Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií
Obor informatika

Bakalářská práce

Problematika bezdrátových sítí v pásmech 2,4 GHz a 5 GHz

Martin DVOŘÁK

Vedoucí bakalářské práce: Ing. Jiří Vaněk, Ph.D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Dvořák Martin

Informatika

Název práce

Problematika bezdrátových sítí v pásmech 2,4 GHz a 5 GHz

Anglický název

Aspects of wireless networks in 2,4 GHz and 5 GHz bands

Cíle práce

Hlavní cíl

Cílem bakalářské práce je představit problematiku budování a provozu bezdrátových sítí v pásmech 2,4 GHz a 5 GHz ve velkoměstech a jejich okolí.

Dílčí cíle

- Seznámení s historickým a budoucím vývojem technologie Wi – Fi .
- Objasnění problematiky zabezpečení Wi – Fi sítí, představení používaných zabezpečovacích mechanismů.
- 2,4 GHz a 5 GHz Wi - Fi - používané technologie pro venkovní a vnitřní nasazení.
- Autorovy osobní zkušenosti s výstavbou a provozem venkovních Wi -Fi sítí v Praze a okolí.

Metodika

První část práce je věnována úvodu do bezdrátových technologií, včetně jejich historie, aktuálně používaných zařízení a frekvencí a budoucího vývoje bezdrátových technologií Wi-Fi.

Dále jsou v práci uvedeny aktuálně nejpoužívanější zabezpečovací mechanismy Wi - Fi sítí.

V další části je řešena problematika nasazení Wi-Fi technologií ve venkovním ale i vnitřním prostředí a autorovy zkušenosti s reálným provozem. Na závěr bude provedeno srovnání a hodnocení řešené problematiky.

Harmonogram zpracování

Studium odborných informačních zdrojů, stanovení dílčích cílů a postupu řešení: 06/2012

Zpracování přehledu řešené problematiky: 07/2012 – 08/2012

Vypracování vlastního řešení, diskuse, doporučení a závěry: 09/2012 - 02/2013

Tvorba finálního dokumentu práce: 02/2013 – 03/2013

Odevzdání práce a tezí: 03/2013

Rozsah textové části
30 - 40 stran

Klíčová slova
Bezdrátové sítě, Wi-Fi, 2,4 GHz, 5Ghz, IEEE 802.11a/b/g/n, IEEE 802.11ac.

Doporučené zdroje informací

HORÁK, J. Vytváříme domácí bezdrátovou síť, . Vyd. 1. Brno: Computer Press, 2011. 296 s.
BARKEN, L. Wi-Fi: Jak zabezpečit bezdrátovou sít. Vyd. 1. Brno: Computer Press, 2004. 174 s.
ZANDL, P. Bezdrátové sítě WiFi: praktický průvodce. Vyd. 1. Brno: Computer Press, 2003. 190 s.
BRISBIN, S. Wi-Fi: Postavte si svou vlastní Wi-Fi sít. Vyd. 1. Praha: Neocortex, 2003.248 s.
KöHRE, T. Stavíme si bezdrátovou síť Wi-fi. Vyd. 1. Brno, Computer Press, 2004. 295 s.

Vedoucí práce
Vaněk Jiří, Ing., Ph.D.

Termín odevzdání
březen 2013

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 15.1.2013

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Problematika bezdrátových sítí v pásmech 2,4 GHz a 5 GHz" jsem vypracoval samostatně, pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou v práci citovány a uvedeny v seznamu na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2013

…….

Martin Dvořák

Poděkování

Rád bych na tomto místě poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za cenné připomínky a odborné rady, kterými přispěl k vypracování této bakalářské práce. Dále děkuji svým kolegům, kteří mi poskytli potřebné informace.

Problematika bezdrátových sítí v pásmech 2,4 GHz a 5 GHz

Aspects of wireless networks in 2,4 GHz and 5 GHz bands.

Souhrn

Práce prezentuje úvod do bezdrátových technologií v pásmech 2,4 GHz a 5 GHz, včetně historického vývoje, aktuálně používaných zařízení, frekvencí a jejich budoucího vývoje. Dále jsou v práci uvedeny nejpoužívanější zabezpečovací mechanismy Wi-Fi sítí. V poslední části je pak uvedena problematika nasazení Wi-Fi technologií ve venkovním a vnitřním prostředí a autorovy poznatky a zkušenosti s reálným provozem.

Summary

Bachelor thesis presents introduction into wireless networks in bands 2,4 GHz and 5 GHz, including historical development, currently used technologies and frequencies and their future development.Further, there are listed the most used security mechanisms in Wi-Fi networks. In the last part there is the issue of using Wi-Fi technologies in outdoor as well as indoor environments and the author's knowledge and real life experience.

Klíčová slova: Bezdrátové sítě, Wi-Fi, 2,4 GHz, 5 GHz, IEEE 802.11a/b/g/n, IEEE 802.11ac.

Keywords: Wireless networks, Wi-Fi, 2,4 GHz, 5 GHz, IEEE 802.11a/b/g/n, IEEE 802.11ac.

Obsah

1 Úvod

Bezdrátové sítě zažívají v posledních přibližně 10 letech obrovský rozmach. Jsou široce využívány jak uvnitř budov, hal a skladů, kde slouží především k připojení mobilních zařízení, tak i ve venkovním prostředí pro propojení bod-bod nebo bod-multibod. Bezdrátový přístupový bod má dnes téměř každá domácnost, kde se používají tablety, chytré telefony nebo přenosné počítače. Venkovní Wi-Fi sítě jsou obzvláště v ČR často využívanou a oblíbenou technologií a to především díky často nekvalitní nebo neexistující metalické nebo optické infrastruktuře v řadě menších měst a vesnic. Výjimkou ale nejsou také některé městské části Prahy či jiných velkých měst, kde je kvalita starých telefonních rozvodů pro použití ADSL nebo VDSL technologie nedostačující.

Ve venkovním prostředí se zprvu rozvinuly sítě v pásmu 2,4 GHz, kde ovšem za velmi krátký čas došlo na mnoha místech k totálnímu zahlcení pásma a tím pádem nepoužitelnosti Wi-Fi technologie na vzdálenosti delší než 300 metrů. ČTÚ (Český telekomunikační úřad) v roce 2005 povolil na území ČR používat pásmo 5 GHz. Od této chvíle nastal skutečný rozmach venkovních Wi-Fi sítí a rovněž začalo rychle přibývat poskytovatelů bezdrátového připojení k internetu. Pásmo 5 GHz má totiž podstatně vyšší povolený vysílací výkon, větší propustnost, 5x více použitelných kanálů a rovněž menší odezvy při přenosu dat, než pásmo 2,4 GHz. V tomto pásmu není problém postavit relativně kvalitní spoj na vzdálenost 5 až 10 km, což je dnes v pásmu 2,4 GHz naprosto nereálné.

Bezdrátové sítě se provozují i v jiných pásmech, avšak převážně jako spoje bod-bod. Dnes nejpoužívanějšími jsou pásma 10 GHz, 11 GHz, 17 GHz, 24 GHz, 32 GHz, 60 GHz a 80 GHz. Infrastrukturní sítě využívají například také pásmo 3,5 GHz (technologie WiMAX a Wi-Fi). Zde je ovšem značný rozdíl v ceně technologií, kde zařízení pro pásma 2,4 GHz a 5 GHz stojí v řádech stovek až tisíců korun, oproti tomu tyto profesionální spoje stojí desetitisíce až statisíce korun. Za tuto cenu však uživatel získá velmi kvalitní spoj, který je schopen pokrýt i ty nejvyšší nároky na přenos dat.

V této práci jsou charakterizována pásma 2,4 GHz a 5 GHz, je zde představen historický vývoj Wi-Fi standardů, včetně představení budoucích sítí 4. generace. Rovněž jsou v práci charakterizovány nejpoužívanější zabezpečovací mechanismy Wi-Fi sítí a také problematika nasazení těchto technologií v praxi, ve vnitřním i venkovním prostředí.

Na závěr jsou v práci sděleny autorovy zkušenosti, které si osvojil během dlouholeté výstavby a provozu vlastní bezdrátové sítě rozkládající se na území Prahy a v jejím okolí.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této práce je představení problematiky budování a provozování vnitřních a venkovních bezdrátových sítí ve volných pásmech 2,4 GHz a 5 GHz, a to především uvnitř velkoměst a v jejich přilehlém okolí.

Dílčími cíli jsou:

- Seznámení s historickým a budoucím vývojem technologie Wi–Fi.
- Vysvětlení základních principů přenosu dat dle standardů 802.11a, 802.11b, 802.11g a 802.11n.
- Problematika zabezpečení Wi–Fi sítí a představení aktuálně používaných zabezpečovacích mechanismů.
- Aktuálně používané technologie pro venkovní a vnitřní nasazení Wi–Fi technologií.
- Autorovy zkušenosti s výstavbou a provozem venkovních Wi–Fi sítí v Praze a jejím okolí.

2.2 Metodika

První část práce je věnována historickému vývoji technologie Wi–Fi v pásmu 2,4 GHz. Dále je zde zhodnocen vývoj pásma 5 GHz a to zejména od roku 2005, kdy bylo toto pásmo v ČR schváleno jako pásmo volné. Od roku 2005 doznalo pásmo 5 GHz obrovských změn a oproti dnes přeplněnému pásmu 2,4 GHz je stále hojně využívané pro venkovní instalace. Závěrem této kapitoly je představení možného budoucího vývoje Wi - Fi technologie v následujících letech a charakteristika modelu sítí 4. generace.

Ve druhé kapitole jsou vysvětleny základní principy fungování Wi–Fi sítí dle standardů 802.11a, 802.11b, 802.11g a 802.11n s konkrétní charakteristikou jednotlivých standardů, které zahrnují technologii rozprostřeného spektra, více druhů modulací signálu, různé přenosové rychlosti, frekvence a také technologie MIMO a protokol TDMA.

V další kapitole jsou vysvětleny principy zabezpečení Wi-Fi sítí od nejjednodušších jako je vypnutí vysílání SSID nebo přístup omezený seznamem MAC adres, přes silnější WEP nebo WPA šifrování až po aktuálně používané WPA2 šifrování.

Dále jsou v práci představeny aktuálně používané technologie Wi–Fi pro venkovní a vnitřní nasazení a to včetně souvisejícího hardware, jakým jsou antény, koaxiální kabely, routery a speciální zařízení pro provoz technologií na atypických místech.

Závěrem jsou do práce zahrnuty autorovy zkušenosti s výstavbou a téměř sedmiletou správou dnes poměrně rozsáhlé struktury Wi–Fi sítí v Praze a jejím okolí. Do této kapitoly jsou zařazeny především zajímavé a užitečné zkušenosti z praxe týkající se výstavby a provozu venkovních Wi–Fi sítí. Na konci práce je zhodnocen vliv a význam Wi–Fi sítí na telekomunikačním trhu.

3 Historický vývoj a budoucnost Wi–Fi technologie

Základy bezdrátových sítí tak, jak je známe nyní, byly položeny v roce 1997, kdy organizace IEEE vydala standard IEEE 802.11.

Ovšem úplně první zmínky o technologii, kterou standard 802.11 využíval, pocházejí již z období druhé světové války, kdy bylo zapotřebí vyvinout rádiovou komunikaci pro ovládání raket a torpéd tak, aby nepřítel nemohl toto spojení dešifrovat, či do něj dokonce zasahovat.

Patent na tuto technologii byl vydán v roce 1942 a v sedmdesátých letech byla technologie poprvé použita v praxi, konkrétně pro rádiovou komunikaci námořnictva USA.

3.1 Historie

Wi–Fi technologie se od svého vzniku neustále vyvíjí, a tak vznikly postupně čtyři základní standardy, které se od sebe liší přenosovými rychlostmi, použitou frekvencí, ale také různými možnostmi využití.

3.1.1 Frekvence

Wi–Fi technologie používá celkem tři různá frekvenční pásma. Jsou to volná pásma 2,4 GHz a 5 GHz a licencované pásmo 3,5 GHz.

U pásma 2,4 GHz je celkem 13 kanálů vzájemně vzdálených 5 MHz, které se při standardní šířce kanálu 20 MHz, respektive 22 MHz, vzájemně překrývají, a tím pádem ruší. Kanály, které se při vzájemném používání neruší, jsou v tomto pásmu jen tři. V pásmu 5 GHz je celkem 26 vzájemně se nerušících kanálů, které jsou od sebe vzdáleny 20 MHz, což je přibližně 8krát více dostupných kanálů než u pásma 2,4 GHz.

Pásmo 5 GHz bylo v ČR schváleno jako volné pásmo až v roce 2005. Základní šířka kanálu je zde rovněž 20 MHz. V případě technologie MIMO také 40 MHz respektive 2x20 MHz. Šířku kanálu je však možné u obou pásem měnit. (3)

3.1.2 Standardy 802.11

Standard 802.11

Norma 802.11 byla vydána v roce 1997. Dnes se již prakticky nepoužívá, protože má nedostačující přenosovou rychlost, která dosahuje maximálně 2 Mbps a v druhé řadě není kompatibilní s novějšími standardy, z důvodu použití rozdílných modulací signálu.

Obrázek 3-1 - Wi-Fi CERTIFIED logo.

Standard 802.11b

Nástupcem 802.11 je standard 802.11b, který byl vydán v roce 1999. Umožňuje dosahovat až 5x vyšší přenosové rychlosti oproti svému předchůdci a je možné na něj stále narážet, především z důvodu vyšší odolnosti vůči rušení, než u jeho nástupců ve stejném frekvenčním pásmu.

Standard 802.11g

Je dalším standardem pro pásmo 2,4 GHz, který umožňuje přenášet data teoretickou rychlostí až 54 Mbps. Využívá jinou modulaci, než starší 802.11b, což je zároveň také jeho hlavní nevýhodou, jelikož má díky tomu poměrně nízkou odolnost vůči okolnímu rušení.

Standard 802.11a

Tento standard byl schválen v roce 1999, přibližně ve stejnou dobu jako standard 802.11b. Je to de facto stejný standard jako 802.11g, ale odlišuje se především využívanou frekvencí, tedy 5 GHz. Dalším rozdílem je pak podstatně větší počet kanálů než v pásmu 2,4 GHz.

Standard 802.11n

Dosud poslední oficiálně vydaný standard, který dosahuje přibližně 6krát vyšších přenosových rychlostí, než předchozí standardy 802.11g a 802.11a. Tento standard využívá

technologie MIMO (Multiple Input Multiple Output). Zařízení podporující tento standard disponují více anténami, zpravidla dvěma nebo třemi. Tento standard podporuje pásmo 2,4 GHz i pásmo 5 GHz a je rovněž zpětně kompatibilní se staršími standardy 802.11a, 802.11b a 802.11g. Nominální rychlost činí 300 Mbps.

Obrázek 3-2 – Wi-Fi karta pro pásmo 2,4 GHz s 3x3 MIMO technologií.

Vývoj standardu 802.11n

Standard 802.11n doznal od svého vydání v roce 2009 dalších vylepšení, díky kterým je komunikace ve venkovním prostředí stabilnější, rychlejší a kvalitnější i v nepříznivých podmínkách, jako například při vyšší míře rušení, špatných klimatických podmínkách, rozdílné kvalitě signálů klientských zařízení při topologii bod-multibod a podobně.

Řešením je použití protokolu TDMA (Time Division Multiple Access). Jedná se o časový multiplex, kdy každá stanice má vyhrazený určitý čas neboli časový slot, ve kterém může komunikovat. V případě, že žádná z klientských stanic nemá problémy s komunikací, jsou časové sloty pro všechny stanice stejně velké. Pokud začne mít některá klientská stanice z jakéhokoli důvodu problémy při přenosu dat, přístupový bod změní velikost časového slotu pro tuto stanici tak, aby ovlivňovala komunikaci s ostatními stanicemi, například z důvodu opakovaného přenosu dat, co nejméně. Jednotlivé informace o standardech IEEE 802.11 byly čerpány ze zdrojů (3),(5).

3.2 Budoucnost

Budoucnost Wi-Fi, ale i ostatních bezdrátových technologií, spočívá především ve zvyšování přenosových rychlostí, vyšší kvalitě spojení a zejména zlepšení mobility.

Rovněž se uvažuje o zavedení SIM karty do klientských zařízení. Ta bude zajišťovat autentizaci zařízení, podobně jako je tomu u mobilních sítí a uživatel tak nebude muset zadávat žádné heslo nebo vkládat certifikáty.

3.2.1 Standard 802.11ac

Standard 802.11ac je od roku 2007 až doposud stále ve vývoji, avšak routery s podporou 802.11ac je již dnes možné koupit. Tento standard je schopen dosáhnout teoretické přenosové rychlosti až 3,4 Gbps, což je oproti 300 Mbps u standardu 802.11n velký skok. Tento standard využívá pouze frekvenci 5 GHz a to především z důvodu šířky kanálu, která se pohybuje od 40 MHz do 160 MHz, a tím pádem by se při plné šíři ani nebylo možné do pásma 2,4 GHz vejít.

Velkou nevýhodou tohoto standardu bude rušení od okolních Wi-Fi zařízení na frekvenci 5 GHz. Zatímco u 802.11n byla šířka kanálu maximálně 40 MHz, tedy dva standardní kanály, při šířce kanálu 160 MHz už je to 8 kanálů. V praxi se v případě standardu 802.11a vešlo do 5 GHz pásma 26 vzájemně se nerušících zařízení. Při použití plné šíře kanálu u standardu 802.11ac to budou pouze 3 zařízení. Další nevýhodou je nutnost v praxi použít ještě větší počet antén, než u standardu 802.11n. Pro plnou přenosovou rychlost jsou to 4 antény.

3.2.2 Sítě 4. generace

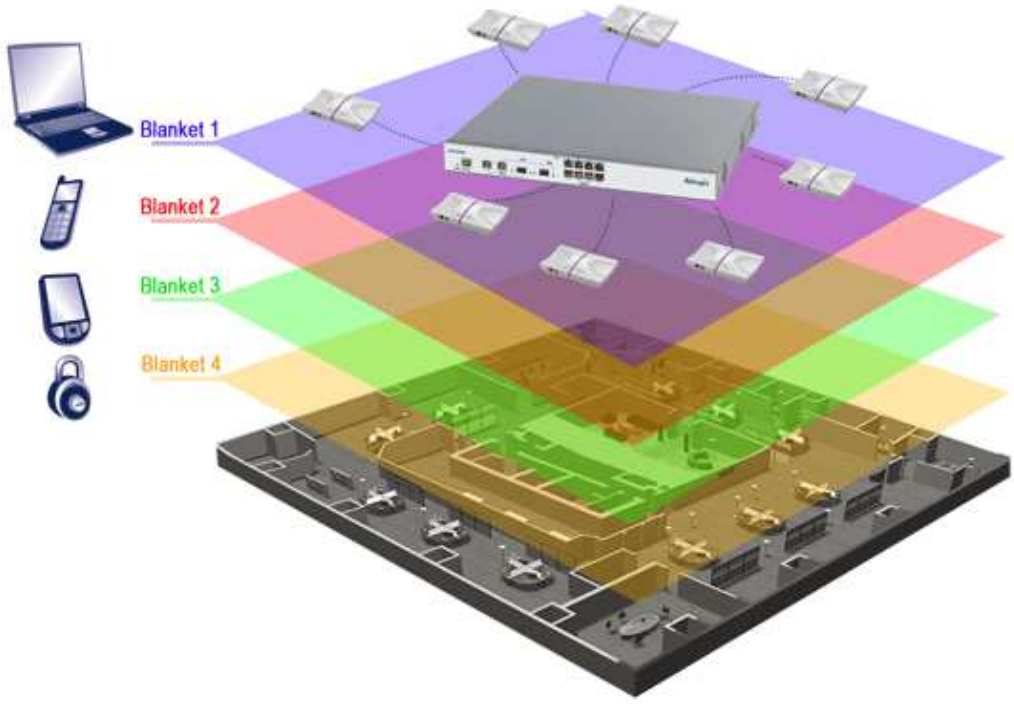
Čtvrtá generace Wi-Fi sítí přináší zásadní změnu v celkovém dosavadním vývoji. Zatímco u sítí 1., 2. a 3. generace se používaly fyzicky oddělené přístupové body, takzvané buňky, vysílající na různých kanálech, ve 4. generaci se díky použití blanket technologie chovají jednotlivé přístupové body jako jeden a rovněž jsou všechny naladěny na stejný kanál, aniž by se vzájemně rušily.

Jinak řečeno, máme-li dnes pro pokrytí větší budovy, například univerzity, velké firmy apod. použito 20 přístupových bodů, potom při pohybu budovou se bude klientské zařízení připojovat vždy na přístupový bod s aktuálně nejsilnějším signálem. Z tohoto důvodu bude docházet k výpadkům spojení. Ve 4. generaci se všechny tyto přístupové

body chovají pro klientská zařízení jako jeden fyzický bod. Klientské zařízení se tedy nemá důvod neustále připojovat k bodu s nejsilnějším signálem, protože se všechny fyzické přístupové body tváří jako jeden bod.

Všechny přístupové body blanket technologie jsou řízeny centrálním řídícím prvkem, který je synchronizuje. Z tohoto důvodu je možné mít vedle sebe několik přístupových bodů na stejném kanále.

Další výhodou je optimalizace sítě pro všechny typy Wi-Fi zařízení. Je tedy možné postavit síť tak, aby přístupové body podporovaly paralelně všechny dostupné standardy, tedy 802.11a, 802.11b, 802.11g a 802.11n. Řešení spočívá v použití přístupových bodů s více fyzickými vysílači, kdy je pro každý standard vyhrazen jeden samostatný vysílač a nedochází tak v případě připojení staršího zařízení k ovlivnění přenosové rychlosti všech zařízení připojených na daný přístupový bod, jako je tomu v případě sítí 3. generace. Informace o sítích 4. generace čerpány ze zdroje (21)

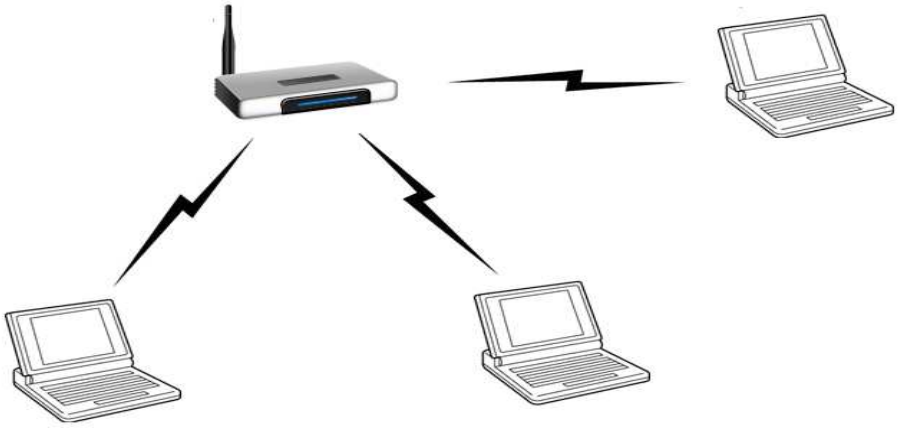


Obrázek 3-3 - Schéma Wi-Fi blanket technologie.

4 Základní principy fungování Wi-Fi sítí

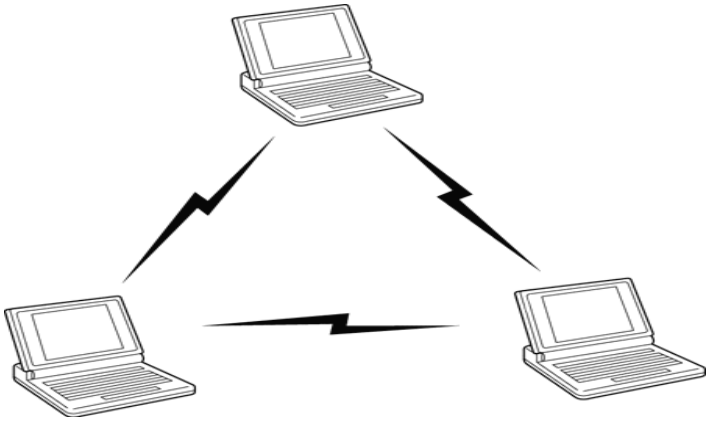
4.1 Topologie Wi-Fi sítí

Topologie Wi-Fi sítí se dělí do dvou základních skupin. Rozšířenější skupinou jsou takzvané infrastrukturní sítě neboli BSS/ESS (Basic Service Set/Extended Service Set) s přístupovým bodem, na který se připojují jednotlivá klientská zařízení. Přístupový bod slouží jako řídící prvek a řídí veškerou komunikaci v síti. (4)



Obrázek 4-1 – Schéma infrastrukturní sítě.

Druhou skupinou jsou sítě typu ad-hoc, neboli IBBS (Independent Basic Service Set), kde není žádný přístupový bod a síť vzniká přímo propojením jednotlivých klientských zařízení. Tento druh sítí se využívá většinou na dočasné propojení počítačů například za účelem výměny dat a podobně. (3)



Obrázek 4-2 – Schéma sítě ad-hoc mezi přenosnými počítači.

4.2 Standard 802.11

Dle (5) pracuje na frekvenci 2,4 GHz, je zde použita modulace FHSS nebo DSSS, šířka pásma je 1 MHz nebo 22 MHz, v závislosti na použité modulaci. Nominální přenosová rychlost 2 Mbps.

FHSS (Frequency Hopping Spread Spectrum). Jedná se o modulaci používající technologii přeskakování mezi několika frekvencemi za určitý časový úsek. V tomto případě v pásmu 2,4 GHz, kde je vyhrazeno celkem 79 kanálů, každý se šířkou 1 MHz. Změna frekvence je pseudonáhodná.

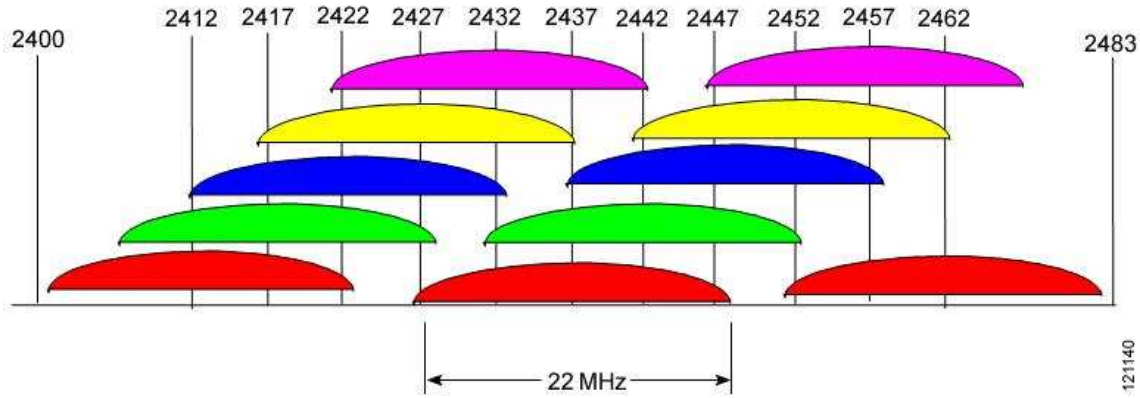
FHSS se dále dělí dle rychlosti přeskoků na dvě podkategorie. První z nich je FFH (Fast Frequency Hopping), kdy dochází ke změně frekvence i během přenosu jednotlivých bitů, druhá je SFH (Slow Frequency Hopping), kdy dochází ke změně frekvence vždy po přenesení určité skupiny bitů. Standard 802.11 využívá model SFH.

Technologie FHSS je díky frekvenčním skokům závislá na správné časové synchronizaci přijímače a vysílače. Její výhody spočívají ve vysoké odolnosti vůči rušení, teoreticky je možné vedle sebe v jeden okamžik provozovat až 26 vysílačů, prakticky o něco méně, což je u jiných modulací z rodiny standardu 802.11 v pásmu 2,4 GHz zcela nemožné. Nevýhoda FHSS je v nízké přenosové rychlosti z důvodu úzké šířky pásma.

Tento typ modulace dosáhl nepříliš velkého rozšíření, avšak ještě donedávna bylo na tyto sítě možné narazit. Jedná se například o populární zařízení od firmy Alvarion zvané BreezeNet. Dnes už jsou tato zařízení vzácností a to především z důvodu nedostačující propustnosti a rušení novějších technologií v pásmu 2,4 GHz.

DSSS (Direct Sequence Spread Spectrum) je druhá modulace použitá u standardu 802.11. Jedná se o techniku přímého rozprostřeného spektra. Princip přenosu dat spočívá v použití nadbytečnosti. K jednomu bitu vysílaných dat se připojí další pseudonáhodně vygenerované bity a takto zakódovaná data se odešlou. Na jeden bit reálných dat připadá 7 pseudonáhodně vygenerovaných bitů. Vysílaný signál se poté ostatním přijímačům jeví jako šum a bez znalosti pseudonáhodně vygenerovaného klíče nejsou schopni správná data žádným způsobem získat. Výhodou této technologie je také vysoká schopnost opravit doručená data v případě jejich částečného poškození a to dokonce i v případě, že jsou poškozeny 3 bity z celkových 8.

Tato modulace používá kanál o šířce 22 MHz a dosahuje nominální přenosové rychlosti 2 Mbps. Díky rozprostřenému spektru je poměrně odolná vůči rušení, avšak nevýhodou je existence pouze tří samostatných, nerušících se kanálů v pásmu 2,4 GHz. Proto je možné provozovat paralelně jen tři vzájemně se nerušící bezdrátové sítě.



Obrázek 4-3 – Kanály v pásmu 2,4 GHz.

4.3 Standard 802.11b

Zde je použita upravená modulace HR-DSSS, tedy stejný systém jako u 802.11. HR-DSSS znamená High Rate-DSSS. Dosahuje nominální rychlosti až 11 Mbps. Je prvním globálně rozšířeným Wi-Fi standardem a dodnes jej podporují všechny vyráběné Wi-Fi zařízení pro pásmo 2,4 GHz. Reálná rychlost se za optimálních podmínek pohybuje kolem 6 Mbps.

Po nástupu 802.11g v roce 2003 se zdálo, že se 802.11b stane minulostí, stejně jako jejich předchůdce 802.11, ale není tomu tak. Standard 802.11g používá modulaci OFDM (Orthogonal Frequency Division Multiplexing), která má relativně velké potíže i s nižší úrovní rušení a proto je dnes na mnoha venkovních přístupových bodech opět používán starší 802.11b, jelikož komunikace přes 802.11g je v místech s vysokým rušením velmi nestabilní. Zpravidla tam, kde 802.11g již není schopná přenášet data ani na nejnižší přenosové rychlosti, se při přepnutí na starší 802.11b dostaneme až na rychlost 5 Mbps. (4)

4.4 Standard 802.11a

Byl vydán v roce 1999, tedy zároveň se standardem 802.11b. V té době byla nominální rychlost v pásmu 2,4 GHz pouze 11 Mbps. Tento standard pracuje v pásmu

5 GHz. Používá modulaci OFDM, která byla později použita také ve standardu 802.11g. Díky této modulaci dosahuje nominální rychlosti 54 Mbps.

Pásmo 5 GHz má oproti pásmu 2,4 GHz několik výhod. První z nich je 26 vzájemně se nerušících kanálů, další výhodou je vysoká nominální přenosová rychlost a nakonec také vyšší stabilita přenosu. Celková šířka pásma činí přibližně 500 MHz, zatímco u 2,4 GHz je to necelých 80 MHz. Toto pásmo nalezlo využití převážně ve venkovních sítích, kde prakticky nahradilo již nepoužitelné pásmo 2,4 GHz. Je možné s ním bez problému provozovat spojení na více než 10 km, s reálnou přenosovou rychlostí kolem 30 Mbps.

Modulace OFDM (Orthogonal Frequency Division Multiplexing) je multiplex s kmitočtovým dělením. Standardní šířka kanálu je 20 MHz, avšak je možné používat také poloviční šířku 10 MHz nebo čtvrtinovou šířku 5 MHz. Snížením šířky kanálu dojde rovněž ke snížení přenosové rychlostí na nominálních 27 Mbps, respektive 13,5 Mbps. Toho využijeme například v případě rušení, které je v poslední době problémem také v pásmu 5 GHz. V jednom standardním 20 MHz kanálu je tak možné paralelně provozovat až 4 bezdrátové sítě se šířkou kanálu 5 MHz. Informace o standardu 802.11a byly čerpány ze zdrojů (3),(4).

4.5 Standard 802.11g

Vychází v roce 2003 jako nástupce 802.11b. Jeho hlavním cílem je zvýšení nominální přenosové rychlosti až na 54 Mbps. Je zde použita modulace OFDM.Tento standard je prakticky shodný s 802.11a, kde jediným rozdílem je použité pásmo. Díky použití OFDM je 802.11g prakticky nepoužitelná ve větších městech, jelikož je extrémně náchylná k rušení, které je v pásmu 2,4 GHz vysoké nejen díky rozšíření technologie Wi-Fi, ale i jiných technologií jako je například Bluetooth či některé domácí bezdrátové telefony pracující rovněž v pásmu 2,4 GHz. Z důvodu rušení od okolních zařízení dochází ke ztrátám spojení nebo minimálně k výraznému snížení jeho kvality. Na některých místech již dosáhlo rušení takové úrovně, že je často problémem i uvnitř budov a bytů. Například na sídlištích v Praze není žádná výjimka nalézt uvnitř bytu s běžným notebookem až 20 Wi-Fi sítí. Na střeše vyšších panelových domů pak obvykle nalezneme více než 100 sítí. Pokud vezmeme v potaz, že paralelně se dají provozovat jen tři nerušící se bezdrátové sítě, je úroveň rušení opravdu velká. (3)

4.6 Standard 802.11n

Byl vydán v roce 2009. Jedná se o menší revoluci v bezdrátových sítích, jelikož tento standard používá MIMO technologii. Přijímač a vysílač tak disponuje větším počtem antén, typicky dvěma až čtyřmi. Jedná se o první standard, který podporuje obě frekvenční pásma a zároveň je kompatibilní i se staršími standardy. Dosahuje nominální rychlosti 300 Mbps, reálně kolem 120 Mbps. Používá stejně jako 802.11a a 802.11g modulaci OFDM.

802.11n umožňuje taktéž použití více komunikačních rychlostí, které se určují pomocí MCS (Modulating and Coding Scheme). Celkový počet modulačních a kódových schémat (MCS) je 77. Díky nim je možné nastavit mezi vysílačem a přijímačem komunikaci v módu SISO (Single Input Single Output), tedy jedna anténa na každé straně, tak jako u starších standardů z rodiny 802.11 a nebo 2x2 MIMO či 3x3MIMO s dvěma nebo třemi anténami na každé straně.

4x4 MIMO se čtyřmi anténami existuje pouze na teoretické úrovni a v praxi se zatím nepoužívá. Jeho nominální rychlost činí 600 Mbps.

Obrázek 4-4 – Router podporující 802.11n s 3x3 MIMO pro pásmo 2,4 GHz.

5 Možnosti zabezpečení Wi-Fi sítí

Bezdrátové sítě mají velkou nevýhodu, jelikož jejich provozovatel v podstatě nikdy přesně neví, kde všude je signál sítě možné zachytit. Navíc s použitím výkonných externích antén je možné síť zachytit v podstatně větších vzdálenostech od vysílače, než například s integrovanými anténami v přenosných počítačích. Naopak u kabelových sítí je možné připojení vždy jen tam, kde je vedena jejich strukturovaná kabeláž. Z těchto důvodů byly postupně zavedeny různé typy zabezpečení, které lze rozdělit do dvou hlavních skupin. První skupinou je řízení přístupu uživatelů do sítě neboli autorizace. Druhou skupinou je šifrování přenášených dat mezi klientským zařízením a přístupovým bodem. Jednotlivé možnosti zabezpečení jsou charakterizovány v následujícím textu, bylo čerpáno ze zdrojů (1), (2), (3), (5).

5.1 Řízení přístupu do sítě - autentizace

U bezdrátových sítí je na rozdíl od kabelových sítí potřeba používat řízení přístupu uživatelů. U kabelových sítí je možné řídit přístup pomocí speciálních přepínačů, u nichž je možné spravovat jednotlivé porty a ponechat tak aktivní jen ty, které jsou fyzicky propojené s počítači či dalším zařízeními anebo umístit přepínače do prostor, kam se dostanou jen povolané osoby.

U bezdrátových sítí není možné nikdy přesně určit pokryté území a tak je třeba jiných mechanismů k omezení přístupu uživatelů. Standard 802.11 má dvě základní metody autentizace. První z nich je metoda open-system, kdy je síť přístupná každému, kdo zná její název neboli SSID. Použití této metody je však zároveň nutnou podmínkou pro komunikaci v jakékoli Wi-Fi síti. Bez znalosti SSID není možná komunikace klientského zařízení s přístupovým bodem.

Druhým typem autentizace je metoda shared-key. Tato metoda se používá ve spojení s WEP šifrováním. Podstata autentizace spočívá v klíči, který je nutno zadat do každého zařízení, které se chce do takto zabezpečené sítě připojit.

Klientské zařízení požádá přístupový bod o připojení, přístupový bod odešle náhodný text tomuto zařízení. Zařízení tento text zakóduje podle klíče, který jsme mu zadali, a odešle zpět přístupovému bodu. Ten tato data dekóduje podle klíče, který má nastavený. Pokud se původní odeslaná data shodují s dekódovanými daty,

má klientské zařízení zadáno správný klíč a je mu umožněn přístup do sítě. V opačném případě je přístup zamítnut.

5.2 Skrytí názvu Wi-Fi sítě

Jedná se o nejjednodušší formu zabezpečení Wi-Fi sítě, kterou je možné velmi jednoduše obejít. SSID (Service Set Identifieer), neboli název sítě, je řetězec znaků, který přístupové body pravidelně vysílají a které vidíme při vyhledávání dostupných sítí na klientském zařízení.

SSID se musí shodovat na obou komunikujících stranách, tedy u přístupového bodu i u klientského zařízení, jinak nemůže probíhat komunikace. Na přístupových bodech je možné vypnout vysílání SSID, respektive zapnout funkci skrytí SSID. V případě, že se útočník chce do takto zabezpečené sítě prolomit, není to pro něj při použití správného programu vůbec žádný problém. Přístupový bod sice SSID nevysílá, ale klienti, kteří jsou na něj připojeni a komunikují, vysílají SSID v paketech, které posílají přístupovému bodu. Útočníkovi tak stačí některý z paketů odchytit a SSID z něj přečíst. Potom už mu v připojení k síti nic nebrání.

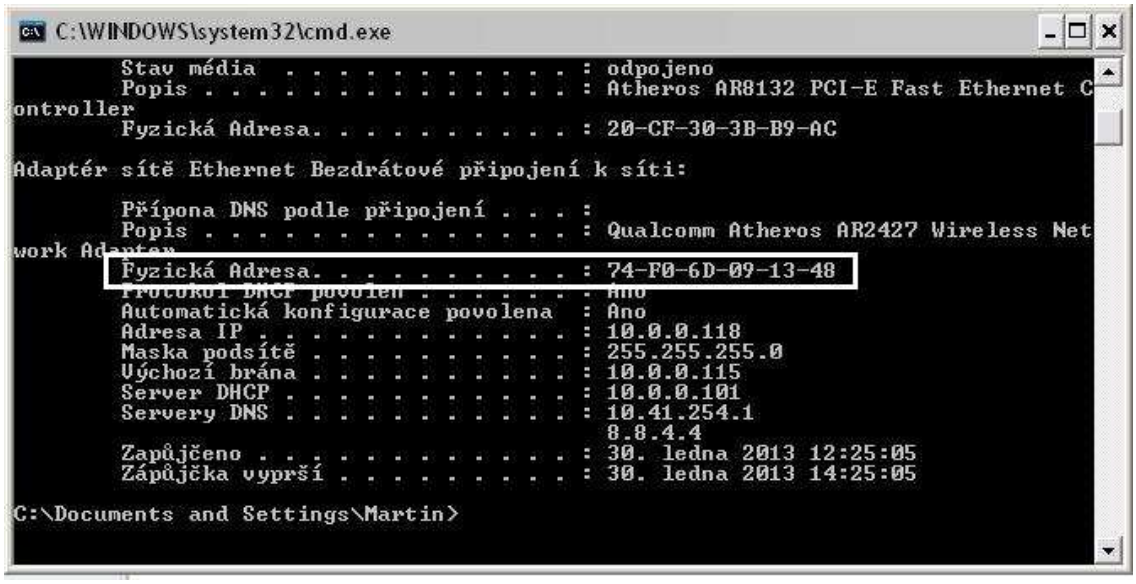
5.3 Filtr MAC adres

Další možností zabezpečení je použití filtru MAC adres. V přístupovém bodu se vytvoří seznam MAC adres, který je možné aplikovat dvojím způsobem. Buďto mají zařízení na seznamu MAC adres přístup k síti zakázán a všechny ostatní zařízení se mohou připojit anebo se naopak mohou připojit jen zařízení, jejichž MAC adresa je v seznamu a žádné jiné zařízení se nepřipojí.

Problém takového zabezpečení spočívá v tom, že pakety, které si mezi sebou zařízení předávají, obsahují MAC adresu odesílatele i příjemce, tudíž prolomení je téměř stejně rychlé a jednoduché jako při zabezpečení pomocí skrytého SSID. Stačí odchytit paket z komunikace klienta a přístupového bodu a přečíst si z něj MAC adresu klienta. Poté stačí změnit MAC adresu útočníkova zařízení na stejnou MAC adresu jakou má některý z připojených klientů. Nyní se útočníkovo zařízení bude tvářit jako zařízení, které má přístup v seznamu MAC adres povolen a tudíž mu nic nebrání se do sítě připojit.

Nevýhodou této metody je, že přístupový bod neumožní připojení dvou zařízení se stejnými MAC adresami naráz. Situace většinou dopadne tak, že zařízení, které má skutečně přístup povolený, se po útoku do sítě většinou nepřipojí, protože útočník

použije agresivní metodu, pomocí které si vynutí přednost připojení a tím druhé zařízení vyřadí z komunikace.

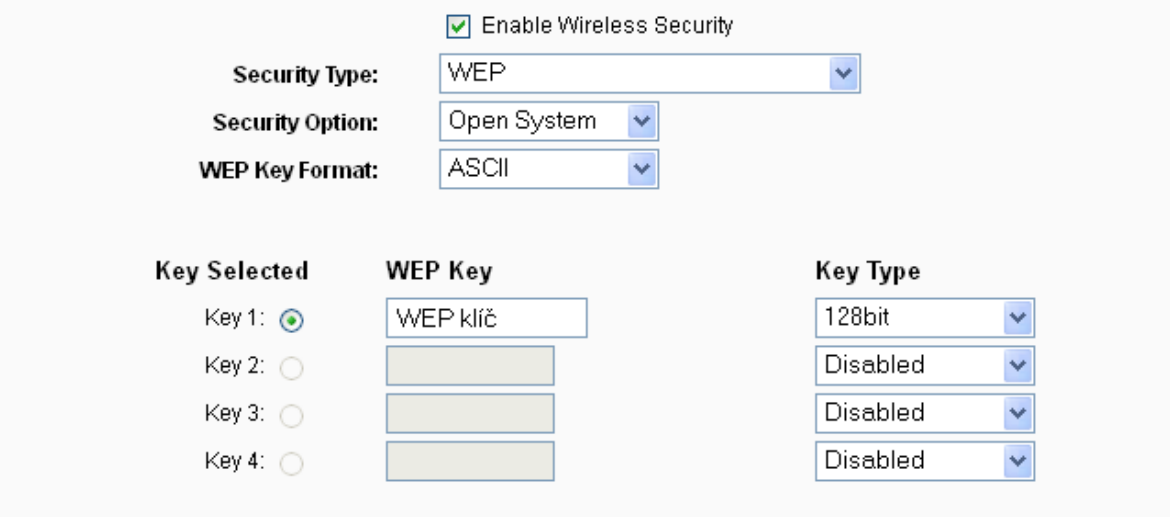


Obrázek 5-1 –Výpis fyzické (MAC) adresy Wi-Fi karty v OS MS Windows XP.

5.4 WEP šifrování

Dle (2) je WEP (Wired Equivalent Privacy) standard pro zabezpečení Wi-Fi sítí, který zabezpečuje komunikaci mezi klientským zařízením a přístupovým bodem. Používá symetrickou streamovou šifru RC4. Podle této šifry se data na straně odesílatele zašifrují a na straně příjemce opět dešifrují. Klíč se vždy přizpůsobuje délce odesílaných dat rozšířením pomocí pseudonáhodného inicializačního vektoru na délku odesílaných dat. Samotné šifrování probíhá pomocí logické operace XOR mezi daty a klíčovacím streamem. Obdobně pak probíhá dešifrování na straně příjemce.

Problémem tohoto zabezpečení je distribuce bezpečnostního klíče, který musí znát všechna komunikující zařízení v rámci sítě. Klíč je navíc zapotřebí ručně zadat do každého jednotlivého zařízení, čímž se výrazně snižuje celková úroveň zabezpečení, především díky účasti lidského faktoru.



Obrázek 5-2 –Nastavení 128bitového WEP klíče u 2,4 GHz Wi-Fi sítě.

5.4.1 Délka klíče

Samotný standard WEP podporuje pouze 40bitovou respektive 64bitovou délku klíče, která je často prezentována výrobci a prodejci zařízení, avšak není správná. Délka samostatného šifrovacího klíče je pouze 40bitů, před které se připojí 24bitů inicializačního vektoru. Inicializační vektor zajišťuje pseudonáhodnost celého klíčovacího streamu.

Výrobci časem zahrnuli do svých zařízení podporu i delších WEP klíčů než je základních 40bitů. Problémem však je, že delší klíče samotný standard nepodporuje a tak se může stát, že některá zařízení nejsou schopna s delšími klíči pracovat. Jedná se o klíče s délkou 128bitů, 192bitů a 256bitů.

5.4.2 Síla WEP šifrování

WEP šifrování bylo prolomeno již v roce 2001. V tomto roce byl rovněž vydán program AirSnort, určený k rekonstrukci WEP klíčů, který je schopen ovládat téměř každý mírně pokročilý uživatel počítače. S tímto programem je možné prolomit 64bitový WEP klíč během 6 až 12 hodin. Záleží především na velikosti provozu v dané bezdrátové síti.

Hlavní slabina WEP šifrování spočívá ve způsobu použití inicializačního vektoru. Inicializační vektor je totiž používán i v jiných, mnohem bezpečnějších šifrovacích systémech. Jedná se o otevřený text, tudíž není problém získat jeho přibližný vzhled a díky jeho znalosti je následně možné rozluštit i samotný WEP klíč.

Druhým problémem je délka šifrovacího klíče. Například klíč o délce 128bitů zajistí pouze dvojnásobnou dobu nutnou k prolomení, oproti času potřebného k prolomení 64bitového klíče. Délka času, nutného k prolomení klíče, v poměru k délce klíče tak nestoupá exponenciálně, ale pouze lineárně, tudíž delší klíč nepředstavuje v případě útoku o mnoho větší překážku.

5.5 WPA zabezpečení

WPA (Wi-Fi Protected Access) je bezpečnostní mechanismus vydaný v roce 2002 jako nástupce prolomeného WEP. Technologie WPA vychází ze standardu 802.11i, který byl v té době ještě ve vývoji, nicméně bylo třeba co nejrychleji vydat nástupce prolomeného WEP a nebylo tudíž možné čekat na dokončení a vydání kompletního 802.11i standardu. WPA přijímá ze standardu 802.11i jak šifrování komunikace mezi přístupovým bodem a klientskými stanicemi tak i řízení přístupu uživatelů do sítě. Zároveň bylo třeba, aby měla i většina starších zařízení vyrobených před vydáním WPA mechanismu možnost toto zabezpečení dodatečně použít a vyhnout se tak slabému WEP šifrování. WPA byl vyvinut pouze jako softwarový update, který podporuje i starší hardware. Na starší zařízení byly vydány nové verze firmware s podporou WPA a stačil tedy jen update firmware.

Výjimkou však byly některé přístupové body, které díky slabšímu výkonu procesoru nebyly schopné WPA používat, z důvodu jeho vyšší náročnosti na výpočty klíčů než tomu je u WEP šifrování.

5.5.1 Protokol TKIP

Pro šifrování komunikace je použit protokol TKIP, který využívá stejného šifrovacího algoritmu jako WEP, ale s dvakrát delší, tedy 128bitovou šířkou klíče. Tento klíč má navíc každé zařízení jiný, jelikož se klíč mimo jiné tvoří dle MAC adresy odesílatele. Inicializační vektor, který je rovněž použit u WEP šifrování má u WPA dvojnásobnou délku, tedy 48bitů, což značně prodloužilo jeho vyčerpání na rozdíl od WEP, kde se 24bitový inicializační vektor v síti s vyšším provozem vyčerpal již během několika hodin a poté se začal opakovat znovu od 0, což usnadňuje prolomení WEP šifry. TKIP na rozdíl od WEP akceptuje inicializační vektory pouze v rostoucí číselné řadě a hodnoty mimo tuto číselnou řadu jsou ignorovány, na rozdíl od WEP kde toto pořadí není kontrolováno a je tak možné podstrkovat podvržené pakety. Další zásadní

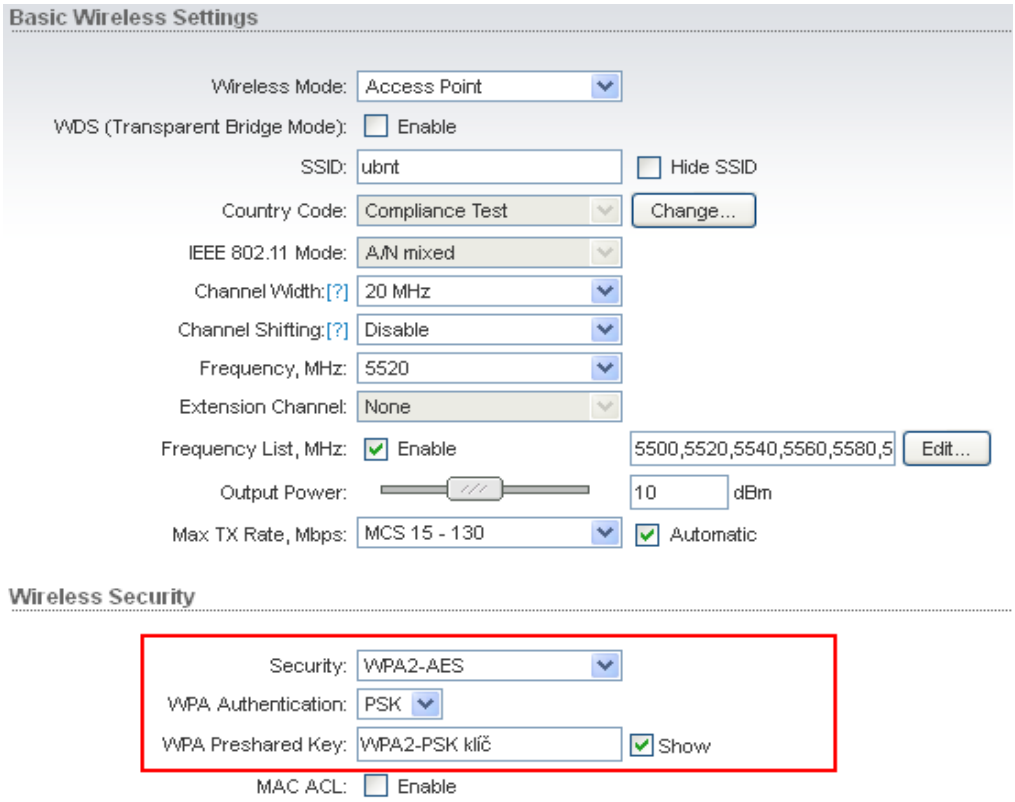
změnu představuje dynamický dočasný klíč. WEP měl tento klíč statický a neměnil se po celou dobu komunikace. TKIP mění dočasný klíč u klíčového mechanismu každých 10 000 paketů, na rozdíl od WEP šifrování, kde byl klíč statický. (5)

5.5.2 Autentizace

WPA podporuje dva druhy autentizace. Prvním je autentizace pomocí 802.1x, například serverem RADIUS. Tento typ autentizace je často používán ve větších sítích. V domácích sítích by se často jednalo o příliš složité a nákladné řešení. Proto byl do WPA přidán ještě druhý způsob autentizace pomocí tzv. Pre-Shared Key (PSK). Jedná se o klíč, který se zadává do všech zařízení, které se připojují do sítě. Je to tedy podobný mechanismus jako u WEP, avšak s tím rozdílem, že WPA používá tento klíč pouze jako text, podle kterého se odvozují konečné šifrovací klíče. WEP používal šifrovací klíč pouze jeden, WPA však mění šifrovací klíče každých 10 000 paketů. Bezpečnost distribuce klíče do klientských zařízení je na stejné úrovni jako u WEP, avšak šifrování komunikace v bezdrátové síti má podstatně vyšší úroveň zabezpečení, než při použití WEP.

5.6 WPA2, 802.11i zabezpečení

Standard 802.11i, rovněž označovaný jako WPA2, byl vydaný v roce 2004 a je nyní posledním a nejsilnějším zabezpečením, které lze ve Wi-Fi sítích používat. Jedná se o nástupce standardu WPA, který částečně ze standardu 802.11i vychází. Největší změna přišla s použitím blokové šifry AES (Advanced Encryption Standard). Předchůdcem AES je šifra DES (Data Encryption Standard) používaná v USA od 80. let, která používá algoritmus s 56bitovým symetrickým klíčem. DES je však v dnešní době již nepoužitelná z důvodu neustále se zvyšujícího výpočetního výkonu. Byla prolomena již v roce 1997.



Obrázek 5-3 –Nastavení WPA2-PSK klíče u 5 GHz Wi-Fi zařízení.

5.6.1 Šifra AES, protokol CCMP

AES je stejně jako DES symetrická bloková šifra, která používá k šifrování a dešifrování dat stejný klíč. AES však na rozdíl od DES používá delší klíč. Můžeme nastavit klíče o délce 128bitů, 192bitů a 256bitů.

Zatímco u předcházejících šifrování WEP a WPA je použita proudová šifra RC4, která šifruje data bit po bitu, AES šifruje data po blocích o délce 128bitů. Samotný AES pracuje ve více režimech. Ve standardu 802.11i je použit v módu CCMP (Counter Cipher Mode Protocol).

5.6.2 Autentizace EAP

WPA2 podporuje, stejně jako WPA, dva druhy autentizace. Jedná se o autentizaci protokolem 802.1x nebo před-sdíleným klíčem WPA2-PSK. Tento klíč je opět třeba zadat do všech zařízení, která se připojují do sítě. Jedná se o mechanismus podobný WPA. Rozdílem však je použití mnohem silnějšího šifrování přenášených dat v síti než u WPA nebo WEP. Problémem je však i nadále distribuce klíče do klientských

zařízení, kde je stále třeba lidského faktoru. Důležitou změnou je pak použití autentizačního protokolu EAP (Extensible Authentication Protokol), který definuje přibližně 40 metod autentizace. Jedna z metod je použita například u GSM sítí mobilních operátorů. Jedná se o EAP-SIM, tedy použití SIM karty jako ověřovacího prostředku. Tuto metodu se v budoucnu chystají výrobci zavést právě ve Wi-Fi sítích 4. generace.

Standard 802.11i používá metodu EAP-TLS (EAP-Transport Layer Security). Tuto metodu podporuje většina Wi-Fi zařízení. Ve spojení se serverem RADIUS se jedná o poměrně robustní zabezpečení. Slabinou však mohou být ověřovací certifikáty klientských zařízení. Každé klientské zařízení rovněž potřebuje privátní klíč, což je jedna z překážek, díky které se metoda TLS příliš nerozšířila. Privátní klíč je možné snadno distribuovat například pomocí čipových karet.

5.7 Protokol 802.1x

Jedná se o protokol, který řídí přístup jak do bezdrátových tak i do kabelových počítačových sítí. Byl vyvinut zároveň s rozšířením počítačů mezi širokou veřejnost. Dříve nebylo zabezpečení nutné, jelikož počítače používaly pouze k tomu určené osoby a ostatní k nim neměli přístup, natož možnost získat z nich jakákoli data.

5.7.1 Autentizace pomocí 802.1x

Připojí-li se klientské zařízení k síti, má zablokován veškerý přístup mimo autentizačního protokolu EAP. Přístupový bod bezdrátové sítě provádí autentizaci buď na základě seznamu, který je uložen přímo v přístupovém bodu a nebo pomocí externích autentizacích systémů jakými jsou například server Kerberos nebo server RADIUS (Remote Authentication Dial on User Service). Autentizace pomocí 802.1x se často kombinuje například s VPN (Virtual Private Network), kdy se autorizované zařízení dostane jen do veřejné části sítě a následně se pomocí šifrovaného VPN připojí k interní privátní síti.

5.7.2 Server RADIUS

Dle (3) se jedná o protokol, který řídí autentizaci, autorizaci a uživatelské účty. Pouze ověření uživatelé tak mají přístup do sítě. Může být použit v lokální síti,

ale rovněž také formou roamingu, kdy jeden či více serverů zajišťuje přístup do více bezdrátových či kabelových sítí v rámci jednoho podniku.

Proces autentizace pomocí protokolu 802.1x se dělí do 4 kroků. Prvním krokem je odeslání žádosti o připojení klientem přístupovému bodu, označovaného jako NAS (Network Access Server), který následně požádá klienta o sdělení totožnosti pomocí protokolu EAP. V dalším kroku klient odpoví zprávou s jeho identifikačními údaji. Přístupový bod tyto údaje přepošle serveru RADIUS. Ve třetím kroku server RADIUS ověří údaje o klientovi a odešle zpět přístupovému bodu zprávu s povolením nebo zamítnutím přístupu, kterou přístupový bod následně přepošle klientovi. V posledním kroku je v případě úspěšné autentizace povolen klientovi přístup a jsou mu zaslána nastavení nutná ke komunikaci v síti.

5.8 Alternativní možnosti zabezpečení Wi-Fi sítě

Mimo zabezpečení na softwarové úrovni existují také jiné možnosti zabezpečení bezdrátových sítí. V kancelářích je například možné použít primitivní, avšak velmi účinné řešení pomocí časových spínačů u napájení přístupových bodů, které připojují přístupové body k elektrické síti jen v pracovní době. Mimo tuto dobu jsou tak vypnuty a tím pádem není možné provést jakýkoliv pokus o prolomení zabezpečení. (3)

Další možností zabezpečení je nedávný japonský vynález v podobě speciálního nátěru na zeď na bázi hliníku, který slouží jako stínění. Jedná se o stejný efekt, jako kdyby se celý dům zabalil do alobalu. Tento nátěr odstíní rádiové vlny v rozmezí 1 GHz až 180 GHz. Tudíž není možné bezdrátovou síť mimo vyhrazené území vůbec zachytit.

Tyto metody zabezpečení jsou samozřejmě náročnější na údržbu a realizaci než softwarové metody, avšak existují místa, kde je možné je bez větších problémů uplatnit.

6 Aktuálně používané Wi-Fi technologie

Díky neustálému konkurenčnímu boji výrobců Wi-Fi zařízení přichází každý rok několik nových vylepšení stávajících standardů, které se týkají zejména přenosových rychlostí, kvality spojení a výkonnějších procesorů, které umožňují vyšší počet připojených zařízení na jeden přístupový bod při zachování vysoké kvality a bezpečnosti přenosu a také zajišťují vyšší propustnost sítě.

6.1 Technologie v pásmu 2,4 GHz

Ačkoli je pásmo 2,4 GHz na mnoha místech přeplněné a tím pádem často špatně použitelné, jedná se stále o nejvíce používané pásmo. Důvodem je zaprvé mnohem lepší prostupnost překážkami než v pásmu 5 GHz, kde činí překážky podstatně větší problém. Dalším důvodem ještě donedávna byla také cena zařízení pro pásmo 2,4 GHz, která byla mnohonásobně nižší, než cena zařízení pro pásmo 5 GHz. Dalším důvodem je menší podpora pásma 5 GHz v klientských stanicích, kam i dnes výrobci často integrují jen přijímač pro frekvenci 2,4 GHz. Výrobci přístupových bodů tento trend akceptují a proto je v dnešní době možné vybírat z bezpočtu domácích přístupových bodů, popřípadě i přijímacích zařízení pro pásmo 2,4 GHz, zatímco u pásma 5 GHz je na výběr jen z omezeného sortimentu.

V pásmu 2,4 GHz přišlo se standardem 802.11n mnoho dalších zařízení, která slibovala lepší dosah uvnitř budov, kde je pomocí systému MIMO možné přijímat více různých odrazů téhož signálu a vybrat vždy ten nejkvalitnější. Největším problémem nejen MIMO technologie ale také SISO technologie jsou železobetonové zdi nebo kovové konstrukce, které signál utlumí často na nepoužitelnou úroveň. Technologie MIMO má v takovýchto objektech často ještě daleko větší potíže než starší SISO technologie.

6.2 Technologie v pásmu 5 GHz

Dle (3) bylo pásmo 5 GHz v České republice schváleno pro volný provoz v roce 2005. V této době byla technologie pro toto pásmo poměrně drahá a výběr byl úzký. Další nevýhodou je horší prostupnost přes překážky, tudíž toto pásmo nedosáhlo, co se týče použití uvnitř budov, velkého rozšíření. Naopak co se týče venkovních bezdrátových sítí, zde nastal s povolením pásma 5 GHz obrovský rozmach. Stávající vysílače a spoje bod – bod již byly díky stále se zvyšujícímu zahlcení pásma 2,4 GHz

prakticky nepoužitelné a tak většina provozovatelů postupně měnila 2,4 GHz technologii za novou, v pásmu 5 GHz. Pásmo 5 GHz má navíc v reálném provozu lepší stabilitu, odezvu a přenosovou rychlost než pásmo 2,4 GHz a je možné s ním u spojů bod-bod dosahovat několikanásobně větších vzdáleností.

6.2.1 Standardy 802.11a a 802.11n

Zatímco v přeplněném pásmu 2,4 GHz byla rychlost spoje maximálně 10 Mbps a kvalita spojení velmi kolísavá, standard 802.11a umožňuje komunikaci reálnou rychlostí až 30 Mbps, navíc s nesrovnatelně vyšší kvalitou spojení. Tento standard, dříve hojně využívaný, je dnes nahrazován standardem 802.11n, který umožňuje reálnou přenosovou rychlost až 70 Mbps. S využitím šířky pásma dvou 20 MHz kanálů pak až 120 Mbps. Ve vnitřním prostředí není pásmo 5 GHz příliš rozšířeno a výrobci se tak věnují převážně technologiím pro venkovní nasazení. Dnes jsou na trhu pro koncové uživatele dostupné výrobky firem MikroTik a Ubiquity. Oba výrobci používají ve svých zařízeních odlišné technologie, díky kterým je možné dosahovat výrazně vyšších rychlostí, než umožňuje samotný standard 802.11a. Problémem je, že tyto technologie nejsou vzájemně kompatibilní, a tak, chceme-li plně využívat všechny dostupné protokoly a ne pouze základní standard 802.11a, je vždy nutné používat v jedné síti pouze zařízení od jednoho výrobce.

6.2.2 MikroTik NStreme

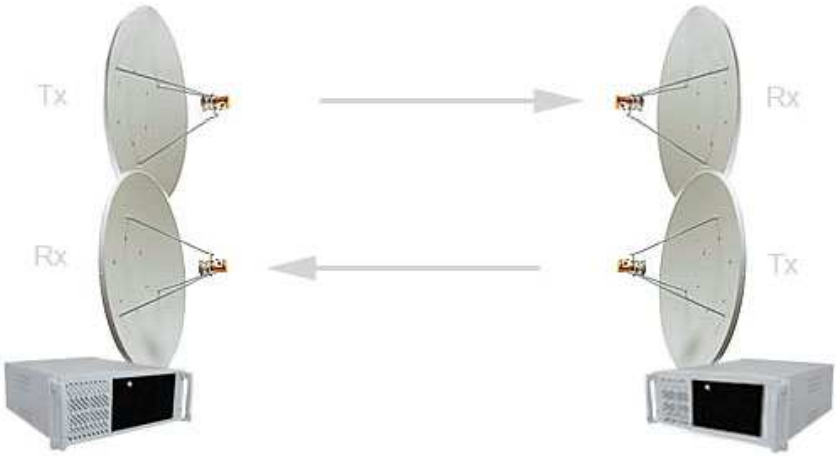
Jedná se o protokol, který dosahuje vyšších rychlostí než samotný standard 802.11a díky tomu, že nepřenáší kontrolní rámce. V bezdrátových sítích dochází během přenosu dat k mnoha chybám a tak je třeba posílat společně s daty také kontrolní rámce, díky kterým je možné na druhé straně rozpoznat, zdali byla data přenesena bezchybně anebo nikoli. Protokol NStreme tyto kontrolní rámce vynechává, díky čemuž uvolní část přenosové rychlosti, která se využívá pro přenos těchto rámců a umožní místo nich přenos reálných dat, čímž zvýší propustnost sítě. (6)

6.2.3 MikroTik NStreme Dual

Společnost MikroTik vyvinula technologii, která umožňuje budovat v pásmu 5 GHz plně duplexní spoje. Plně duplexní spoje jsou schopné přenášet data stejnou rychlostí tam i zpět zároveň. Technologie Wi-Fi je však od začátku konstruována pro half duplexní přenos.

Sdílí jedno přenosové pásmo pro oba směry komunikace zároveň. Vysílat tak vždy může jen jedna strana a druhá přijímá. Pokud potřebují vysílat obě strany, pak se musí ve vysílání střídat, což celou komunikaci zpomaluje. Technologie Dual NStreme tento problém odstraňuje a zrychluje jak přenosovou rychlost, tak i odezvu spoje. Dual NStreme potřebuje na obou stranách spoje dvě rádiové karty a dvě antény, kdy jedna karta data vysílá a druhá přijímá a na druhé straně je tomu naopak. Jedná se tak o dva fyzicky oddělené spoje, které se na softwarové úrovni tváří jako spoj jeden.

Jelikož technologie Nstreme vynechává kontrolní rámce, je velmi náchylná na jakékoli rušení, překážky mezi přijímačem a vysílačem a také na kvalitu použitých komponent. Je tedy třeba použít kvalitnější hardware, konkrétně se jedná o kvalitní antény, kvalitní koaxiální kabely a rádiové karty. Výslednou přenosovou rychlost spoje tak ovlivňuje především kvalita hardware, kdy za použití nekvalitních komponent může být komunikační rychlost i poloviční oproti rychlosti, kterou dosáhneme s kvalitními komponenty.



Obrázek 6-1 – Schéma spoje na technologii MikroTik Dual Nstreme.

6.2.4 Mikrotik NV2 a Ubiquity AirMax

Jedná se o technologie založené na stejném principu, tedy protokolu TDMA (Time Divison Multiple Access). Protokol TDMA umožňuje přístup klientských stanic do sítě pomocí časového rozdělení přístupů. Každá stanice tak má vyhrazený předem daný čas, po který může komunikovat. Firma Ubiquity navíc přidala časové řízení přístupů jednotlivých stanic dle jejich kvality signálu. Pokud mají všechny stanice podobnou kvalitu signálu, má každá z nich vyhrazen stejný časový úsek pro komunikaci. Má-li však některá

ze stanic výrazněji horší nebo naopak lepší signál než ostatní, potom se délka jejího vysílacího času mění tak, aby zbytečně opakovaným vysíláním nezatěžovala síť a nezpomalovala tak komunikaci ostatních stanic. Informace o protokolech TDMA a NV2 čerpány ze zdroje (6).

7 Stavba venkovních bezdrátových sítí

Bezdrátové sítě našly využití také v oblasti venkovního nasazení, kde často zastupují jiné, mnohonásobně dražší technologie. Jedná se o sítě FWA (Fixed Wireless Access), kde se donedávna nasazovaly pouze profesionální datové spoje s pracovní frekvencí 9 GHz a vyšší. Pořizovací cena těchto datových spojů se dodnes pohybuje v řádech desítek až stovek tisíc korun.

Technologie Wi-Fi se tak po svém nástupu na trh stala na mnoha místech náhradou za tyto drahé spoje. Jednalo se zejména o použití při distribuci internetového připojení pro domácnosti a malé firmy, takzvaná poslední míle a také všude tam, kde nejsou požadovány vysoké nároky na kvalitu spojení. Problémem však zezačátku byla nedostupnost technologií určených pro venkovní instalaci. S venkovním nasazením Wi-Fi totiž ze začátku nikdo nepočítal. Uživatelé však začali k zařízením určených pro vnitřní provoz připojovat pomocí koaxiálních kabelů směrové či sektorové antény s vysokým ziskem, díky kterým bylo možné v pásmu 2,4 GHz budovat spoje i na vzdálenost několika stovek metrů či jednotek kilometrů.

Postupem času však došlo k značnému rozšíření vysílačů v pásmu 2,4 GHz a takto vybudované spoje, díky stále se zvyšujícímu zahlcení pásma, ztrácely na kvalitě a zejména přenosové rychlosti.

V roce 2005 přichází v ČR otevření pásma 5 GHz a velká část majitelů venkovních sítí v pásmu 2,4 GHz vyměňuje své dosluhující spoje za nové, v pásmu 5 GHz. Výhodou pásma 5 GHz byla větší dostupnost zařízení určených pro venkovní instalace než v pásmu 2,4 GHz, ovšem za podstatně vyšší ceny, než zařízení pro vnitřní instalace. Z tohoto důvodu se stejně, jako u pásma 2,4 GHz, používala zařízení určená k vnitřní instalaci a montovala se do vodotěsných rozvaděčů a skříní přímo na anténní stožár. Vzdálenost mezi rádiovým zařízením a anténou je omezena koaxiálním kabelem, na kterém dochází k útlumu signálu. Z tohoto důvodu není zpravidla vhodné překračovat vzdálenost delší než 7 metrů. Umístěním přístupového bodu přímo na stožár byl vyřešen problém s délkou koaxiálního kabelu, ale vznikl problém s napájením rádiového zařízení.

Tento problém vyřešil příchod technologie PoE (Power over Ethernet), kdy je zařízení napájeno pomocí datového kabelu UTP, který se skládá ze čtyř kroucených

párů vodičů. Po dvou párech kabelu probíhá datová komunikace a po zbývajících dvou nevyužitých párech je zařízení napájeno.

Postupem času však začali výrobci vyrábět speciální vodotěsné boxy s integrovanou anténou, určené pro instalaci na stožár či anténní držák. Do boxu pak stačilo vložit pouze přístupový bod a připojit UTP kabel.

Poslední novinkou v oblasti venkovních Wi-Fi zařízení jsou antény, které mají elektroniku přístupového bodu integrovanou přímo ve své konstrukci. Zařízení vypadá podobně jako obyčejná směrová nebo sektorová anténa, jen má místo klasického N konektoru vstup pro UTP kabel. V následujících podkapitolách jsou představeny aktuálně používané technologie, informace byly čerpány ze zdrojů (1), (3), (4), (5).

7.1 Wi-Fi přístupové body a routery

Přístupový bod neboli AP (Access Point) je zařízení, které zajišťuje přenos dat mezi rádiovým pásmem, tedy Wi-Fi, a metalickou nebo optickou infrastrukturou počítačové sítě. Pracuje výhradně v režimu síťového mostu.

Další kategorií jsou routery s podporou Wi-Fi. Na první pohled od přístupového bodu téměř nerozeznatelné zařízení, avšak s podporou mnoha síťových režimů. Zatímco přístupový bod podporuje pouze režim síťového mostu, router umí data, která jím procházejí, dále zpracovávat. Jedná se například o routovací tabulky, firewall, pravidla pro řízení rychlosti, směrování portů a podobně. V dnešní době většina zařízení umí pracovat v obou módech.

Mnoho výrobců začalo vyrábět přístupové body určené pro venkovní instalaci. Elektronika zůstává zpravidla stále stejná, jen je doplněna o přepěťové ochrany, možnost napájení pomocí PoE technologie a je umístěna do speciálních vodotěsných boxů.

Obrázek 7-1 – Venkovní přístupový bod CISCO s anténním systémem 3x3 MIMO.

7.2 Antény

Stejně jako u jiných rádiových technologií, i u Wi-Fi se používá několik různých druhů antén. Každá z nich je určena pro jiné využití a tyto zásady je nutné pro kvalitní komunikaci v síti dodržovat a rovněž je po uživatelích sítě striktně vyžadovat.

7.2.1 Polarizace

Bezdrátový přenos používá dvou základních polarizací rádiových vln. Jedná se o polarizaci lineární a polarizaci kruhovou. Chceme-li dosáhnout při spojení co nejlepších výsledků, je nutné použít jak na straně vysílače, tak i na straně přijímače, shodné polarizace. V případě, že toto není dodrženo, dochází ke ztrátám přijímaného signálu a může docházet k chybám v přenosu dat.

Více druhů polarizace využijeme zejména v místech, kde je rádiové pásmo přeplněné a dochází tím ke snížení rychlosti či výpadkům v přenosu dat. Změnou polarizace potlačíme rušení od okolních sítí přibližně o 20 dB. Wi-Fi používá převážně lineární polarizaci a to horizontální nebo vertikální. Vertikální polarizace je ve městech dnes zpravidla nepoužitelná, jelikož většina vysílačů, včetně domácích přístupových bodů pracuje právě s touto polarizací. Proto je i a na místech s velkou hustotou Wi-Fi sítí možné v horizontální polarizaci stále dosáhnout uspokojivé kvality spojení.

Druhý typ polarizace je kruhová polarizace, která se dělí na pravotočivou a levotočivou. Zatímco u lineární polarizace je možné změnit vertikální polarizaci na horizontální pouhým otočením antény o 90°, změna kruhové polarizace možná není, protože závisí přímo na konstrukci zářiče antény.

7.2.2 Zisk antény

Zisk je u antény nejdůležitějším parametrem. Máme-li anténu s malým ziskem, nejsme schopni zachytit žádný vzdálenější signál. Jednotlivé typy antén mají odlišný zisk. Všesměrové antény mají zpravidla zisk nejmenší. Větší zisk mají antény sektorové a největšího zisku dosahují antény směrové.

Zisk antény se nejčastěji udává v jednotkách dBi (decibel na isotop)

7.2.3 Anténa všesměrová

S tímto typem antén je možné se setkat u každého přístupového bodu určeného pro vnitřní použití. Jedná se o anténu, která vyzařuje signál v úhlu 360°. Tento typ antén se používá pouze u přístupových bodů, jelikož je díky vyřazovacímu úhlu možné pokrýt velkou plochu pomocí jediné antény. Všesměrové antény nejčastěji disponují vertikální polarizací, jelikož výroba horizontálních všesměrových antén je mnohem složitější a nákladnější. Na trhu se ale vyskytují i všesměrové antény s horizontální polarizací.

V případě použití všesměrové antény u přijímacího zařízení způsobujeme zbytečné síření šumu do éteru a naopak sami nežádoucí šum z okolního éteru přijímáme v několikanásobně větším množství než při použití správné antény.

Obrázek 7-2– Vnitřní a venkovní všesměrová anténa pro pásmo 2,4 GHz.

7.2.4 Anténa sektorová

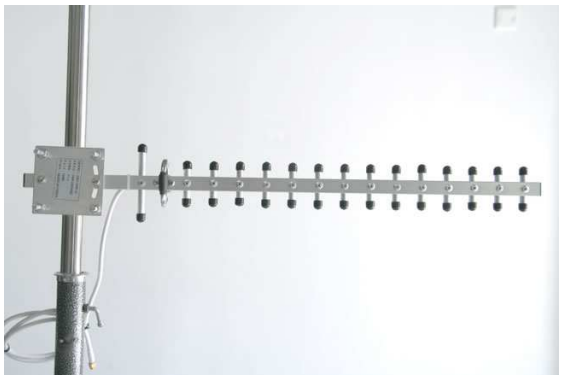
Sektorové antény se používají podobně jako všesměrové zejména na straně vysílačů. Jejich výhoda spočívá v menším vyzařovacím úhlu a tudíž vyšším zisku. Sektorové antény nečastěji disponují vyzařovacími úhly v rozmezí 25° až 180°. Sektorové antény s menším úhlem vyzařovaní se rovněž velmi často používají také na stranu přijímačů, jelikož jsou menší a především levnější než antény směrové. Toto řešení však není příliš rozumné, jelikož vyzařovací úhel je stále zbytečně velký a dochází opět k nežádoucímu vysílaní a přijímaní okolního šumu, ke kterému v případě použití směrové antény nedochází zdaleka v tak velké míře.

Obrázek 7-3– Venkovní sektorová 2x2 MIMO anténa pro pásmo 5 GHz.

7.2.5 Anténa směrová

Směrové antény se nejčastěji používají u spojů bod-bod. Rovněž se používají na straně přijímačů v sítích bod-multibod. Směrové antény dosahují největšího zisku ze všech dostupných typů antén a zároveň mají nejmenší vyzařovací úhly. Kvalitní směrová anténa pro pásmo 5 GHz má vyzařovací úhel pouhých 5°, pro pásmo 2,4 GHz pak přibližné 10°.

Směrových antén se vyrábí několik typů. Prvním z nich je anténa typu YAGI, dříve velmi oblíbená v pásmu 2,4 GHz pro svoji malou váhu a rozměry v poměru k vysokému zisku. Dnes se ve Wi-Fi sítích používá poměrně málo, avšak například pro příjem televizního signálu se jedná o nejrozšířenější typ antény, kterou můžeme vidět téměř na každém domě.



Obrázek 7-4 – Anténa typu YAGI pro pásmo 2,4 GHz.

Dalším typem směrové antény je síto. Jedná se o anténu s drátěným reflektorem, před kterým je umístěn zářič, který ozařuje reflektor. Anténa pracuje na podobném

principu jako například parabolické světlomety u automobilu, kde se světlo vyzářené žárovkou odráží v parabolickém reflektoru za žárovkou, a ten světlo odráží zpět dopředu v úzkém paprsku s mnohem vyšší intenzitou.

Předností antén s drátěným reflektorem je jejich nízký odpor vůči větru, tudíž se hodí na větrná místa nebo na místa, kde není možné přidělat kvalitní držák pro parabolické antény. Nevýhodou těchto antén je vyšší míra přijímaného šumu z okolí za anténou, jelikož drátěný reflektor neposkytuje dostatečné odstínění.

Posledním typem směrových antén je parabola. Jedná se o anténu s parabolickým reflektorem. Princip je stejný jako u antény typu síto, avšak tato anténa disponuje mnohem lepšími parametry. Především se jedná a dobré odstínění šumu přicházejícího zezadu.

U speciálních parabolických antén s límcem je pak odstíněn také všechen šum, který přichází ze stran a zepředu, mimo vyzařovací úhel dané antény.

Obrázek 7-5 – Parabolická anténa pro pásmo 5 GHz.

7.3 Konektory a koaxiální kabely

7.3.1 Koaxiální kabely

Stejně důležitý, jako výběr vhodné antény, je také výběr správného koaxiálního kabelu, kterým je anténa k Wi-Fi zařízení připojena. Koaxiálních kabelů se vyrábí celá řada. Pro technologii Wi-Fi je však důležité vybírat kabely s impedancí 50 ohmů. Pokud použijeme kabel s jinou impedancí, může docházet, stejně jako při použití nevhodné antény či její polarizace, ke snížení rychlosti a kvality přenosu či k výpadkům spojení.

Koaxiální kabely však často nejsou v dnešní době potřeba, jelikož nově vyráběné venkovní Wi-Fi zařízení již mají integrovanou elektroniku s rádiem přímo v anténě, tudíž stačí přivést pouze datový kabel UTP (Unshielded Twisted Pair) po kterém je zařízení možné rovněž napájet a odpadá tak použití koaxiálních kabelů.

Koaxiálních kabelů, určených pro Wi-Fi technologie, existuje několik druhů. Jejich nejdůležitější vlastností je mimo impedance také útlum neboli ztráta signálu na metr délky kabelu. V případě, že máme zařízení vzdálené od antény 5 až 7 metrů, je možné použít kabely s vyšším útlumem. Pro pásmo 2,4 GHz se jedná například o kabel s označením H155. Jeho průměr je přibližné 5mm. Jedná se o měkký a poddajný kabel, tudíž při manipulaci s ním nevznikají většinou žádné potíže. V případě, že máme zařízení od antény vzdálené více než 7 metrů, je nutné použít kabel s nižším útlumem. Pro pásmo 2,4 GHz se jedná například o kabel s označením H1000, který má dvakrát nižší útlum než kabel H155. Průměr kabelu H1000 je ale více než 1cm. Díky tloušťce je kabel poměrně dost tvrdý a velmi nepoddajný. Jakýkoli větší ohyb kabelu je tak problém.

7.3.2 Konektory

Poslední důležitou součást tvoří konektory. U Wi-Fi technologie se používají většinou čtyři druhy konektorů. Jedná se o konektory N, TNC, SMA a U.FL.

Konektory N a TNC jsou určeny pro venkovní použití. Jedná se o robustnější konektory větších rozměrů, přizpůsobené větším průměrům koaxiálních kabelů. Naopak konektory typu SMA a U.FL jsou určené pro vnitřní použití a na kabely s větším průměrem není možné tyto konektory montovat. N konektor je možné nalézt na většině venkovních antén. Naopak konektorem SMA disponuje většina přístupových bodů. Konektory U.FL jsou pak používány na rádiových kartách, které jsou součástí elektroniky přístupových bodů.

V případě, že od antény vedeme například kabel H1000 o průměru 1cm, nemáme možnost na něj namontovat SMA konektor pro připojení k přístupovému bodu. Tento problém se řeší speciální redukcí zvanou pigtail. Jedná se o krátký a tenký koaxiální kabel, který slouží jako redukce. Na jedné straně je opatřen velkým N konektorem a na druhé straně pak SMA nebo U.FL konektorem, díky kterému jej můžeme připojit k přístupovému bodu či přímo k rádiové kartě.

7.4 Přepěťové ochrany

Rádiová karta, ke které je připojena anténa, je velice náchylná na jakékoli přepětí na svém vstupu. V případě, že je anténa umístěna venku, hrozí nebezpečí jejího zásahu bleskem či naindukování statické elektřiny na koaxiálním kabelu, vedoucím k anténě.

V případě, že k tomu dojde, statická elektřina se uzemní přes cestu nejmenšího odporu, většinou právě přes rádiovou kartu, kterou tím často nenávratně zničí. V případě zásahu antény bleskem je zničeno celé zařízení a s ním často také elektrický rozvod v domě.

Těmto problémům předejdeme montáží přepěťové ochrany neboli bleskojistky. Ochranu montujeme před anténní vstup rádiové karty nebo přístupového bodu. V případě UTP kabelu používáme přepěťovou ochranu pro UTP kabel, kterou rovněž montujeme těsně před vstupem do zařízení.

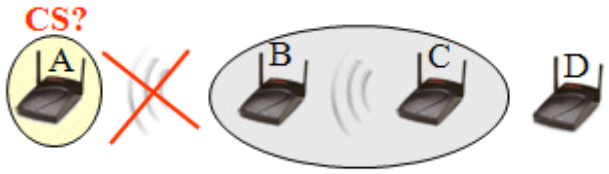
Přepěťové ochrany nás ochrání nejen v případě přímého úderu blesku do antény, ale rovněž při vzniku atmosférického napětí, které se indukuje na anténním kabelu. K naindukování často stačí pouze běžný déšť nebo prudký vítr. Přepěťová ochrana propustí pouze určitou předem danou hladinu vstupního napětí. Pokud je tato hranice z jakýchkoli důvodů překročena, automaticky je napětí omezeno na povolenou mez, aby nedošlo k poškození elektroniky Wi-Fi zařízení.

7.5 Problém skryté a předsunuté stanice

Protokol 802.11 byl vyvinut pro použití uvnitř budov, nikoli ve volném prostranství. Při provozování ve venkovním prostředí totiž dochází u protokolu 802.11 k jevům, které nejsou nijak ošetřeny, protože ve vnitřním prostředí k nim dochází jen ve velmi vzácných situacích anebo vůbec. Jedním z problémů je jev předsunuté a skryté stanice.

7.5.1 Problém skryté stanice

Dle (19) stanice C vysílá data pro stanici B. Ostatní stanice by měly být informovány o tom, že stanice C vysílá a měly by čekat, až s vysíláním skončí a teprve poté zahájit komunikaci. Stanice A však vysílání stanice C nezachytí, jelikož je od ní příliš vzdálena a tak její signál není schopna zachytit. Začne tedy vysílat data pro stanici B, čímž dojde k přerušení právě prováděného přenosu dat mezi stanicemi B a C.



Obrázek 7-6 – Skrytá stanice.

7.5.2 Problém předsunuté stanice

Stanice B vysílá data pro stanici A, její signál však zachytí i stanice C, která chce ve stejnou chvíli poslat data stanici D. Stanice C však špatně vyhodnotí, že právě vysílá jiná stanice a vysílání dat odloží, ačkoli nemá se stanicemi A a B nic společného a jejich komunikaci svým vysíláním nijak neovlivní. (19)

Obrázek 7-7 – Předsunutá stanice.

8 Autorovy zkušenosti s výstavbou venkovních Wi-Fi sítí

Situace na telekomunikačním trhu v České republice v době příchodu Wi-Fi technologie na tuzemský trh přímo předurčovala vznik venkovních Wi-Fi sítí. Hlavním důvodem bylo pomalé a zároveň drahé připojení k internetu. Pokročilí uživatelé se tak začali mezi sebou propojovat pomocí jednotlivých Wi-Fi spojů a sdílet jednu internetovou přípojku mezi několika domácnostmi. Na internetovou přípojku se všichni skládali rovným dílem a při větším počtu uživatelů si tak mohli dovolit připojení, které by samostatně nebyli schopni hradit. Tito uživatelé používali v té době cenově dostupný hardware, který zároveň vykazoval dostatečnou míru stability, což z velké části ovlivňovaly především dostupné ovladače. Oblíbenou komponentou se stala dnes historická radiová karta od firmy PRISM s modelovým označením XI-626, která byla podporována jak operačním systémem Linux tak Windows. Dále několik metrů koaxiálního kabelu H155 nebo H1000 a směrová anténa, takzvaná cantenna. Jedná se o anténu vyrobenou z plechovky, například od potravin.

Obrázek 8-1 – Cantenna, primitivní směrová anténa pro pásmo 2,4 GHz.

Hlavním důvodem používání cantenn byla vysoká cena profesionálních směrových antén, díky které byly pro většinu uživatelů nedostupné. Cantennu si mohl vyrobit doma téměř každý, i méně manuálně zručný uživatel a to téměř zdarma.

8.1 Komunitní síť CZFree.Net

Uživatelé, sdílející mezi sebou internetové připojení, založili v ČR projekt komunitní sítě CZFree.Net. Hlavní myšlenkou této sítě byla svoboda komunikace. V rámci sítě CZFree.Net bylo možné přenášet data a komunikovat s dalšími uživateli zdarma. Za přístup do internetu se pak platil společný příspěvek. V síti CZFree.Net bylo několik internetových přípojek a každý uživatel si mohl vybrat, kterou z nich chce používat.

Ze sítě CZFree.Net se postupem času stala síť schopná bez problému konkurovat komerčním poskytovatelům internetového připojení. Uživatelé sítě zakládali občanská sdružení a spolky, aby svoji činnost zlegalizovali a mohli začít připojovat také ostatní uživatele, díky jejichž příspěvkům mohli síť dále rozvíjet a zdokonalovat.

Základní myšlenka a důvod vzniku sítě CZFree.Net byl však později překonán, jelikož internetové připojení výrazně zlevnilo a zrychlilo, a tak si byl již každý schopen pořídit svou vlastní přípojku, často navíc s lepší kvalitou a vyšší rychlostí, než nabízela síť CZFree.Net.

Síť CZFree.Net dodnes stále existuje, avšak stěží se dá mluvit o síti s původní myšlenkou svobodné komunikace. Jednotlivé spolky uživatelů často přerušily vzájemnou spolupráci a svou síť vůči ostatním osamostatnily. Hlavním důvodem byl příchod nových aplikací a technologií, které umožňují pohodlnější sdílení dat přímo přes internet a také pokles cen internetových přípojek od komerčních poskytovatelů. Dalším důvodem byly často odlišné názory jednotlivých spolků a docházelo ke vzájemným neshodám a dalším problémům. Mnoho uživatelů také přestalo budování a správa sítě bavit a tak ze spolků vystoupili. Jiní uživatelé dali přednost vlastní internetové přípojce a rovněž přestali síť CZFree.Net používat. Menší spolky se připojily k větším, protože samy nebyly schopné sehnat dostatek financí na provoz a obnovu technologií. Větší spolky jsou naopak díky velkému počtu uživatelů v síti schopné pokrýt z příspěvků stejně kvalitní technologie, které nasazují velcí komerční poskytovatelé a tak se stále snaží udržet svoji síť konkurence schopnou a často mohou opravdu nabídnout výrazně lepší a levnější služby než velcí komerční poskytovatelé. (22)

8.2 Budování sítě

Bezdrátovou síť jsme začali budovat společně s rodinnými příslušníky a spolužáky po nástupu na střední školu. Inspirací nám byla mimo jiné i síť CZFree.Net. Síť nyní

pokrývá přibližně třetinu území Prahy a jižní a východní část jejího přilehlého okolí. Nejvzdálenější lokalita, kterou síť aktuálně pokrývá, je město Milovice. V síti je nyní připojených přibližně 1500 uživatelů a firem.

8.2.1 Bezdrátová technologie v síti

Ze začátku byla nasazena na všech přístupových bodech technologie 2,4 GHz a na páteřních spojích pak 5 GHz. Postupem času však vzrostlo rušení v pásmu 2,4 GHz natolik, že bylo nutné přejít na pásmo 5 GHz také na přístupových bodech. Páteřní spoje, s přibývajícím počtem uživatelů, přestávaly kapacitně dostačovat a tak bylo nutné přejít na jinou technologii. Zvolili jsme profesionální spoje v pásmu 10 GHz s kapacitou několik desítek i stovek Mbps. Dalším krokem byl přechod k velkokapacitním poskytovatelům internetové konektivity, od kterých odebírají i největší tuzemští telekomunikační operátoři. Hlavním důvodem byla kvalita služby, nižší cena a teoreticky neomezená kapacita internetové přípojky.

S tímto krokem bylo opět nutné vyměnit spoje na páteřních linkách z důvodu jejich nedostačující kapacity. Na hlavní lince byl osazen spoj na frekvenci 80 GHz s kapacitou 1Gbps. Na páteřních linkách se pak jedná o nové modely spojů s vyšší propustností v pásmech 10 GHz a 24 GHz.

8.2.2 Technologie na koncových bodech

S kapacitou páteřních spojů nebývají zpravidla tak velké problémy jako s kapacitou přístupových bodů a dalších technologií, které předávají konektivitu konečným uživatelům. Z důvodu vzrůstajícího rušení bylo nutné opustit pásmo 2,4 GHz. V dnešní době však začínají být na mnoha místech problémy také v pásmu 5 GHz.

V pásmu 5 GHz bylo uvedeno v poslední době rovněž mnoho inovací stávajících standardů, které jsou uvedeny v předchozích kapitolách této práce. Díky těmto vylepšením je možné ve stejném pásmu a se stejnými komponentami dosahovat i pětinásobných rychlostí oproti prvním Wi-Fi zařízením pro pásmo 5 GHz. Výrobci se snaží vylepšovat také zařízení pro pásmo 2,4 GHz, tam však k větším nárůstům rychlostí zpravidla nedochází z důvodu vysokého rušení.

8.2.3 Problémy s rušením v pásmu 2,4 GHz a 5 GHz

V menších sítích o několika přístupových bodech je možné poměrně bez problému ohlídat rušení a případně přeladit přístupový bod na jiný, volnější kanál. V případě naší sítě se jedná o podstatně obtížnější úkol. Největším problémem je pásmo 2,4 GHz, kde bylo na mnoha přístupových bodech nutné měnit kanál i mnohokrát do týdne. Jediným řešením tak byl přechod na pásmo 5 GHz.

Zdaleka největším problémem je však rušení od jiných technologií. Wi-Fi zařízení až na výjimky nejsou schopné rozpoznat jiný signál než Wi-Fi, a tak v případě použití jiných technologií v pásmu 2,4 GHz není možné jejich signál bez speciálních přístrojů pro měření pásma zachytit a odhalit tak rušení.

V naší síti se vyskytlo několik takovýchto případů, kdy po několika servisních zásazích jak na straně přístupového bodu, tak na straně klienta, nebyly zjištěny žádné závady, avšak problémy s komunikací se vyskytovaly prakticky každý den. Nakonec jsme zjistili, že mezi přístupovým bodem a klientem je kasino, ve kterém je nasazen bezdrátový kamerový systém, který spojení velmi silně rušil.

Pásmo 5 GHz má oproti pásmu 2,4 GHz výhodu v menším počtu zařízení, které toto pásmo podporují, a tím pádem je zde podstatně nižší hladina šumu. Vezmeme-li v potaz většinu notebooků, tabletů, mobilních telefonů a podobně, pak jen menší část z nich podporuje pásmo 5 GHz.

Z tohoto důvodu se tak zařízení pro pásmo 5 GHz častokrát dostane do rukou jen uživatelům, kteří jsou v této oblasti alespoň částečně poučení a vědí, jak se v pásmu chovat a jak své zařízení naladit tak, aby ostatní sítě v okolí nerušilo a nezpůsobovalo tak problémy.

8.2.4 Metody zabezpečení venkovních sítí

Mezi zabezpečením venkovních a vnitřních sítí není teoreticky žádný rozdíl, avšak v praxi jsou pro zabezpečení venkovních sítí některé metody méně vhodné.

Nejjednodušší, a ve většině případů dostačující, je omezení přístupu pomocí seznamu MAC adres. Bohužel se v okolí často najdou hackeři, kteří si přístup do sítě nechtějí hradit a toto zabezpečení prolamují, čímž ostatním způsobují výpadky nebo snížení kvality připojení. V pásmu 2,4 GHz tak bylo třeba na mnoha místech přejít na zabezpečení WPA-PSK a těmto útokům tak zabránit. Zabezpečení WEP nebylo zvoleno

z důvodu jeho snadného prolomení, které není o mnoho složitější, než prolomení přístupu přes seznam MAC adres. WPA2 nebylo možné použít z důvodu jeho slabé podpory ve starších zařízeních, které stále mnoho uživatelů používá.

V pásmu 5 GHz byla vyhrazena pouze určitá zařízení, s kterými je možné se do sítě připojit, abychom předešli pozdějším problémům s kompatibilitou. Bylo použito zabezpečení WPA2-PSK.

Jediným problémem zabezpečení WPA-PSK nebo WPA2-PSK je nebezpečí zneužití klíče koncovým uživatelem. Z tohoto důvodu je nutná přítomnost technika při instalaci zařízení. Ten osobně zadá klíč do zařízení, které následně zabezpečí heslem a uživatel se tak šifrovací klíč nedozví.

8.2.5 Vliv bezdrátových sítí na telekomunikační trh

Bezdrátové sítě najdou své využití především na místech, kde je nemožné realizovat metalickou či optickou síť nebo na místech, kde je tato síť v havarijním stavu. Bezdrátové technologie jsou tak často nasazovány v horách, ale i všude jinde. Hojně je využívají například telekomunikační operátoři, jejichž vysílače se mnohdy nacházejí na těžce dostupných místech uprostřed lesů či na vysokých kopcích, kam není možné dovést žádné metalické či optické datové vedení.

V České republice je Wi-Fi technologie hojně využívána k připojení domácností či firem k internetu, jelikož stará metalická vedení nejsou často schopna dosahovat požadovaných rychlostí a kvalit přenosu a tak podstatná část uživatelů hledá jinou možnost připojení. Důkazem toho je nedávné založení dceřiné společnosti firmy Telefónica Czech Republic, která se zabývá právě budováním bezdrátové infrastruktury.

9 Závěr

Cílem této práce je přiblížit a vysvětlit základní principy fungování technologie Wi-Fi od prvotního standardu 802.11 až po nejnovější standard 802.11ac, který je již nyní do Wi-Fi zařízení implementován ve vývojové verzi DRAFT. Dále jsou v práci vysvětleny standardní i nestandardní metody zabezpečení Wi-Fi sítí, včetně představení jejich slabin v šifrování a distribuci šifrovacích klíčů.

Dalším cílem je představení Wi-Fi hardware a technologií, které jsou v dnešní době plošně nasazované ve vnitřním i venkovním prostředí, včetně dalších speciálních komponent, které jsou nutné pro správnou a stabilní funkčnost technologií nasazených ve venkovním prostředí. V poslední kapitole jsou zahrnuty autorovy zkušenosti a připomínky k provozu vlastní rozlehlé bezdrátové sítě v Praze a jejím okolí. Je zde objasněna problematika týkající se použité technologie na páteřních spojích a přístupových bodech sítě. Rovněž jsou zde představeny používané metody zabezpečení venkovních Wi-Fi sítí. Nakonec jsou zde zhodnoceny zkušenosti s rušením v pásmech 2,4 GHz a 5 GHz a jeho následným řešením.

Přínosem této práce je vysvětlení základních principů fungování Wi-Fi technologie včetně možných způsobů zabezpečení Wi-Fi sítí. Dále je zde objasněn možný budoucí vývoj Wi-Fi sítí 4. generace. V kapitole **Aktuálně používané Wi-Fi technologie** jsou představeny nejnovější a často méně známé protokoly a technologie pro pásma 2,4 GHz a 5 GHz. Dále navazuje kapitola **Stavba venkovních sítí**, kde je představen Wi-Fi hardware v podobě routerů, rádiových karet a anténních systémů s podporou nejnovějších protokolů standardu 802.11n. Poslední kapitola popisuje autorovy zkušenosti a poznatky získané během stavby a provozu vlastní Wi-Fi sítě na území Prahy a jejího okolí.

Obsah této práce pomůže méně pokročilým uživatelům získat základní informace o Wi-Fi technologii a zkušenější uživatelé zde naleznou informace o nových technologiích a protokolech pro standardy 802.11a a 802.11n včetně důležitých informací pro provoz venkovních sítí.

10 Seznam literatury a použitých zdrojů

1. HORÁK, J. Vytváříme domácí bezdrátovou síť, . Vyd. 1. Brno: Computer Press, 2011. 296 s. ISBN 80-251-2977-2
2. BARKEN, L. Wi-Fi: Jak zabezpečit bezdrátovou sít. Vyd. 1. Brno: Computer Press, 2004.174 s. ISBN 80-251-0346-3
3. ZANDL, P. Bezdrátové sítě WiFi: praktický průvodce. Vyd. 1. Brno: Computer Press, 2003. 190 s. ISBN 80-7226-632-2
4. BRISBIN, S. Wi-Fi: Postavte si svou vlastní Wi-Fi sít. Vyd. 1. Praha: Neocortex, 2003.248 s. ISBN 80-86330-13-3
5. KöHRE, T. Stavíme si bezdrátovou síť Wi-fi. Vyd. 1. Brno: Computer Press, 2004. 295 s. ISBN 80-251-0391-9
6. Wiki.mikrotik.com [on-line]. Dostupný z WWW: <http://wiki.mikrotik.com/wiki/Manual:Nv2>
7. Engadget.com [on-line]. Dostupný z WWW: <http://www.engadget.com/2009/10/01/wi-fi-alliance-updates-certified-802-11n-program-intros-shiny-n/>
8. Medicalconnectivity.com [on-line]. Dostupný z WWW: <http://medicalconnectivity.com/2008/03/17/do-medical-devices-need-80211n/>
9. Netronics-networks.com [on-line]. Dostupný z WWW: < http://www.netronics-networks.com/netglide.html>
10. Engineersworld.wordpress.com [on-line]. Dostupný z WWW: http://engineersworld.wordpress.com/2011/07/11/how-to-transfer-data-through-a-adhoc-network>
11. Cisco.com [on-line]. Dostupný z WWW: <http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html>
12. Cz.tp-link.com [on-line]. Dostupný z WWW: <http://cz.tp-link.com/products/details/?model=TL-WR940N>
13. EX extime.vn.ua [on-line]. Dostupný z WWW: < http://extime.vn.ua/?q=node/25>
14. NetworkDirect [on-line]. Dostupný z WWW: <http://networksdirect.co/781-thickbox/air-cap1552e-e-k9.jpgyxcv>

15. Wifi.aspa [on-line]. Dostupný z WWW: < http://www.luxus.cz/obchod_pic/nahledy/11-01-01-vs-m15_velikost_x256.jpg>
16. Aspa.cz [on-line]. Dostupný z WWW: <http://www.luxus.cz/obchod_pic/sektor2-15-1.jpg>
17. WIFI Yagi Antennas [on-line]. Dostupný z WWW: <http://www.gpsinusa.com/WIFI-Yagi-Antennas.html>
18. Wifi.aspa [on-line]. Dostupný z WWW: <http://wifi.aspa.cz/parabolicka-antena-5-6ghz-24dbi-44cm-zz5g6p24-z36766/>
19. Earchiv.cz [on-line]. Dostupný z WWW: <http://www.earchiv.cz/b07/b0300001.php3>
20. Openobject.org [on-line]. Dostupný z WWW: <http://www.openobject.org/objectsinflux/images/mMa/Wireless%20Network/cantenna.jpg>
21. Intelekt.cz [on-line]. Dostupný z WWW: < http://www.intelek.cz/art_doc-D7A489A18B634F84C12575550053ECAE.html>
22. CZFree.Net [on-line]. Dostupný z WWW:<www.czfree.net>

Seznam obrázků

11 Přílohy

Slovník pojmů a zkratek

AES	Advanced Encryption Standard
Ad-hoc	Bezdrátová síť mezi klientskými zařízeními, bez přístupového bodu
Bluetooth	Standard IEEE 802.15 pro bezrátovou komunikaci v pásmu 2,4 GHz
CCMP	Counter Cipher Mode Protocol
ČTÚ	Český telekomunikační úřad
DSSS	Direct Sequence Spread Spektrum
EAP	Extensible Authentication Protokol
EAP-SIM	Extensible Authentication Protokol – Subscriber Identity Module
EAP-TLS	Extensible Authentication Protokol – Transport Layer Security
FHSS	Frequency Hopping Spread Spectrum
HR-DSSS	High Rate - Direct Sequence Spread Spectrum
MAC adresa	Fyzická adresa, jedinečný identifikátor síťového hardware.
MIMO	Multiple Input Multiple Output, technologie standardu 802.11n
OFDM	Orthogonal Frequency Division Multiplexing
SISO	Single Input Single Output, technologie standardů 802.11abg
SSID	Service Set Identifieer, název bezdrátové sítě
TDMA	Time Divison Multiple Access
TKIP	Temporal Key Identity Protocol
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
Wi-Fi	Bezdrátová síť používající standard z rodiny 802.11, Wireless Fidelity (Bezdrátová věrnost)