Díky tomu je zde potenciál pro napojení na další aplikace či platební bránu a rozšířit tak její funkcionalitu dle našich potřeb.

4.6 Testování Hotspotu

Nyní je čas vše co jsem zkonfiguroval otestovat a ukázat jak dané Hotspoty fungují. Také bych chtěl ukázat některé pomocné aplikace, které nám mohou pomoci při testování či případném ladění chyb při výstavbě hotspotové sítě s využitím RADIUS serveru pro ověřování.

4.6.1 Test infrastruktury pro restauraci

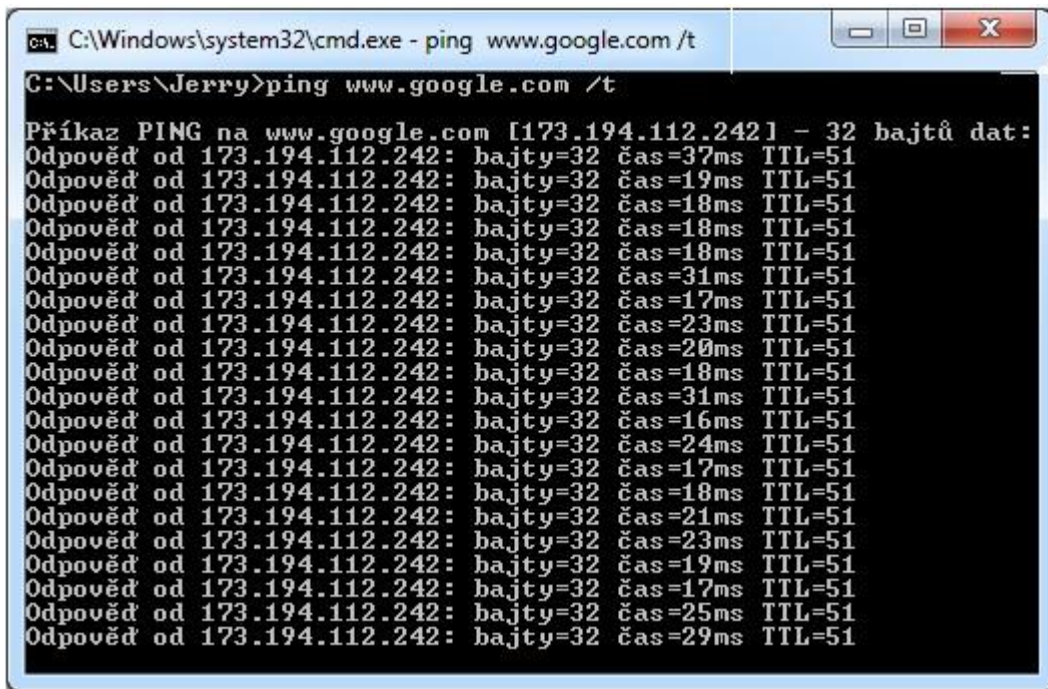
Jako první přejdeme k testování hotspotového řešení, které bylo navrženo pro provoz v restauraci Salamandr. Nejprve připojím stolní kancelářský počítač do portu *ether3* a ověřím si, jak proběhne připojení.



Vlastnost	Hodnota
Přípona DNS specifická...	
Popis	Intel(R) 82579V Gigabit Network Conn
Fyzická adresa	54-04-A6-32-CF-A6
Protokol DHCP je povol...	Ano
IPv4 adresa	192.168.2.254
Maska podsítě IPv4	255.255.255.0
Datum zapůjčení IP adr...	2. prosince 2014 23:23:18
Zapůjčení IP adresy vyp...	6. prosince 2014 12:04:53
Výchozí brána IPv4	192.168.2.1
Server DHCP IPv4	192.168.2.1
Servery DNS IPv4	192.168.2.1 90.183.241.6 90.183.241.2 194.228.2.1

Obrázek 4.14 Přidělení IP adresy a ostatních parametrů lokálnímu PC z DHCP serveru

Jak je vidět na obrázku výše, byla adaptéru přidělena IP adresa pomocí DHCP serveru z rozsahu 192.168.2.10 – 192.168.2.254 a výchozí bránu nám tvoří IP adresa rozhraní *ether3*, což je 192.168.2.1. Adresy DNS serverů jsou převzaté z DHCP serveru, který běží na LocoStation 5. Co se týče tedy přidělení údajů DHCP serverem je vše v pořádku. Nyní je ještě potřeba otestovat konektivitu.



```
ca. C:\Windows\system32\cmd.exe - ping www.google.com /t
C:\Users\Jerry>ping www.google.com /t
Příkaz PING na www.google.com [173.194.112.242] - 32 bajtů dat:
Odpověď od 173.194.112.242: bajty=32 čas=37ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=19ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=18ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=18ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=18ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=31ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=17ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=23ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=20ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=18ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=31ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=16ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=24ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=17ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=18ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=21ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=23ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=19ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=17ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=25ms TTL=51
Odpověď od 173.194.112.242: bajty=32 čas=29ms TTL=51
```

Obrázek 4.15 Testování konektivity pomocí utility ping

Z výše uvedeného obrázku je patrné, že konektivita s dotazovaným serverem byla navázána. K otestování jsem použil utilitu ping integrovanou ve Windows. Ping byl směrován na doménové jméno serveru Google, čímž jsem otestoval jak funkčnost DNS serveru, tak i konektivitu a rychlost odezvy z Internetu. Odezva je velice solidní a připojení funguje tak, jak má. Po otevření prohlížeče můžeme ihned využívat Internet bez nutnosti jakéhokoliv přihlašování.

Další test, který je nutné provést, se týká již samotného Hotspotu. Otestoval jsem přihlášení na laptopu a mobilním zařízení SONY XPERIA Z1 přes WiFi rozhraní jak na Mikrotiku, tak i TP-LINKu. Všechna rozhraní se chovala stejně, jelikož jsou v jednom bridge. K testování jsem vytvořil několik uživatelů s platnou dobou přihlášení 1 minuty.



Obrázek 4.16 Pokus o přihlášení se stejným účtem po vypršení lhůty XPERIA Z1

User sessions							
▼ Username	▼ Status	▼ User IP	▼ From time	▼ Till time	▼ Uptime	▼ Download	▼ Upload
bz8ufw	Start & Stop	192.168.1.252	01/02/1970 13:25:44	01/02/1970 13:26:44	1m	4.1 MiB	294.1 KiB

Obrázek 4.17 Zobrazení informací o uživateli v User manageru

Jak je vidět na obrázcích výše, uživatel byl po vypršení jedné minuty odhlášen a již mu nebylo umožněno opětovné přihlášení pod stejným uživatelským jménem a heslem. Zároveň jak znázorňuje obrázek 4.17, vidíme, od kdy do kdy bylo připojení využito a kolik dat uživatel za tu dobu přijal a odeslal.

4.6.2 Test infrastruktury pro poskytovatele Internetu

Druhá infrastruktura, kterou jsem nasimuloval, by měla sloužit pro zákazníky poskytovatele Internetu ve městě Trutnov. Tento poskytovatel se totiž rozhodl umožnit svým stávajícím zákazníkům možnost připojení prostřednictvím Hotspotů, jimiž chtěl pokrýt několik nejvýznamnějších lokalit, co se v hustotě lidí na plochu týče. Tato infrastruktura využívá centrálně řízený Hotspot zprovozněný na platformě

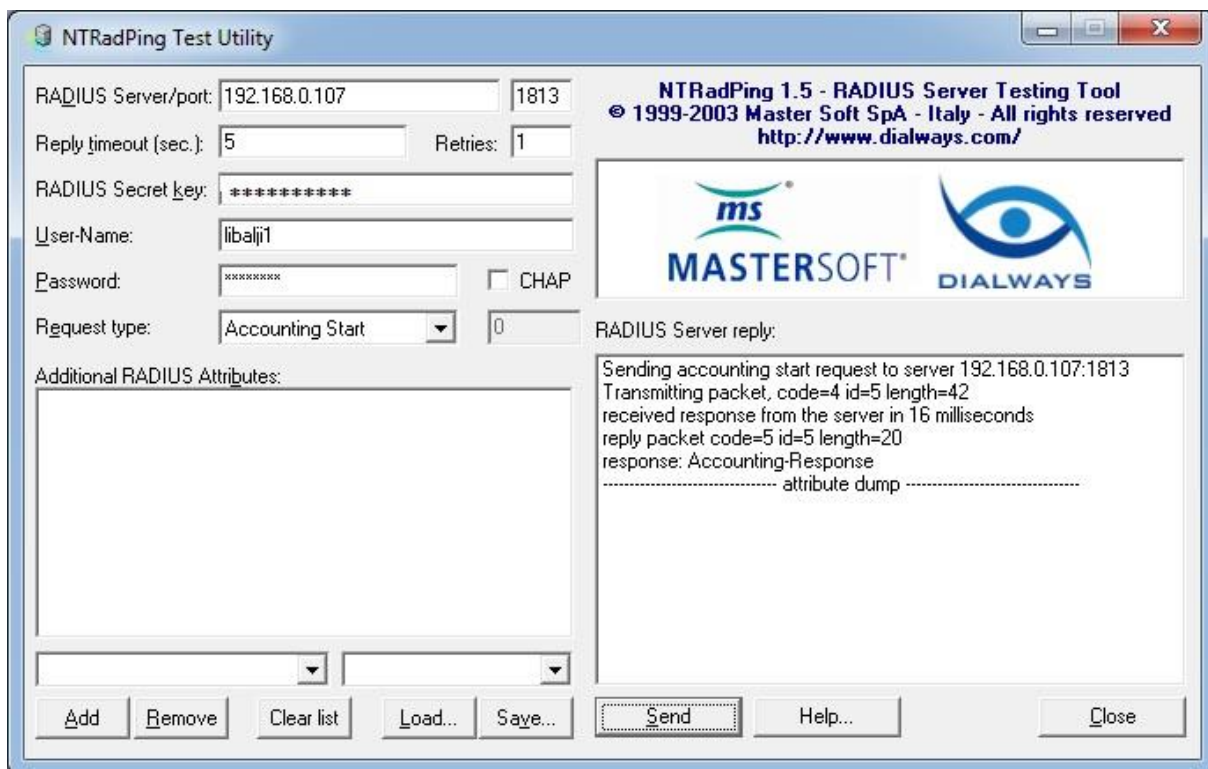
Mikrotik. Otestuji funkčnost RADIUS serveru a představím utilitu, která může napomoci při testování a ladění konektivity s RADIUS serverem. Dále je zapotřebí otestovat připojení uživatelů, přidělování IP adres DHCP serverem a v neposlední řadě správné ověření uživatele na RADIUS serveru a umožnění přístupu k Internetu. V místech, kde je lokalita pokrytá více vysílači, otestuji také roaming při přechodu mezi jednotlivými vysílači.

Nejprve tedy představím utilitu na testování konektivity s RADIUS serverem. Jednou z takových aplikací je *NTRadPing Test Utility*. Ta nám umožní otestovat funkčnost RADIUS serveru ještě dříve, než ho spustíme naostro pro ověřování uživatelů v našem Hotspotu. Tato aplikace nepotřebuje žádnou instalaci a její ovládání je vcelku jednoduché a intuitivní. Do prvního textového pole RADIUS Server vyplníme IP adresu našeho RADIUS serveru a vedle port pro ověřování, který jsem nastavil na 1812. Dále se dá nastavit čas, po který se bude aplikace pokoušet připojit a počet případných opakování pokusů o připojení v případě selhání. Do pole RADIUS Secret key vyplníme heslo, které jsme si nastavili pro komunikaci s RADIUS serverem. Pak už stačí jen vyplnit nějakého uživatele a jeho heslo, kterého máme v databázi. V mém případě jsem testoval RADIUS server na Windows serveru s databází uživatelů v Active Directory. Request type ponecháme na hodnotě Authentication Request a můžeme tlačítkem „Send“ spustit testovací připojení. Pokud vše proběhne v pořádku, výsledek by měl vypadat obdobně jako na následujícím obrázku, přičemž důležitá je hláška: „response: Access-Accept“.



Obrázek 4.18 NTRadPing Test Utility test ověření uživatele na RADIUS serveru

Další věc, co můžeme otestovat, je odezva na portu pro účtování. Pro otestování ponecháme totožné nastavení jako v předchozím případě až na dvě věci. Změníme port z hodnoty 1812 na hodnotu 1813, kterou jsem použil při konfiguraci RADIUS serveru pro účtovací port a v poli „Request type“ změníme hodnotu na „Accounting Start“. Poté můžeme opět spustit test tlačítkem „Send“ a v případě úspěchu dostaneme hlášku: „response: Accounting-Response“.

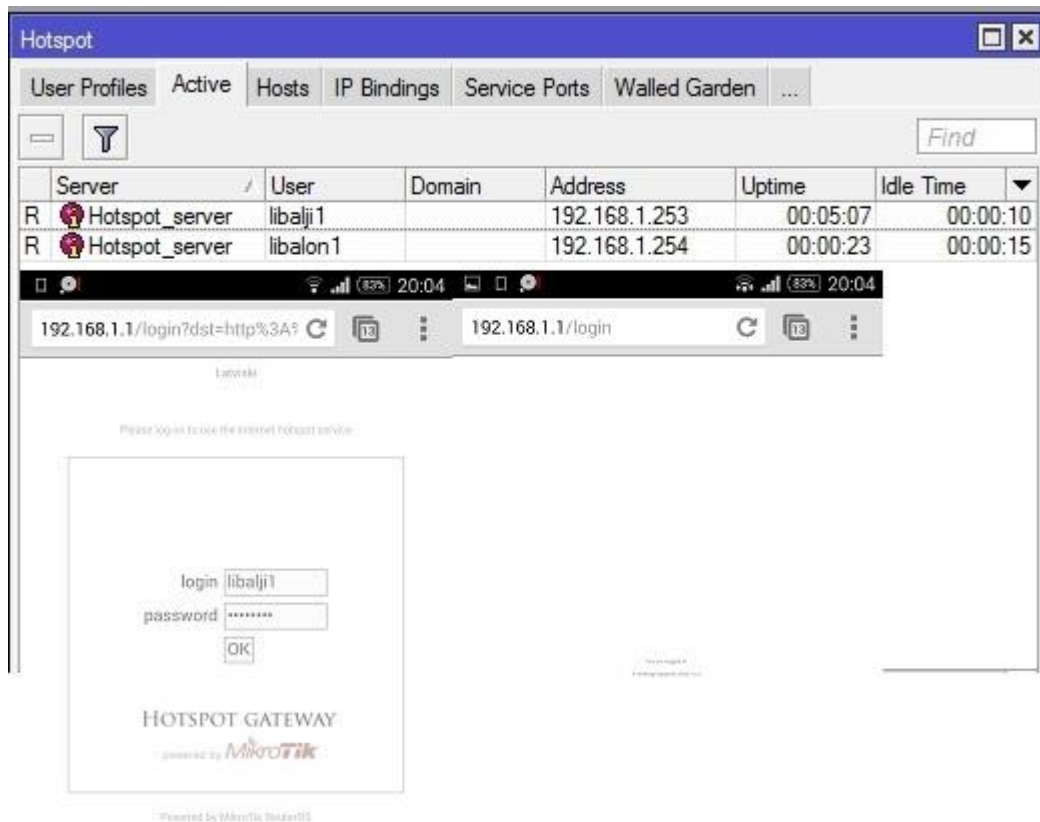


Obrázek 4.19 NTRadPing Test Utility test účtovacího portu

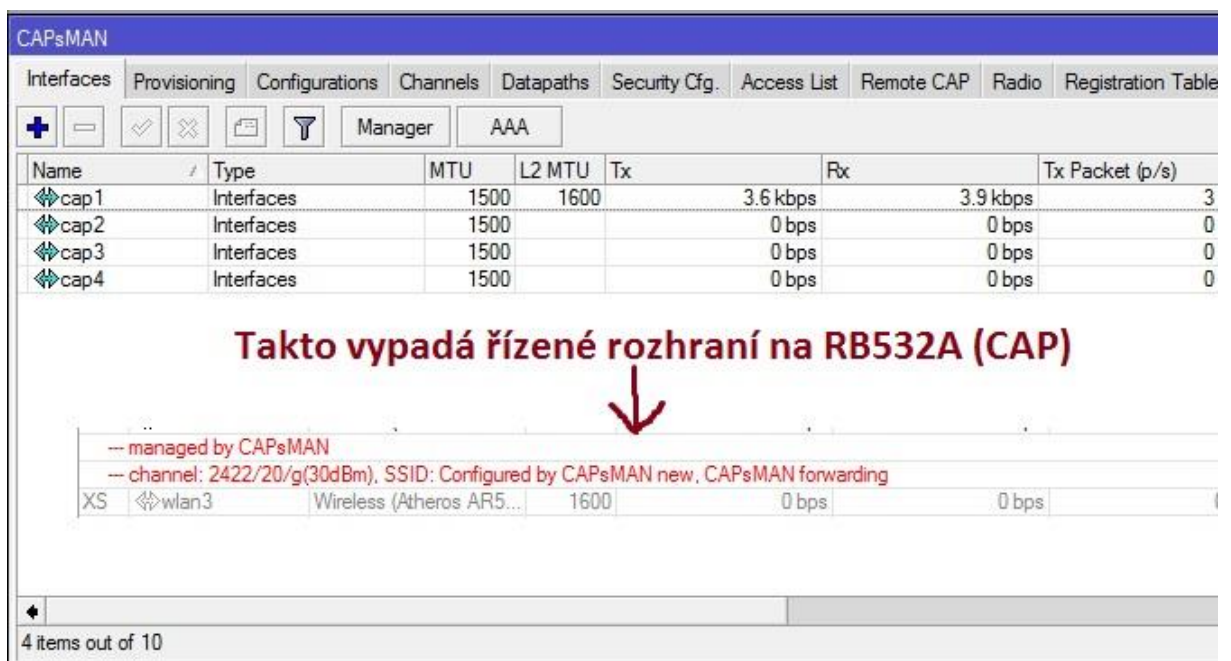
Pokud oba testy prošly v pořádku, RADIUS server by měl být funkční a připravený k použití s naším Hotspotem.

Nyní je čas otestovat tedy samotné připojení a ověření uživatelů v naší hotspotové síti. Připojení jsem testoval na více zařízeních. Nejprve jsem použil laptop, poté tablet a nakonec mobilní telefon. Na všech zařízeních proběhlo připojení bez problémů, což je vidět i z následujících obrázků. Obrázek 4.20 ukazuje připojené a ověřené dva uživatele pomocí RADIUS serveru běžícím na Windows 2003 serveru. Obrázek kombinuje snímek z RouterOS CAPsMANu, kde jsou vidět připojení a aktivní uživatelé a dva snímky z mobilního zařízení s ukázkou přihlašovací obrazovky a úspěšného přihlášení uživatele po ověření. Obrázek 4.21 nám zobrazuje dva snímky. První část je pořizena v CAPsMANu, kde jsou znázorněny jednotlivá kontrolovaná bezdrátová rozhraní nazývaná „CAPs“, druhá část pochází právě z jednoho řízeného Hotspotu tzv. „CAPu“, kde vidíme, jak je znázorněno řízené bezdrátové rozhraní. Zároveň kromě upozornění, že daná rozhraní jsou spravována CAPsMANem nám zde zobrazuje i parametry, které těmto rozhraním jsou přidělovány. Poslední obrázek 4.22

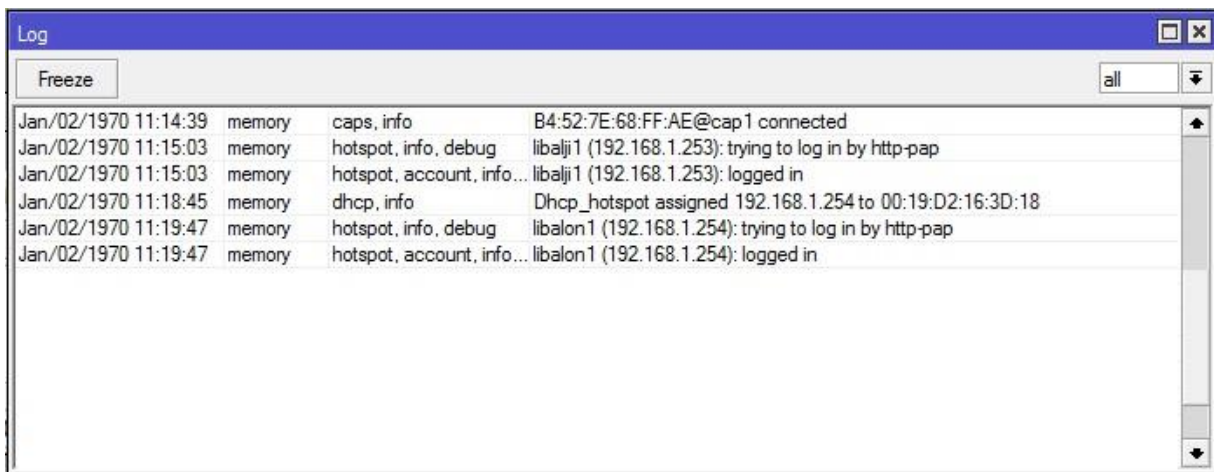
zobrazuje záznam z Logu na RB532, který je zároveň CAPsMANem a prokazuje nám přidělení IP adres a přihlášení obou uživatelů.



Obrázek 4.20 Uživatel připojený na Hotspot v RouterOS



Obrázek 4.21 Přihlašovací obrazovka na mobilním telefonu do Hotspotu



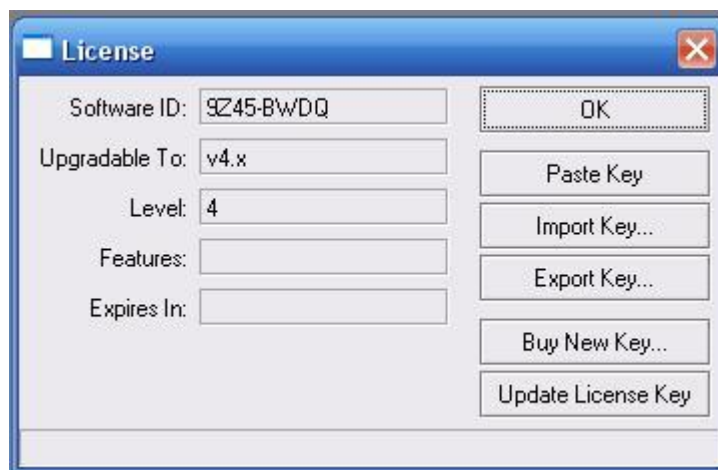
Obrázek 4.22 Log z RB532 (CAPsMANu) zobrazující přihlášení uživatelů na Hotspot

4.7 Problémy a jejich řešení

Během sestavování, konfigurace a dalších kroků prováděných během mé práce na praktické části jsem narazil občas na nějaké problémy či upgrady, které bych zde rád uvedl. Sám vím, že občas některé takové tipy a postřehy kolikrát člověku usnadní nějaké velké trápení v nestandardní situaci, kdy člověk neví, co a jak. V následující části uvedu několik tipů a kroků, na které jsem narazil během mého působení na praktické části této práce.

4.7.1 Zastaralý RouterOS

Pokud se vám dostane do rukou nějaký starší RouterBOARD, jakožto RB532 i RB112 mezi ně patří, budou ve většině případů obsahovat zastaralý RouterOS. Demonstruji svůj postup na RB532A, který jsem upgradoval ze zastaralé verze RouterOS v3.3. Tento model RouterBOARDu se prodává s licencí level 4, která by měla umožňovat upgrade RouterOS na vyšší verzi, konkrétně až na verzi 6.x. Nejvyšší možnou verzi, na kterou můžete nyní přímo upgradovat, zjistíte snadno přes rozhraní WinBoxu. Informace se nachází pod položkou System -> License.



Obrázek 4.23 WinBox License

V tomto případě je momentálně možný upgrade na verzi 4.x. To ale ještě neznamená, že je to nejvyšší možná verze, na kterou lze upgradovat. Mikrotik totiž většinou neumožňuje přímý upgrade o několik verzí, je tudíž nutné upgradovat na verzi, která je aktuálně vypsána v tabulce License a po upgradu opět tuto tabulku zkontrolovat, zdali se nám s upgradem neumožnil upgrade na verzi vyšší.

U některých kusů se může stát, že přestože level vaší licence je level 4, uvidíte v poli „Upgradable To“ pouze verzi 3.x. Důvodem toho je přechod Mikrotiku na novější licenční klíče. V takovém případě stačí updatovat váš klíč na novější. To provedete kliknutím na tlačítko „Update License Key“ nacházející se ve výše zmíněné nabídce „License“. Váš starý klíč by měl být automaticky zálohován do souboru, uložen mezi soubory v paměti Mikrotiku a updatován na klíč nový. Pro jistotu doporučuji ještě před updatem přes položku „Files“ zálohovat soubor s klíčem ručně kamkoliv na externí médium. Tento starší klíč vám může sloužit v případě potřeby downgradu na starší RouterOS nebo při jakémkoliv problému s licencí při upgradu.

4.7.1.1 Upgrade RouterOS

V současné době je pro RouterBOARD z řady RB5xx nejvyšší možná verze 6.20. Jak jsem již avizoval, Mikrotik neumožňuje přímý upgrade z verze 3.x na verzi 6.x. Vždy musíme upgradovat postupně dle nejvyšší možné verze, kterou vidíme v tabulce License. Náš testovací RouterBOARD může být v nynějším stavu upgradován na verzi 4.x, stáhneme tedy dostupnou verzi 4.17. Upgrade lze provést několika metodami –

pomocí rozhraní WinBox, přes FTP⁷⁰, DUDE⁷¹ nebo přes síť. Nejjednodušší a nejpohodlnější varianta je pomocí prostředí WinBoxu. Při výběru balíčku pro upgrade RouterOS je potřeba také dbát na výběr správné instrukční sady, kterou váš RouterBOARD obsahuje. V mém případě je to „mipsle“. Stažený balíček s názvem *routeros-mipsle-4.17.npk* jednoduše zkopírujeme do prostředí WinBoxu mezi ostatní soubory v okně „Files“, přičemž si dáme pozor, aby se námi kopírovaný soubor nahrál opravdu do kořenového adresáře, nikoliv do některé ze složek, které jsou zde již obsaženy. Poté stačí provést restart zařízení a upgrade by měl automaticky proběhnout sám. Poté můžeme zkontrolovat aktuální verzi našeho RouterOS v položce „Packages“ a možnost upgradovat na vyšší RouterOS v položce „License“. Tam se nyní nachází v řádku „Upgradable To“ verze 6.x. Stejným způsobem tedy stáhneme a upgradujeme v současnosti na nejnovější balíček verze 6.20. Nový RouterOS má opravené některé chyby, přidanou funkcionalitu a novější lehce upravené grafické prostředí WinBoxu.

U RB532 a 532A proběhlo vše v pořádku. Problém nastal s RB112, která má přeci jen slabší hardware. Při aktualizaci RouterOS na aktuální verzi 6.20 již RouterBOARD nenastartoval. Byl jsem nucen tedy k nahrání jiného RouterOS pomocí sériové konzole, přičemž nejvyšší verze, kterou jsem na RB112 rozběhl, byla v6.11. Je to zároveň také první verze, která podporuje centrální řízení a může být tedy spravována pomocí CAPsMANu. Pokud ale nepotřebujete tuto funkcionalitu, doporučuji ponechat některou verzi RouterOS v5.x, která funguje o dost svižněji.

4.7.2 Změna přihlašovací stránky Hotspotu

Mnohým majitelům svých provozoven restaurací či provozovatelům bezdrátových Hotspotů se nemusí líbit či hodit výchozí přihlašovací stránka, kterou Mikrotik poskytuje. To není žádný problém. Pokud se přihlásíme do příslušného RouterBOARDu, na kterém běží spuštěný Hotspot server, najdeme v položce „Files“ složku s názvem Hotspot. V této složce se nachází soubor *login.html*, který si můžeme stáhnout a v rámci možností a práce s tvorbou webových stránek si tuto stránku

⁷⁰ File Transfer Protocol

⁷¹ DUDE je bezplatná aplikace od společnosti Mikrotik, která slouží k řízení a monitorování sítě, mimo jiné ji lze využít i pro upgrade směrovačů

upravit dle obrazu svého. Použit je jazyk html a php s využitím kaskádových stylů (css).

5 Závěr

Internet se stává stále silnějším a více využívaným médiem všech věkových skupin. Zároveň se stále zvyšují nároky uživatelů na neustálé připojení k Internetu vysokou rychlostí přenosu dat. O tom jsem ostatně čtenáře této práce přesvědčil hned v úvodu poukázáním na patřičné statistiky a výzkumy provedené v oblasti využití Internetu. To vše napomáhá rozvoji a popularitě bezdrátových Hotspotů, které nabízejí jedno z možných řešení, jak odpovědět na stále zvyšující se poptávku po vysokorychlostním připojení na veřejných místech či v rámci nějaké firmy patřičnou nabídkou.

Problematika Hotspotu provozovaného na bezdrátové síti je velice rozsáhlá. Pokud by měla být sepsána práce detailně popisující veškeré technologie a potřebné znalosti pro zprovoznění a správu bezdrátového Hotspotu, vydala by každá z jednotlivých částí na samostatnou práci o obdobném rozsahu jako je tato. Na to zde ale nebyl prostor a ani to nebylo mým cílem.

Náplní první části této práce bylo stručně a strukturovaně popsat jednotlivé standardy, technologie, přenosové parametry a další dílčí části, které jsou nutné pro funkčnost Hotspotu a uvést do povědomí čtenáře, jak jednotlivé technologie fungují a jaký je mezi nimi rozdíl. Čtenář této práce by tedy měl mít po jejím nastudování například povědomí o tom, jakou technologii při vytváření bezdrátového Hotspotu zvolí a proč.

Druhá část této práce měla za úkol obeznámit čtenáře se samotnou problematikou Hotspotů, jejich funkcemi, typy, kvalitou služeb QoS a v neposlední řadě také velice důležitým zabezpečením. Prvním cílem této práce bylo představení tří platforem, na kterých je možné bezdrátový Hotspot zprovoznit a popsání jejich výhod a nevýhod při nasazení v určitém sektoru. Vše bylo nakonec shrnuto v provedeném srovnání. Hlavní pozornost byla věnována platformě Mikrotik, s kterou jsem chtěl čtenáře seznámit podrobněji a ostatně o tom vypovídá i podtitul této práce. Důvodem k zvýšené pozornosti této platformě je, jak jsem již zmiňoval v úvodu, její velká a stále vzrůstající popularita, kterou si platforma získává svým výborným poměrem ceny a výkonu, který za to nabízí. V závěru teoretické části bylo pojednáno o platebních

bránách pro hotspotové systémy a popsal jsem několik návrhů na implementaci platební brány pro možnost provozování placeného Hotspotu.

V třetí části mojí práce jsem se věnoval svému druhému cíli, který byl pro mě nejvíce přínosný. Jsou zde uplatněny všechny nastudované vědomosti ohledně bezdrátových Hotspotů a jejich technologií v praxi při implementaci na již zmiňovanou platformu Mikrotik. Z hlediska velké rozlehlosti této problematiky, která zahrnuje také důkladnou znalost v oboru počítačových sítí a bezdrátových sítí vůbec, jsem se zaměřoval v rámci popisu konfigurace hlavně na části týkající se Hotspotu a s tím spojeného zabezpečení v podobě autentizace přes RADIUS server, šifrování přenosu či nastavení některých omezení uživatelů. V rámci implementace jsem navrhl dvě různé topologie a vyzkoušel tři různé RADIUS servery, které jsem zkonfiguroval pro spolupráci s hotspotovým systémem na platformě Mikrotik. Následně jsem tyto RADIUS servery porovnal a popsal jejich výhody a nevýhody. Závěrem jsem oba implementované hotspotové systémy otestoval a popsal užitečné utility a tipy, které se mohou hodit při konfiguraci, ladění a testování Hotspotu s ověřováním uživatelů přes RADIUS server. Veškerá nastavení se prokázala být funkční a dané topologie fungovaly tak, jak bylo plánováno. Jedna z topologií, zkonfigurovaných v této práci, bude dokonce brzy použita v reálném provozu.

Osobně si myslím, že bezdrátové Hotspoty jsou stále v době svého rozmachu a jejich počet bude narůstat. V západní Evropě je jejich popularita značně vyšší, ale z celosvětového hlediska je ještě spousta zemí, kde se Hotspoty masivně začínají implementovat. To mohu ztvrdit svou vlastní zkušeností z pobytu v Thajsku a na Taiwanu, kde jsou nyní Hotspoty vcelku oblíbené. Možností na implementaci bezdrátových Hotspotů je spousta a doufám, že po přečtení této práce bude povědomí čtenářů o Hotspotech zase o něco bohatší a moje praktické poznatky z implementace na platformě Mikrotik jim budou nápomocny.

6 Seznam použité literatury a další prameny

- [1] INTERNET WORLD STATS *Internet users in the world* [Online] 31. 12. 2013 [Citace: 20. 5. 2014] Dostupné z: <http://internetworldstats.com/stats.htm>
- [2] ČESKÝ STATISTICKÝ ÚŘAD *Analýza internetu* [Online] [Citace: 22. 5. 2014] Dostupné z: [http://www.czso.cz/csu/redakce.nsf/i/internet_telekomunikacni_a_internetov_a_infrastruktura_a_a_k/\\$File/2013_inet_rev2.pdf](http://www.czso.cz/csu/redakce.nsf/i/internet_telekomunikacni_a_internetov_a_infrastruktura_a_a_k/$File/2013_inet_rev2.pdf)
- [3] EPRIN *Základní přehled standardů IEEE 802.11* [Online] [Citace: 23. 5. 2014] Dostupné z: <http://www.eprin.cz/zakladni-prehled.html>
- [4] ŽIVĚ.CZ *Nový standard IEEE 802.11ac* [Online] 3. 10. 2012 [Citace: 23. 5. 2014] Dostupné z: <http://www.zive.cz/clanky/novy-standard-wi-fi-gigabit-vzduchem/sc-3-a-165687/default.aspx>
- [5] RADIO-ELECTRONICS *IEEE 802.11n Standard* [Online] [Citace 26. 5. 2014] Dostupné z: <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11n.php>
- [6] INTEL *What is MIMO* [Online] 1. 1. 2007 [Citace: 28. 5. 2014] Dostupné z: <http://www.intel.com/support/wireless/sb/cs-025345.htm>
- [7] INTEL *Helping define IEEE 802.11 and other Wireless LAN Standards* [Online] [Citace: 29. 5. 2014] Dostupné z: <http://www.intel.com/content/dam/www/public/us/en/documents/case-studies/802-11-wireless-lan-standards-study.pdf>
- [8] AGILENT *Wireless LAN at 60GHz – IEEE 802.11ad Explained* [Online] 30. 5. 2013 [Citace: 10. 7. 2014] Dostupné z: <http://cp.literature.agilent.com/litweb/pdf/5990-9697EN.pdf>
- [9] PRNEWSWIRE *WiGig market – worldwide forecasts, business models, technology roadmap, analysis (2014 – 2019)* [Online] 12. 5. 2014 [Citace: 12. 7. 2014] Dostupné z: <http://www.prnewswire.com/news-releases/wireless-gigabit-wigig-market-ieee-80211ad-60-ghz-7gbps-wi-fi-wireless-gigabit-alliance-access-points-routers-residential-gateways-backhaul-equipment---worldwide-forecasts-business-models-technology-roadmap-and-anal-258915951.html>

- [10] HABRAHABR *802.11ad (WiGig) - дальность и полезность* [Online] 5. 6. 2014
[Citace: 12. 7. 2014] Dostupné z: <http://habrahabr.ru/post/228779/>
- [11] LUPA.CZ *Kvalita služby ve WLAN: 802.11e* [Online] 5. 2. 2004 [Citace: 13. 7. 2014] Dostupné z: <http://www.lupa.cz/clanky/kvalita-sluzby-ve-wlan-802-11e/>
- [12] CISCO.COM *Authentication, Authorization and Accounting Overview* [Online]
[Citace: 5. 8. 2014] Dostupné z:
http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.html#wp31053
- [13] ELEKTROREVUE.CZ *Univerzální autentizační rámec* [Online] 30. 3. 2009
[Citace: 22. 7. 2014] Dostupné z:
<http://www.elektrorevue.cz/cz/download/univerzalni-autentizacni-ramec/>
- [14] KLARA NAHRSTEDT *Quality of Services in Wireless Networks Over Unlicensed Spectrum* Carnegie Mellon University Morgan & Claypool 2012 ISBN 9781608457311
- [15] MIKROTIK *Mikrotik* [Online] [Citace: 9. 8. 2014] Dostupné z:
<http://www.mikrotik.com/>
- [16] ROUTERBOARD.SK *Přehled RouterBOARDů* [Online] [Citace: 13. 8. 2014]
Dostupné z: <http://www.routerboard.sk>
- [17] ROUTERBOARD.COM *RouterBOARD 500 Series User's Manual* [Online] [Citace 20. 8. 2014] Dostupné z: <http://routerboard.com/pdf/rb500ugM.pdf>
- [18] CISCO.COM *Cisco CleanAir Technology* [Online] [Citace 10. 9. 2014] Dostupné z: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/cleanair-technology/aag_c22-594304.pdf
- [19] CISCO.COM *Cisco ClientLink: Optimized Device Performance with 802.11n* [Online] [Citace 13. 9. 2014] Dostupné z:
http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/white_paper_c11-516389.pdf
- [20] CISCO.COM *Cisco Wireless Intrusion Prevention System* [Online] [Citace 17. 9. 2014] Dostupné z:
http://www.cisco.com/c/dam/en/us/products/collateral/wireless/adaptive-wireless-ips-software/at_a_glance_c45-504521.pdf

- [21] WIKIMEDIA.ORG *Struktura módů v IOS* [Online] [Citace 20. 9. 2014] Dostupné z: <http://upload.wikimedia.org/wikipedia/commons/thumb/0/04/Cisco-router-1.svg/1052px-Cisco-router-1.svg.png>
- [22] SAMURAJ-CZ.COM *Centrální řízení WiFi sítě* [Online] 3. 4. 2007 [Citace 1. 10. 2014] Dostupné z: <http://www.samuraj-cz.com/clanek/cisco-wlc-1-centralni-rizeni-wifi-site/>
- [23] HOTSPOTSYSTEM.COM *Billing Hotspot Solution* [Online] [Citace 5. 10. 2014] Dostupné z: <http://www.hotspotsystem.com>
- [24] INVOCOM *DCF Scheme* [Online] [Citace 8. 10. 2014] Dostupné z: http://www.invocom.et.put.poznan.pl/~invocom/C/P1-4/p1-4_en/p1-4_7_4.htm
- [25] PAYU.CZ *Platby na Internetu* [Online] [Citace 13. 10. 2014] Dostupné z: <http://www.payu.cz/>
- [26] PAYU.CZ *Implementační manuál PayU pro e-shopy* [Online] [Citace 13. 10. 2014] Dostupné z: http://www.payu.cz/sites/czech/files/dock/payu_implementation_manual_sablona.pdf
- [27] JON EDNEY, WILLIAM A. Arbaugh *Real 802.11 Security: WiFi protected access and 802.11i* Pearson Education Inc 2004 ISBN 0321136209
- [28] STEWART MILLER *Wi-Fi Security* McGraw Hill Professional 2003 ISBN 0071410732
- [29] NATHAN MULLER *Wi-Fi for the Enterprise* McGraw Hill Professional 2003 ISBN 0071429166
- [30] LEE BARKEN *Wireless Hacking: Projects for Wi-Fi Enthusiasts: Cut the cord and discover the world of wireless hacks!* Syngress 2004 ISBN 0080481787
- [31] NEIL P. REID, RON SEIDE *802.11 (Wi-Fi): Networking Handbook* McGraw-Hill/Osborne 2003 ISBN 0072226234
- [32] RADEK HORSKÝ *Bezdrátové sítě Wi-Fi v rekordním čase* Grada publishing a.s. 2006 ISBN 8024717905
- [33] TEIK-KHEONG TAN, BENNY BING *The World Wide Wi-Fi: Technological Trends and Business Strategies* John Wiley & Sons 2004 ISBN 0471478245
- [34] DENNIS BURGESS *Learn RouterOS* Lulu.com 2009 ISBN 055709271X

- [35] JESSE RUSSELL, RONALD COHN *Mikrotik Book on Demand* 2012 ISBN 5510759763
- [36] MAODE MA, MIESO K. DENKO *Wireless Quality of Service: Techniques, Standards and Applications* CRC Press 2008 ISBN 1420051318
- [37] DAVID D. COLEMAN, DAVID A. WESTCOTT *CWNA: Certified Wireless Network Administrator Official Study Guide: Exam PW0-105* John Wiley & Sons 2012 ISBN 111812779X