# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

## TECHNICKÁ FAKULTA

## Katedra technologických zařízení staveb


## DIPLOMOVÁ PRÁCE

# Zhodnocení a návrh reálného využití bezdrátových přenosů ve vlnovém pásmu 5 GHz a 10 GHz v porovnání s pásmem 2.4 GHz – provozní, technické a nákladové parametry


Vedoucí práce : Ing. Zdeněk Votruba

Vypracoval : Pavel Sochor



**PRAHA 2009**

## Prohlášení:

Prohlašuji, že jsem diplomovou práci na téma „Zhodnocení a návrh reálného využití bezdrátových přenosů ve vlnovém pásmu 5 GHz a 10 GHz v porovnání s pásmem 2.4 GHz – provozní, technické a nákladové parametry “ vypracoval samostatně za pomoci uvedené literatury a konzultačních hodin.

**V Praze, dne 30.4.2009 ……**

**Poděkování:**

Poděkování patří především Ing. Zdeňku Votrubovi za ochotu, pomoc, užitečné rady a připomínky, které mi věnoval při tvorbě diplomové práce.

## Abstrakt:

Diplomová práce se zabývá zhodnocením a návrhem reálného využití bezdrátových přenosů ve vlnovém pásmu 5GHz a 10GHz, jež porovnává s pásmem 2,4GHz a to provozními, technickými a nákladovými parametry. V kapitole „Technické a technologické parametry přenosu“ je popsán standard jednotlivých technologií a popisuje druh jednotlivých modulací. V kapitole „Zabezpečení bezdrátových sítí“ je charakterizována bezpečnost bezdrátových sítí a popis jednotlivých typů zabezpečení. Kapitola „Technické řešení a testování v reálném provozu“ navrhuje použití jednotlivých druhů technologií a jejich správné dimenzování pro dosažení nejlepších výsledů a dále otestování každé technologie, zjištění maximálního datového přenosu a stability.



## Klíčová slova:

Technologie, přenos, zabezpečení, bezdrátová síť.



## Summary:

Thesis is dealing with the real appreciation of design and use of wireless transmissions in free wavelength band of 2,4 GHz, 5 GHz, 10 GHz and each zone between the technically and economically compared. In the chapter "Technical and technological parameters of the transfer" is described the standard by the various technologies and describes each type of modulation. In the chapter "Wireless Security" is characterized by security of wireless network and a escription of each type of security. Chapter "Technical solutions and testing in real traffic" suggests the use of different types of technology and good design to achieve the best results. It also includes testing of each technology, determine the maximum data transfer and stability.



## Key words:

Technology, transfer, security, wireless network

## Obsah:

# 1. Úvod

O výhodách využití bezdrátových lokálních sítí (*Wireless Local Area Network*, WLAN), jež vedly k rozšíření stávajících podnikových intranetů i jejich plnohodnotné náhradě není třeba příliš hovořit. Jejich donedávna malé rozšíření souviselo s pomalou standardizací, nižšími přenosovými rychlostmi a také dražšími zařízeními. Normalizace i trh dnes vypadají jinak a stáváme se tak svědky jejich výrazného nástupu, jak v podnikovém nebo domácím prostředí, tak na veřejných místech.[1]

Rádiové vysílání, jímž je dnes řešena většina komerčně nasazovaných sítí, je náchylné na rušení, a to všemi prostředky, které mohou na příslušných kmitočtech pracovat (např. i mikrovlnné trouby – což se týká zejména bezlicenčního pásma 2,4 GHz). Optické bezdrátové sítě či sítě založené na infračerveném záření zase nesnesou překážky mezi vysílačem a anténou přijímače. Jejich použití je tedy omezené. Dosah související s kvalitou přenosu pak omezuje jejich velikost i počet systémů, které se v rámci daného prostoru mohou nacházet, aby nedocházelo k nežádoucímu rušení. Zajištění bezpečnosti bezdrátové komunikace je při rádiovém vysílání jedním z nejobtížnějších problémů, podobně jako *roaming* a směrování mezi různými sítěmi.[11] Toto je ovšem již záležitostí vyšších vrstev, jíž je např. Mobile IP. Nikoliv však nejnižších dvou, jež definují normy IEEE 802.[1]

Shora uvedenými záležitostmi se zabývá i následující diplomová práce, v níž jsem se snažil osvětlit, za jakých podmínek je možné bezdrátové sítě využívat. V práci jsem dále pak porovnal technické i praktické možnosti jednotlivých technologií a jejich správné dimenzování pro dosažení nejlepších výsledů. Též i otestování každé technologie, zjištění maximálního datového přenosu a stability.

# 2. Historie a vývoj bezdrátových sítí

## 2.1. Vznik sítí IEEE 802.11

Hlavní odlišnost bezdrátových Wi-Fi sítí od jiných druhů bezdrátových sítí (např. GSM, CDMA) tkví v používaném frekvenčním pásmu, od něhož se také odvíjí dostupnost běžným uživatelům. Většina ostatních bezdrátových sítí (tedy ne Wi-Fi) jsou tzv. licencované sítě, což znamená, že každá taková síť má svoji přidělenou frekvenci a pásmo, na kterou musí mít provozovatel licenci vydávanou regulačními orgány. Na dané frekvenci smí vysílat jen ten, kdo si zaplatil licenci. Kromě těchto licencovaných pásem existuje i pásmo veřejné – tzv. pásmo ISM (Industrial Scientific and Medical). ISM pásmo využívají kromě vědeckých, průmyslových a lékařských organizací také např. mikrovlnné trouby a bezdrátové telefony (typu DECT, avšak ne mobilní). Pásmo ISM je vymezeno na frekvenci 2,4 GHz v Evropě regulační organizací ETSI a v USA regulátorem FCC. Pásmo ISM neuniklo pozornosti ani výrobcům bezdrátových sítí, zpočátku však každý výrobce vyráběl vlastní technologie (např. izraelský výrobce BreezeNet). Tyto proprietární technologie většinou nebyly kompatibilní s ostatními bezdrátovými sítěmi, proto vznikl v roce 1997 společný standard pro bezdrátové sítě v pásmu ISM. Tento standard vytvořený institutem IEEE (Institute of Electrical and Electronic Engineers) je znám pod označením 802.11 a umožňuje komunikovat o maximální rychlosti 2 Mb/s. Ačkoliv šlo o standard, tak stále nebylo možné v některých případech provozovat a kombinovat zařízení od různých výrobců. Nekompatibilita výrobků vzbuzovala nedůvěru uživatelů a snižovala zájem o sítě 802.11. Proto vznikla certifikační společnost WECA, která testuje kompatibilitu jednotlivých zařízení standardu 802.11 a výrobkům vyhovujícím všem požadavkům uděluje logo Wi-Fi (taktéž WiFi), což znamená Wireless Fidelity (zde je patrná analogie s označením Hi-Fi, používaným u audio a video techniky). Wi-Fi technologie dosáhla takového úspěchu, že se sama společnost WECA přejmenovala roku 2003 na WiFi.

V dnešní době, pokud mluvíme o Wi-Fi sítích, máme na mysli především sítě standardu 802.11 a jeho dalších variant.

Od září 2005 je generálním oprávněním uvolněna frekvence 5GHz (přesněji 5,470GHz ~ 5,725GHz). Tato frekvence přináší několik výhod, ale i nevýhod. Nejvýznamnějšími výhodami jsou necitlivost na atmosférickou vlhkosti (spoj není tolik citlivý na déšť apod.), menší průměr Fresnelovy zóny a díky V.O. vyšší povolený vyzářený výkon a větší množství povolených nepřekrývajících se kanálů. Naopak nevýhodami jsou větší útlum (v prostředí i v koaxiálním vedení), nižší odrazivost (není možné použít odrazu k vybudování spoje) a obecně vyšší technická náročnost na všechny komponenty spoje.

Samostatnou kapitolou je potom pásmo 10 GHz, které je vyloženě českou specialitou a je dnes nosnou infrastrukturou malých ISP a rád bych mu věnoval nejvíce času. Základní zajímavostí je, že dané pásmo se dnes používá pouze v ČR, je stejně jako výše zmíněná pásma volné a provoz není nutné hlásit ČTU. Pásmo je kvalitativně rozdílné od předešlých dvou a to především použitou technologií, která nevychází z masově vyráběných zařízení, ale je na stejné úrovni jakou jsou profesionální spoje do licencovaných pásem s ohledem především na spolehlivost a kvalitu přenášených dat. Jsou konstruovány jako spoje Bod-Bod. Narozdíl od Wi-Fi jsou plně duplexní s nezávislým provozem v obou směrech. Pokud tedy Wi-Fi funguje jako klasická vysílačka, která v jeden moment buď přijímá nebo vysílá a musí se dělit o přenosový kanál s protější stranou, tak u spojů v pásmu 10 GHz vysílají obě strany neustále, ale na jiných frekvencích (tzv. Duplexních kanálech) a každá strana má svůj nezávislý přijímač a vysílač.[3]

## Vývoj 802.11:

Hned po vzniku standardu 802.11 bylo jasné, že v porovnání s klasickými sítěmi bude potřeba bezdrátové sítě zrychlit a rozšířit jejich funkce, protože např. již zmíněná rychlost 2 MBit se ukázala jako nedostačující. S postupem doby byly tedy definovány následující standardy (zde uspořádány v abecedním pořadí): [2]

• 802.11a – Uveden roku 1999 a určen pro bezdrátové sítě v pásmu 5 GHz. V Evropě tento standard není povolen, využívá se v USA. Maximální rychlost činí 54 MBit.

• 802.11b – Patrně nejznámější a nejrozšířenější standard, který byl uveden společně se standardem 802.11a, ale na rozdíl od něho využívá 2,4GHz pásmo s rychlostí až 11 MBit. . Tento standard spolu s 802.11g se u nás neuvěřitelně rychle rozšířil a ve větších městech je již problém s umístěním vlastního AP, aby jste nerušily některé z okolních sítí.

• 802.11c – Jde o standard definující procedury pro síťové bridge. Je využíván hlavně přístupovými body.

• 802.11d - se vznikem standardu 802.11 se ukázalo, že je potřeba mezinárodní kooperace a harmonizace. Například 5GHz pásmo se používá v mnoha státech různě a bylo třeba přizpůsobit standardizaci tak, aby vycházela vstříc nejen požadavkům USA a Japonska.

• 802.11e - rozšíření MAC pro službu Quality of Service (QoS). QoS zajišťuje vyrovnanou kvalitu služby, která je důležitá např. pro multimédia (trvalý tok dat potřebný pro videokonferenci apod. ).

• 802.11f – přináší Inter Access Point Protocol (IAPP). Předchozí specifikace 802.11 nezahrnují standardizaci komunikace mezi jednotlivými access pointy (přístupovými body, viz dále) pro zajištění roamingu (tzn. přechodu uživatele od jednoho access pointu k druhému).

• 802.11g – další velice důležitý standard, schválený v roce 2002. 802.11g umožňuje komunikovat v pásmu 2,4 GHz rychlostí až 54 MBit. Navíc je zde zpětná kompatibilita s 802.11b.

• 802.11h - změny v řízení přístupu k spektru 5GHz pásma tak, aby bylo možno tyto sítě využívat mimo budovy.

• 802.11i - zlepšení bezpečnosti v 802.11 bezdrátových sítích vylepšením autorizačního a šifrovacího algoritmu.

• 802.11j – rozpracovaný standard týkající se alokací nových frekvenčních rozsahů pro multimediální služby bezdrátových sítí (hlavně v Japonsku).

• 802.11k – jedná se o pokračování předešlého standardu 802.11j. Vzhledem k rozšíření jednotlivých standardů na našem území, se bude tato práce zaměřovat především na standard 802.11b, ale také na 802.11g (jelikož je zpětně kompatibilní a při výstavbě nových sítí se mu postupně začíná dávat přednost před 802.11b). [27]

## 2.2. Trendy vývoje

Již v roce 2003 se začalo pracovat na novém standardu. Za dobu své historie byl několikrát přepracováván, což vede k velmi nepříjemným důsledkům pro firmy, které si zakoupily tzv. prestandardizované zařízení pro 802.11n. Nyní je posuzován draft 2.0 (verze 2.0). [10]

Standard 802.11n se od předchozích liší zvýšením rychlosti pomocí principu MIMO (multiple input, multiple output). Díky tomu je teoretické navýšení rychlosti až 10-ti násobné. Tzn. až na 540 MBit. A nejen to – měl by se zvýšit i dosah. [27]

Zařízení pracující s tímto standardem, přesněji řečeno jeho draftem, musí mít minimálně dvě a dvě antény pro příjem a vysílání. Zařízení by měla pracovat v 2.4GHz a 5GHz pásmu, měla by umět detekovat starší sítě a umět se jim přizpůsobit. To znamená snížení rychlosti nebo uvolnění pásma pro 802.11a v případě přítomnosti obou sítí. [3]

### Praktické využití:

Do budoucna se počítá s tím, že jednotlivá zařízení v domácnostech budou mezi sebou schopna komunikovat bezdrátově. To třeba znamená, že si na počítači pustíte film, bezdrátově se připojíte k dataprojektoru nebo TV a můžete se dívat. Zní to jako samozřejmost, ale doposud to bezdrátovou cestou pomocí Wi-Fi nebylo možné. Standardy 802.11a/b/g totiž mají maximální teoretickou rychlost 54 MBit, a to není dostačující rychlost pro přenos obrazu. Pro názornost

si udělejme takový malý výpočet: 802.11g má teoretické maximum 54 MBit. Na plynulé video je však zapotřebí podstatně více - např. při rozlišení 1024 x 768 bodů při 16M barvách to je 1024 x 768 (počet bodů na obrazovce) x 3 (R, G a B barevná složka) x 8 (převod z bytů na bity, ve kterých se počítají přenosové rychlosti) x 25 (počet obrazů za vteřinu pro plynulé video) = přesně 450 MBit.

Hlavní výhodou zařízení pracující v pásmu pásma 10 GHz je, že data se nikde nezdržují a rovnou bez čekání na svůj čas vyrážejí na druhou stranu. Spoje se potom chovají tak, že data vycházející na druhém konci jsou ve stejné kvalitě jako když do spoje vcházejí. Přenosové rychlosti jednotlivých výrobců dnes dosahují od 16mbit do 100mbit. Možná se vám to číslo nezdá nikterak vysoké, nicméně vězte, že se jedná o skutečné rychlosti na rozdíl od Wi-Fi, kde 54MBit znamená ve lepším případě 20MBit atd.[2]

Zásadní překážkou pro masové nasazení spojů v pásmu 10 GHz byla a je především jejich cena a potom i zcela jiné požadavky na montáž a servis spojů. Cena jako limitující faktor potom dovoluje používat toto exkluzivní frekvenční pásmo s větší rozvahou a pochopením, zatímco u spojů v pásmu 2,4 a 5 GHz je jejich použití spíše otázkou otrlosti některých uživatelů a systémem pokusů a omylů se možná dostaví výsledek – hlavně, že to funguje, spoje na 10 GHz jsou dodávané a konstruované tak, aby i při vadné instalaci a nedodržení instalačních postupů neporušovaly žádné předpisy a pokud jsou vadně nainstalované, tak ani většinou nefungují, nebo citelně omezí provoz okolních spojů, takže řešení na sebe nenechá dlouho čekat. Vědomě bezproblémově však zprovozní spoj jenom zkušený technik s odpovídajícími zkušenostmi. Proto, pořizujete-li si takovýto prostředek, je rozumné, abyste uvedení do provozu věnovali maximální pozornost a péči. [28]

Spoje v pásmu 10 GHz většinou pořizují firmy a poskytovatelé, pro které se stala prioritou kvalita poskytovaných služeb a investice do těchto technologií jenom potvrzují jejich hluboké přesvědčení, že čím méně bude v síti nestabilních prvků, tím více úsilí budou moci investovat do zkvalitňování úrovně služeb. Koncoví zákazníci to pocítí především tak, že výpadky se minimalizují a internet

běží plynule se stabilními odezvami. A to především proto, že tato profesionální zařízení jsou konstruovaná jako bezúdržbová s maximálním důrazem na spolehlivost. Proto není divu, že i mezi odběrateli vzniká celá řada informačních skupin a konzultačních fór, které kvality a nedostatky jednotlivých výrobků probírají, případně hledají rady, jak jednotlivým problémům předcházet.

Zařízení jsou provozována na základě Všeobecného oprávnění vydaného ČTU. Pro provoz zařízení není nutná žádná licence a spoje jsou provozovány na sdíleném kmitočtu. V praxi to znamená, že nově instalované pojítko je nutné nainstalovat tak, aby neomezilo činnost ostatních zařízení. To znamená prozkoumat volné kanály na obou stranách, zhodnotit průběh trasy a určit odpovídající velikosti a typy antén. Celkově je velkou ostudou, pokud někomu zarušíte trasu nebo kanál, nehledě na fakt, že díky dobré koordinaci na lokaci lze umístit až několik desítek spojů na jednom místě, aniž by to mělo vliv na kvalitu. Tzv. Rušiči se potom stávají vděčným tématem posměchu s oprávněnými výtkami k jejich profesionalitě. Rychlosti se pohybují od 16 MBit až po100 MBit s latencemi pro ping 1500 Byte od 1 milisekundy až po 7 milisekund a použitým rozhraním fast ethernet. Pokud uvažujete o koupi nebo pronájmu spoje na 10 GHz je dobré si předem ověřit jeho technické parametry, mezi které patří především reálná přenosová kapacita, latence spoje, přeladitelnost, citlivost mikrovlnné části, možnost dohledu, spotřeba, záruka a servisní zabezpečení. [28]

# 3. Technické a technologické prostředky přenosu

## 3.1. Standard IEEE 802.11

IEEE 802.11 je Wi-Fi standard s dalšími doplňky pro lokální bezdrátové sítě (Wireless LAN, WLAN) vyvíjený 11. pracovní skupinou IEEE LAN/MAN standardizační komise (IEEE 802). Výraz 802.11x je používán pro množinu doplňků k tomuto standardu. Výraz IEEE 802.11 je také spojován s původním 802.11 standardem (tedy bez dalších doplňků).[27]

Standard 802.11 zahrnuje šest druhů modulací pro posílání radiového signálu, přičemž všechny používají stejný protokol. Nejpoužívanější modulace jsou definované v dodatcích k původnímu standardu s písmeny: b, a a g . 802.11n přináší další techniku modulace. Původní zabezpečení bylo vylepšeno dodatkem i. Další dodatky (c–f, h, j) pouze opravují nebo rozšiřují předchozí specifikaci. [27]

Standardy 802.11b a 802.11g používají 2.4 gigahertz (GHz) pásmo. Proto mohou zařízení interferovat s mikrovlnnými troubami, bezdrátovými telefony, s Bluetooth nebo s dalšími zařízeními používajícími stejné pásmo. Oproti tomu standard 802.11a používá 5 GHz pásmo a není tedy ovlivněn zařízeními pracujícími v pásmu 2.4 GHz. [27]

## 3.2. Přenosové rychlosti IEEE 802.11

### 3.2.1. IEEE 802.11b

Tento standard je jedním z doplňků norem IEEE 802.11 zabývajících se definicí bezdrátového komunikačního standardu známým pod komerčním názvem Wi-Fi. Byl schválen v roce 1999 a oproti původnímu standardu navyšuje přenosovou rychlost na 11 MBit v přenosovém pásmu 2,4 GHz.. Existují i některé typy karet (D-Link), které uváděli maximální přenosovou rychlost 22 MBit. Na tento standart je navazující IEEE 802.11bg Je zpětně kompatibilní,

vysílá ve stejném frekvenčním pásmu 2400 - 2485 MHz, ale maximální nominální rychlost je 54 MBit, což odpovídá přenosům přibližně o rychlosti 25 MBit.

Použité modulační schéma je OFDM pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 MBit, přičemž pro rychlosti 1, 2, 5.5 a 11 MBit je použito stejné schéma jako ve standardu IEEE 802.11b. Vysílací výkon je snížen oproti IEEE 802.11b z 200 mW na 65 mW.

### 3.2.2. IEEE 802.11a

Tento standard využívá WiFi v pásmu 5Ghz. Používá modulaci OFDM. Oproti standardu IEEE 802.11b/IEEE 802.11g je tento stabilnější a vyspělejší. Má větší povolený vyzařovací výkon oproti 802.11b/g, tím ho lze požívat na delší vzdálenosti. V tomto standartu je maximální rychlost 54 MBit. [27]

### 3.2.3. Standard 10GHz

Reálnou přenosovou rychlostí se rozumí skutečná propustnost spoje v jednotlivých směrech. Jednotliví výrobci deklarují přenosovou rychlost v mbitech. Ta se však proti deklarované rychlosti liší. Například deklaruje-li výrobce rychlost 25 MBit a skutečná rychlost je 19 MBit, jistě bude odběratel minimálně rozčarován. A tak lze například narazit na 40mbitové spoje s reálnou propustností 36, 34 MBit s 32 MBit průtokem atd**..** Z tohoto důvodu seriozní výrobci sdělí odběrateli I reálnou rychlost spoje. Faktem zůstává, že tyto rychlosti jsou konečné a jejich objem se s vytížením jednotlivých stran neliší.[28]

# 4. Zabezpečení bezdrátových sítí

Bezdrátové sítě jsou do jisté míry snadno chránitelné proti "anonymnímu" přístupu. Bohužel většina správců těchto sítí netuší co činí a podle odhadů je více jak 60% firemních sítí otevřených anonymnímu přístupu. Jejich správci pak buďto nevědí, jak systém zabezpečit, případně se spoléhají na to, že nikdo nebude chtít jejich síť "využít". V obou případech jde o velký problém.

Bezdrátová síť je na tom stejně jako počítač či router (nebo jiné síťové zařízení). Po zakoupení a instalaci není bezpečně nainstalována a je nutné ji dodatečně zabezpečit. Stejně jako například u routerů drátových, i ty bezdrátové jsou nainstalovány se "standardními" neboli defaultními hesly, které dodává výrobce.

Zabezpečit bezdrátovou síť je mnohem složitější než typickou "drátovou" síť, protože drátová síť má omezené množství pevných přístupových bodů, kdežto k bezdrátové síti se můžete připojit z jakéhokoli místa v dosahu signálu.

Je důležité vědět alespoň o základních bezpečnostních prvcích, které bezdrátové sítě využívají. [1]

## 4.1. WEP

Zajišťuje šifrování rámců na 2. síťové vrstvě. Šifruje tedy veškeré rámce (blok binárních dat), které vedou od klienta k AP a ne pouze určité služby. Pokud je však AP připojen do Internetu, tak mezi AP a internetovým serverem šifrování neprobíhá. Právě použitá šifra je u WEPu největší problém.

K šifrovaní se používá algoritmus RC4, jehož autorem je R. Rivest a zveřejněn byl v roce 1994. Algoritmus používá proudovou symetrickou šifru s délkou klíče 40, 104 a 232 Bitů. Již v roce 2001 však bylo v algoritmu objeveno hned několik bezpečnostních nedostatků. Se symetrickým šifrováním je problém v tom, že někde musí mít klient uložený statický klíč, kterým šifruje a zároveň dešifruje komunikaci. Lepší výrobci chrání přístup ke klíči ve speciální paměti síťové karty (NVRAM), ke které lze přistupovat jen pod heslem. Bohužel

tímto způsobem to zdaleka nedělají všichni a najdou se i případy, kdy je klíč uložen v registrech a to v otevřené podobě.

WEP bohužel nijak neřeší distribuci klíče a tak je musíme ve většině případů manuálně zapsat do konfigurace zařízení. Tím trochu odpadá podstata šifrování. Útočník sice zatím klíč nezná, ale oprávněný uživatel ano a tak pro něj není složité komunikaci dešifrovat a protože 70% útoků je vedeno zevnitř sítě, tak tento fakt je velkým bezpečnostním nedostatkem. Ani oprávněný uživatel by o podobě klíče neměl vůbec vědět.

Odesílatel i příjemce musí mít stejný klíč používaný k šifrování/dešifrování komunikace. Pro vyšší bezpečnost je nutné klíč průběžně obměňovat. To ale WEP ani RC4 nijak neřeší a tak jediný možný způsob změny klíče je opětovné nahrazení stávajícího v konfiguraci adaptéru. U distribuce klíčů je problém, protože případný útočník může nový klíč při předání získat. Proto to v dnešních sítích chráněných WEPem vypadá tak, že se celý rok používá stejný klíč. Přičemž v lepších případech by se měl klíč měnit po několika minutách.

Proč tedy právě tato šifra ? Jednoduše proto, že ji lze snadno implementovat do hardwaru bezdrátových adaptérů a díky tomu nemá aktivování šifrování téměř žádný vliv na výkon počítače.

Zašifrování stejné zprávy symetrickou šifrou totiž pokaždé generuje stejnou šifrovanou zprávu a tím pádem je mnohem jednoduší klíč uhodnout. Proto je součástí WEP ještě inicializační vektor (IV), který se mění s každým paketem a doplňuje klíč o dalších 24 Bitů. Při použití WEPu s klíčem dlouhým 128 Bitů má klíč pouze 104 Bitů + 24 Bitů IV. Generování IV zajišťuje vysílací strana, která ho nejenom použije k sestavení šifrovaného streamu, ale přidá ho v otevřené podobě i do záhlaví rámce. Tím by se mohlo zdát, že se pokaždé použije "jiný klíč" a šifra je tím bezpečnější, ale není tomu tak. Unikátních IV je pouze 224 a pokud se tedy odešle 224 paketů, začne se IV opakovat. Inicializačním vektorem se tedy nic nevyřeší a šifra je stále napadnutelná řadou útoků. Navíc prodloužení klíče má k délce jeho luštění lineární závislost => pro 2x delší klíč je potřeba pouze 2x více času k dešifrování.

Integritu šifrované zprávy zajišťuje známá funkce CRC-32 (Cyclic Redundancy Check), jejíž hodnota je společně s daty zašifrovaná v těle zprávy. Bohužel však díky lineárnosti funkce CRC32 ji lze obelstít určitou formou záměny bitů, které nedokáže odhalit. [3]

### Derivace klíče díky CRC32

Jak bylo již několikrát uvedeno, tak WEP používá kontrolní součet CRC32. Nyní si popíšeme jednoduchý příklad, jak toho využít. O nedostatcích CRC32 se ví již dlouho. Záměnou určitých bitů zůstane kontrolní součet stejný. Takže pokud bity zaměníme a odešleme, paket projde přes kontrolu integrity a předá se do vyšší vrstvy. Tam paket způsobí chybu, protože data nebudou dávat smysl a odešle se zpět zpráva s chybovým hlášením. Její podobu můžeme odhadnout a tím odvodit i šifrovací klíč pro daný IV. [3]

## 4.2. WPA

WPA (WiFi Protected Access) je novější bezpečnostní mechanizmus a původně měl opravit chyby, kterých se WiFi Aliance dopustila u WEPu. Sice nešťastně používá stejný šifrovací algoritmus RC4, kvůli jednoduchému upgradu firmwaru stávajících zařízení, ale určitě sebou přináší řadu vylepšení. Standardně používá 128 bitový dynamický klíč, který se mění každých 10 000 paketů. Dalším zlepšením je MIC (Message Integrity Check), jež je používán současně s CRC32 a tím řeší jeho nedostatky, díky kterým bylo možné změnit zprávu při zachování stejného kontrolního součtu. [3]

## 4.3. 802.11i/WPA2

Komplexní zabezpečení pro všechny typy 802.11 přinesla až vloni schválená norma 802.11i**.** Ta zahrnuje vzájemnou autentizaci na základě 802.1x a nový protokol CCMP pro silné šifrování pomocí AES (*Advanced Encryption Standard*). Volitelně se pro zpětnou slučitelnost s WPA používá protokol TKIP s šifrováním na základě RC4 (šifry používané také u WEP).

CCMP (*Counter-mode CBC – Cipher Block Chaining)* MAC *(Message Authentication Code) Protocol*) používá dynamické regenerování 128 Bitových

klíčů, kontrolu integrity zpráv (MIC, kontrolní pole má délku 64 Bitů) a číslování paketů na ochranu proti útokům typu replay.

Povinné prvky, podle nichž Wi-Fi Alliance certifikuje zařízení, se označují jako WPA2. Norma sama ovšem nabízí řadu dalších prvků volitelných, jako pre-authentication a key-caching, které umožňují rychlý a bezpečný roaming mezi přístupovými body (důležité pro hlasové služby po WLAN).

Nová norma pro zabezpečení má za cíl minimalizovat útoky na bezpečnost WLAN. Dokáže již čelit útokům man-in-the-middle, ovšem stále nezabrání neautorizovaným přístupovým bodům. Navíc stále hrozí krádeže identity v souvislosti s krádežemi zařízení, kde jsou uloženy identifikační údaje v cage. AES je zatím nepokořený šifrovací algoritmus, takže utajení dat je vskutku spolehlivé.

WPA2 je zpětně slučitelné s WPA, takže souběžné použití WPA a WPA2 je v sítích běžné (na rozdíl od nepřijatelné kombinace WPA2/WEP). Certifikace pro WPA2 je rozdělena do dvou kategorií, podobně jako tomu bylo v případě WPA: **podnikové** (s plnou podporou WPA2, včetně 802.1x a PSK) a méně náročné **osobní** (domácí) sítě (pouze PSK).

Pro kvalitní zabezpečení WLAN není vždy bezpodmínečně nutné použít 802.11i/WPA2. Domácím sítím, malým kancelářím a podnikům postačí WPA, protože WPA2 pro ně neznamená výrazné zlepšení, zejména pokud současná síťová infrastruktura nezahrnuje server RADIUS. Větší podnikové sítě by se ale určitě měly vydat cestou k plnému zabezpečení WPA2 podle nejnovější normy. [3]

## 4.4. MAC autentizace

Z důvodu méně častého používání WEP, které zpočátku nebylo ani Wi-Fi zařízeními podporováno, přišli výrobci Wi-Fi techniky na řešení autentizace pomocí filtrování MAC adres – MAC adresa je unikátní síťová adresa každého síťového zařízení. V nastavení AP tak lze zadat seznam MAC adres, kterým je povolen přístup do bezdrátové sítě. Nebo naopak je možno vytvořit seznam zakázaných MAC adres a ostatním adresám je přístup povolen. Některé Wi-Fi

zařízení (AP, routery) umí časově omezit přístup určitým MAC adresám, popřípadě jim přidělit předem definovanou šířku pásma.

Bohužel je MAC adresa uložena ve firmware síťového zařízení, a tak je možné ji změnit. U klientských zařízení je potřeba software od výrobce, který je špatně dostupný, existují však i softwarové utility na změnu MAC adresy. S routery je situace ještě jednodušší, protože jde MAC adresa změnit přímo přes nastavení routeru ve webovém rozhraní. Je to kvůli snazšímu sdílení internetu, kdy internetoví provideři registrují uživatele přímo na MAC adresu síťové karty, a proto při sdílení internetu je potřeba přidělit routeru MAC adresu původní síťové karty. Toho lze však zneužít pro přístup do Wi-Fi sítě, zejména odposlechem MAC adres a následným použitím povolené MAC adresy pro průnik do bezdrátové sítě. [3]

## 4.5. Řízení přístupu do sítě

Řízení přístupu do sítě, neboli autentizace uživatele, je další částí bezpečnostní strategie Wi-Fi. Jedná se vymezení působnosti sítě a rozhodnutí, kdo (jaký uživatel) smí síť využívat. Autentizace ve Wi-Fi sítích je jednosměrná – stanice musí žádat o autentizace, avšak síť se vůči stanici autentizovat nemusí. Tohoto faktu využívají útoky man-in-the-middle, které spočívají v podvržení falešného AP mezi stanici a skutečný AP. Ve standardu 802.11 jsou zahrnuty dvě metody autentizace: open-system a shared-key. [3]

### Open-system autentizace

Tato metoda funguje následujícím způsobem: AP přijme stanici na základě údajů, které mu stanice poskytne, ale AP je nijak neověřuje. Stanice posílá údaje o sobě – identifikaci v podobě SSID (Service Set Identifier). V okamžiku, kdy AP vysílá své SSID, může každá stanice v dosahu, která není nastavená na svoje SSID, přijmout SSID přístupového bodu. Za pomoci takto získaného SSID může stanice vstoupit do sítě. Je tedy dobré vysílání SSID AP vypínat a zabránit tak přístup do sítě uživatelům, kteří neznají SSID přístupového bodu. [3]

## Shared-key autentizace

Při použití autentizace sdíleným klíčem se musí v síti také používat WEP. Je vyžadováno standardem 802.11, aby zařízení s WEP mohlo používat shared-key autentizaci. Základem této metody je klíč známý všem zařízením v síti. Stanice se při autentizaci musí prokázat tímto klíčem, který přístupový bod klíč ověří. Pokud klíč souhlasí, je teprve stanice autentizována. Ověření spočívá v tom, že AP generuje náhodné číslo, které pošle stanici. Stanice zakóduje toto náhodné číslo pomocí RC4 podle sdíleného klíče. Přístupový bod pak zprávu dekóduje – pokud se dekódované číslo rovná odesílanému číslu, je zařízení autentizováno.

Metoda sdíleného klíče se však v praxi příliš neprosadila – ne zcela vyřešena je bezpečná distribuce a obměna sdíleného klíče (stejně jako v případě WEP). Metoda shared-key otevírá malá bezpečnostní dvířka, protože dokážeme odposlechnout vygenerovaný text a poté jeho zašifrovanou podobu. Derivovat klíč, pokud známe původní a šifrovanou podobu zprávy, je totiž mnohem snazší. Takže je paradoxně bezpečnější využití standardního mechanismu ověřování klienta přístupovým bodem (Open Key Authentication), při kterém se žádné autentizační údaje nepředávají. Autentizace je jednoduše zajištěna tím, že AP i klient mají stejný šifrovací klíč. Jinak by nesouhlasil ICV (Integrity Check Value) a AP by provoz blokoval.

### Standard 802.1x + EAP

Standard 802.1x je společným standardem pro všechny typy sítí a zahrnuje autentizaci, šifrování zpráv i distribuci klíčů. Tento standard je založen na základě protokolu EAP (Extensible Authentification Protocol), jenž byl vytvořen pro zabezpečený přenos paketů prostřednictvím spojové vrstvy LAN sítí (zprávy EAP se zapouzdřují do rámců 802.1x). Přístupový bod v bezdrátové síti na základě požadavku klientů provádí jejich ověření. Ověření probíhá na základě seznamu klientů, popř. pomocí speciálních autentizačních serverů Radius (Remote Authentication Dial In User Service) nebo Kerberos. Autentizace začíná tím, že stanice odešle zprávu na přístupový bod, který odpoví

požadavkem na totožnost klienta. Na tento požadavek klient odpoví svojí identifikací, jež pošle přístupovému bodu. AP zprávu klienta pošle autentizačnímu serveru. Poté autentizační server odpoví přístupovému bodu povolením nebo zákazem přístupu klienta do sítě (AP zprávu přepošle klientské stanici). Výhodou 802.1x je užití dynamických klíčů k šifrování komunikace. Dynamické klíče mají omezenou dobu trvání, jsou určeny pouze pro daný port, na který se klient přihlásil, přičemž klíč zaniká při odhlášení klienta. Nevýhoda 802.1x spočívá v jednostranné autentizaci, která může být použita pro útok typu man-in-the-middle. [3]

# 5. Technické řešení a testování v reálném provozu

## 5.1. Využití bezdrátového přenosu v ČR

Přípojné body, hot-spoty, se začaly masově budovat v USA již před několika lety. Rostou o 82 % ročně (Gartner - srpen 2002). Světový počet byl k srpnu 2002 více jak 25 tisíc. Nyní prožívá Wi-Fi velký rozvoj i u nás. Spolu s Estonskem je prý ČR na špici nejrychlejšího rozvoje použití Wi-Fi ve střední a východní Evropě. Je to dáno tím, že v některých lokalitách není dostupnost kabelového připojení a jediná možnost je právě připojení přes Wi-Fi. Další faktor k tomu napomáhající je, že na trhu je velké množství výrobků umožňující bezdrátovou komunikaci. Jedná se o bezdrátové body, klientské adaptéry až po nejnovější platformy typu Wrap či RouterBoard.[7]

## 5.2. Zařízení pro pásmo 2.4GHz

Na trhu existuje velká řada výrobků. Jedná se buď o přístupové body (HW AP) nebo o klientské adaptéry (PCI, PCMCIA, MiniPci karty, USB adaptéry).

Nejznámější výrobky jsou od výrobců Compex, D-Link, ASUS, Ovislink. Většina výrobků je z většiny HW části totožná, obsahuje v mnoha případech stejný čip. V dnešní době je pro pásmo 2.4 GHz používaný chipset Atheros, Prism II, Realtec 8186. Rozdíl v zařízení tvoří firmware, který si každý výrobce upraví podle vlastních potřeb.

**Porovnání cen zařízení pro pásmo 2.4 GHz (přístupové body)**

| Název zařízení | Cena |
|---|---|
| Wirelles broadband routek | 1 010 Kč |
| Alfa AIP-W610 WiFi routek | 1 035 Kč |
| OvisLink WL-5460AP | 1 224 Kč |
| StraightCore WRT-312 | 1 487 Kč |
| Linksys WAP-54G – WB | 1 905 Kč |
| Compex WP-54G | 2 457 Kč |

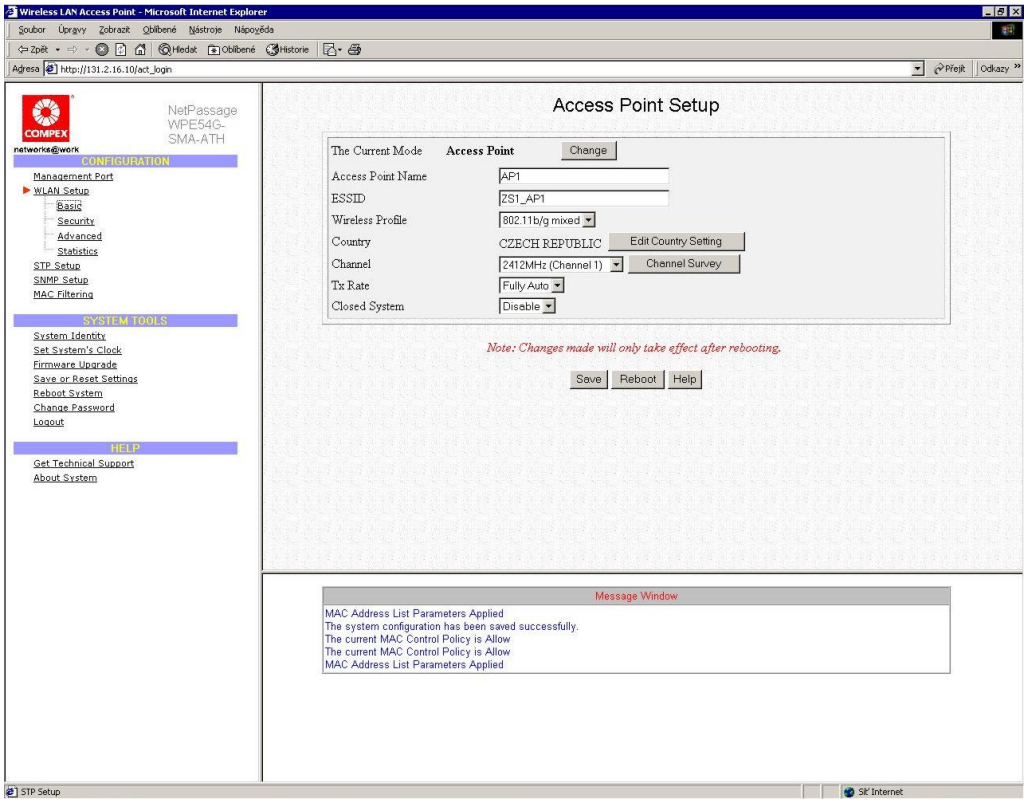
Tab. 1: Porovnání cen pro přístupové body

**Porovnání cen zařízení pro pásmo 2.4 GHz (klienstké adaptéry)**

| Název zařízení | Cena |
|---|---|
| MSI PC54G3, 802.11g PCI | 578 Kč |
| ASUS WL-167g WiFi MiniUSB | 696 Kč |
| ASUS WL-107g WiFi PCMCIA | 820 Kč |
| COMPEX WL54G PCMCIA | 1 428 Kč |
| D-Link DWL-G650+ | 1 561 Kč |
| OvisLink WL-5480USB-80 | 1 617 Kč |

Tab. 2: Porovnání cen pro klientské adaptéry

Nastavení HW zařízení se provádí přes webové rozhraní nebo správou přes telnet či ssh. Správa přes webové rozhraní je stále oblíbenější a rozšířenější. Je dostupná každému a navíc není nutné instalovat speciální utilitu, je možno ho použít ihned.




*Obr. 1: Ukázka webového rozhraní*

Podle vlastních praktických zkušeností se mi nejvíce z přístupových bodů osvědčila zařízení od výrobce Compex. Podrobněji bych chtěl představit model WPE54G.

Compex WPE54G je nástupcem úspěšného modelu WP11B+. Toho se prodalo v ČR několik tisíc kusů a až na drobné problémy s „tuhnutím" zařízení při velmi slabém či rušeném signálu byli všichni s tímto zařízením velice spokojeni. WP11B+ nabídnul přibližně před dvěma roky funkce, které dosud nebyl schopen žádný jiný výrobce implementovat. Jednalo se především o režim „routing client", který umožňoval připojit zařízení do existující Wi-Fi sítě a provádět NAT překlad. Tím se vyřešil problém připojení více PC za jeden Access Point v režimu Client.[20]

*Obr. 2* viz. Přílohy

**Specifikace zařízení:**

Jednotka pracující v těchto 5 režimech:

- AP Mode
- AP Client Mode
- Gateway Mode
- Wireless Routing Client Mode
- Wireless Ethernet Adapter

Parametry :

| | |
|---|---|
| **Konektor ext. antény:** | RSMA male |
| **LAN:** | 10/100 Mbps |
| **Norma IEEE:** | 802.11bg |
| **Regulace výstupního výkonu:** | Ano, po 1dB v celém rozsahu |
| **Správa pomocí SNMP:** | Ano, v1 i v2 |
| **Výstupní výkon:** | 802.11bg - 18 dBm |
| **WLAN:** | 2,4 až 2,48 |
| **Zabezpečení:** | WEP, WPA, 802.1x |

**Praktické zkušenosti**

WPE54G jsem testoval nepřetržitě 2 dny a za tu dobu se nestalo, že by Access Point „zatuhl“. To je asi to nejdůležitější, co uživatelé od Access Pointu čekají a vyžadují. Na začátku bych se zaměřil na mód „Access Point Client“, který je právě dnes tak často používán. První menší nedostatek jsem po zkušenostech s WP11B+ již tak trochu očekával – Access Pointem v režimu Client neprochází DHCP pakety. Ty se totiž nešíří sítí pomocí běžného TCP protokolu, ale používají kombinaci UDP protokolu a ethernetových paketů na fyzické MAC vrstvě. A právě v tom je „zakopaný pes“ – WPE54G se v módu „Access Point Client“ nechová transparentně a všechny PC připojené na ethernetový port jsou skryty za jednu jedinou MAC adresu tohoto Compexu. WPE54G tak provádí jakousi obdobu NAT na fyzické ethernetovské vrstvě. Proč to? Dle normy 802.11x totiž může být v režimu „Infrastructure Client“ připojená pouze 1 MAC adresa. Pro více MAC adres není „bezdrátový paket“ stavěný a proto to musí výrobci Access Pointů a karet různě obcházet (např. WDS, překlad MAC adres, atd.) Co z toho tedy plyne? Jednak je to velká výhoda toho, že na ethernetový port můžete navěsit přes množství HABů a SWITCHů libovolné množství PC. Naopak velkou nevýhodou je to, že pokud provádíte na serveru např. IP Accounting na základě MAC adres, nebudete schopni rozlišit jednotlivá PC za tímto Access Pointem. Všechny se vám budou jevit jako jedno jediné. Jako obrovské plus, které nemá na českém trhu konkurenci, považuji bezproblémovou funkci regulace výstupního výkonu. Výkon lze regulovat v rozsahu 2 – 17 dBm s krokem 1 dBm !!! Navíc tato regulace výkonu funguje ve všech pracovních režimech.[20]

Dále jsem testoval maximální propustnost tohoto bodu v ideálních podmínkách ve všech režimech, tedy ze stolu na stůl bez použití externích antén a porovnal ho s ostatními body, které jsem měl k dispozici. Pro měření jsem použil protokol FTP.

| Režim | DOWNLOAD (ap > pc.) | UPLOAD (pc > ap) |
|---|---|---|
| Access Point | 2760 kB/s | 1850 kB/s |
| Access Point Client | 2480 kB/s | 1420 kB/s |
| Access Point WDS | 1670 kB/s | 1120 kB/s |
| Gateway | 2340 kB/s | 1550 kB/s |
| Routing klient | 2060 kB/s | 1050 kB/s |
| Ethernet adapter | 2750 kB/s | 1650 kB/s |

*Tab. 3: Otestování přenosu*

*Graf č. 1* viz Přílohy

Při výběru Wi-Fi karty pro PC je nejvhodnější volba karty s chipsetem Atheros. Dříve se prodávala karta Z-COM 626, která obsahovala chipset PRISM II, ale v dnešní době si již nevyrábí. Kartami Z-COM 626 máme osazenu většinu vysílacích bodů. V kapitole „Návrh testovaného spoje“ jsou popsány vlastnosti této karty.

## 5.3. Zařízení pro pásmo 5 GHz

V dnešní době je na trhu, také jako u frekvenčního pásma 2.4 GHz, velká nabídka přístupových bodů a klientských adaptérů. Navíc se začínají vyrábět zařízení, která jsou duální, tzn. umožňují pracovat jak v kmitočtovém pásmu 2.4GHz, tak i v pásmu 5GHz.

**Porovnání cen zařízení pro pásmo 5 GHz (přístupové body)**

| Název zařízení | Cena |
|---|---|
| Straight Core WRT-511 AP | 2 137 Kč |
| OvisLink WLA-5200AP | 2 514 Kč |
| Sparklan WX-7800 | 2 721 Kč |
| OvisLink WLA-5000AP | 2 735 Kč |
| Compex WP-54AG | 3 568 Kč |
| ORINOCO AP-4000 802.11 a / b / g | 15 116 Kč |

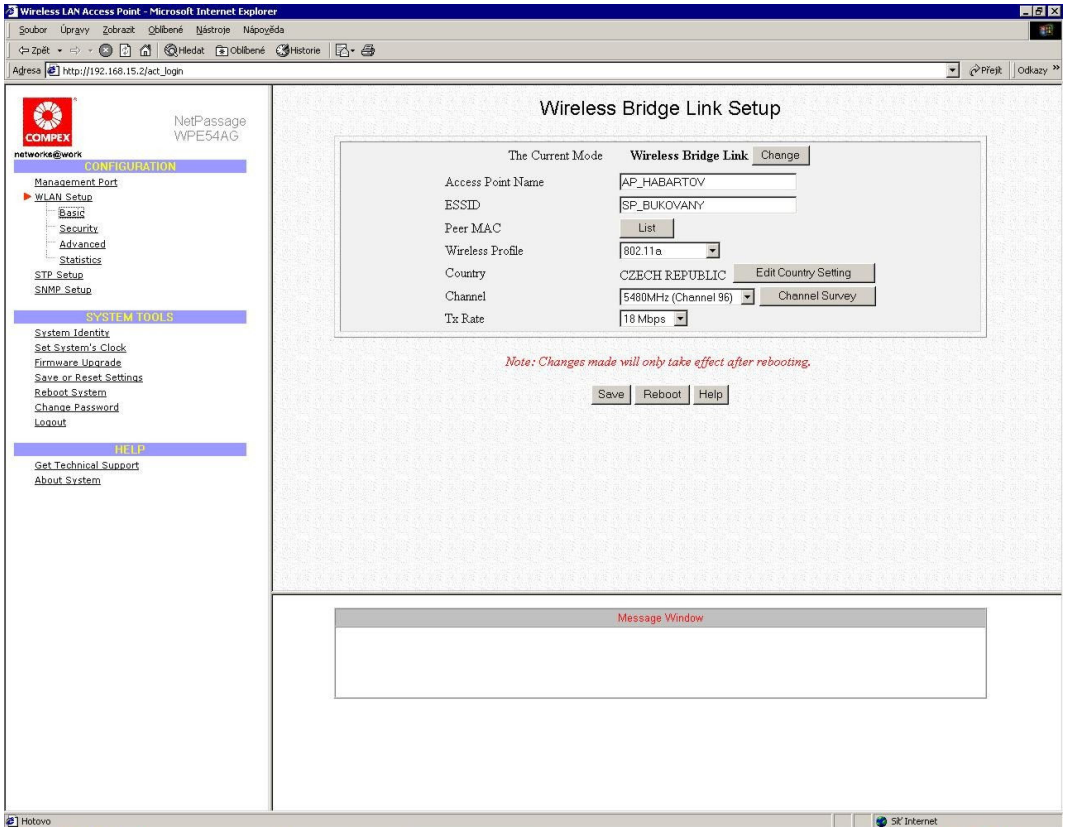
*Tab 4: Porovnání cen přístupových bodů.*

**Porovnání cen zařízení pro pásmo 5 GHz (klienstké adaptéry)**

| Název zařízení | Cena |
|---|---|
| CM9 MiniPCI | 744 Kč |
| CM10 MiniPCI | 775 Kč |
| TP-Link PCI Card 802.11 a | 835 Kč |
| Trendnet TEW 501PC Cardbu | 1 225 Kč |
| Trendnet TEW-504 USB | 1 450 Kč |

*Tab 5: Porovnání cen klientských adaptérů*

Konfigurace bodů je obdobná jako u zařízení pro frekvenci 2.4GHz




*Obr. 3: Ukázka webového rozhraní*

Pro testování a měření jsem opět použil výrobek Compexu model WPE54AG.

**Specifikace zařízení:**

Jednotka pracující v těchto 5 režimech:

- AP Mode
- AP Client Mode
- Gateway Mode
- Wireless Routing Client Mode
- Wireless Ethernet Adapter

Parametry :

**Konektor ext. antény:** RSMA male
**LAN:** 10/100 MBit
**Norma IEEE:** 802.11abg
**Regulace výstupního výkonu:** Ano, po 1dB v celém rozsahu
**Správa pomocí SNMP:** Ano, v1 i v2
**Výstupní výkon:** 802.11a – 14, 802.11bg - 18 dBm
**WLAN:** 2,4 až 2,48; 5,1 až 5,3 5,7 až 5,8
**Zabezpečení:** WEP, WPA, 802.1x

Měření jsem provedl opět ve všech režimech.

| Režim | DOWNLOAD (ap > pc.) | UPLOAD (pc > ap) |
|---|---|---|
| Access Point | 2590 kB/s | 2390 kB/s |
| Access Point Client | 2510 kB/s | 2350 kB/s |
| Access Point WDS | 2380 kB/s | 2100 kB/s |
| Gateway | 2500 kB/s | 2240 kB/s |
| Routing klient | 2350 kB/s | 1950 kB/s |
| Ethernet adapter | 2680 kB/s | 2430 kB/s |

*Tab.6: Otestování přenosu*

*Graf č. 2* viz. Přílohy

Tak jako pro pásmo 2.4GHz, tak i v tomto pásmu používám karty s chipsetem Atheros. Nejrozšířenější kartou je CM9, která obsahuje chip Atheros 5213, nyní je na trhu už novější verze CM10 obsahující Atheros 5214.

## 5.4. Zařízení pro pásmo 10 GHz

Dnes je na trhu celkem 6 českých výrobců**.** Historicky nejstarším výrobcem byla firma KonWes, od které se následovně vývojově odloučila firma Alcoma a Miracle, jež si začal vyrábět vlastní mikrovlnné části, nakonec se odloučila firma SVM. Dále jsou na trhu ještě firmy Summit Development, který koncepčně vyšel z firmy Miracle a firma KPE. Zatímco první skupina firem jsou zkušenými matadory na trhu mikrovlnných spojů a zákaznických řešení, poslední zmínění vnikli na trh v posledních 2 letech a stojaté oligopolní vody zcela rozčeřili.[28]

**Porovnání cen zařízení pro pásmo 10 GHz**

| Název zařízení | Cena |
|---|---|
| Alcoma AL10D V32 | 78 540 Kč |
| ALCOMA AL10D MEL90 | 118 881 Kč |
| SUMMIT QAM 100/10GHz | 146 097 Kč |
| MW link Orcave 2222 / 105Mbps ETH_10GHz | 124 950 Kč |

*Tab 7: Porovnání cen zařízení 10GHz*

Pro testování a měření jsem opět použil výrobek Alcoma model AL10F.

Parametry :

**Kmitočtové pásmo (GHz):** 10,3–10,6
**Kanálování (MHz):** 14 / 28 / 28
**Kapacita MBit:** 47 / 100/ 155
**Modulace QAM:** 32 / 32/ 128
**Výkon TX (dBm):** 3
**Citlivost RX:** –73 dBm
**Napájení:** 48V

Měření jsem provedl v režimu Point to Point.

| Režim | DOWNLOAD (ro2 > ro1) | UPLOAD (ro1 > ro2) |
|---|---|---|
| PtP (Bridge) | 18300 kB/s | 18250 kB/s |

*Tab.8: Otestování přenosu*

*Graf č. 3* viz. Přílohy

## 5.5. Návrh testovaného spoje pro pásmo 2.4GHz, 5GHz a 10GHz

Zde popíši jak postupovat obecně při návrhu bezdrátového spoje a jeho dalšího šíření. Následně podrobně popíši návrh mého spoje jak v pásmu 2.4 GHz, 5GHz, tak i v pásmu 10 GHz.

V prvním případě je potřeba si ujasnit několik následujících aspektů:

**Požadavky na propustnost sítě** – jaké jsou požadavky na rychlost sítě?Očekávaná odpověď je maximální, takže tyto požadavky jsou spojité s finančním limitem a tedy používanou technologií, v daném případě lze čekat volbu mezi 802.11b nebo 802.11g technologií a tedy spočítání a vyhodnocení přínosu a cenových rozdílů mezi cenou jedné a druhé technologie v závislosti na způsobu používání sítě.[4]

**Oblast pokrytí –** jak velká oblast má být pokryta a jaká je hustota uživatelů v jednotlivých částech pokrývané oblasti. [4]

**Možnost mobility** – je požadována plná mobilita uživatelů s plynulým přechodem od jedné stanice k druhé za běhu síťového připojení, nebo se uvažuje spíše „nemobilní připojení“ – tedy jen občasný pohyb, kde automatická rekonfigurace chvilkové přerušení síťového provozu nevadí. [4]

**Počet uživatelů –** kolik uživatelů bude používat bezdrátovou síť a jakou kvalitu očekávají? Jako vždy buďte připraveni na růst počtu uživatelů i jejich kvalitativních nároků, ale snažte se správně odhadnout jejich reálné požadavky. [4]

**Podpora páteřní sítě –** jakým způsobem bude realizováno připojení bezdrátové sítě do páteřní sítě? Bude třeba kvůli bezdrátové síti protáhnout ethernetovou síť, přidat další ethernetové zásuvky? Je možné přístupové body instalovat a připojit do Ethernetu všude tam, kde je potřeba je připojit? [4]

**Logika síťového plánování –** kolik IP adres bude nutné přiřadit bezdrátovým uživatelům, je možné toto přiřazení provést? Nebude nutné provést přečíslování i v ethernetové síti? Jak to bude se směrováním provozu? Bude nebo již je provozován DHCP server? [4]

**Charakteristika používaných aplikací –** je možné používat překlad IP adres pro aplikace, které se v síti mají používat? Jak jsou aplikace citlivé na zpoždění, přenášejí nějaká časově kritická data? Pokud ano, je třeba podívat se po produktech s podporou Point Coordination Function (PCF). [4]

**Požadavky na zabezpečení –** jakým způsobem bude řešena bezpečnost sítě a jaké jsou předpoklady pro její zlepšení? Očekává se provoz bezdrátové sítě v prostoru s omezeným pohybem cizích osob, nebo jde o zcela veřejné prostranství? Omezit přístup k důležitým prostředníkům či službám z bezdrátové sítě? Autentizace uživatele byla dlouho slabinou sítí WLAN. V zásadě můžeme uvažovat pouze o autentizace podle MAC adresy a podle WEP klíče. MAC adresa je problematické řešení, lépe bude používat WEP. Ale i ten přináší problémy, především pak snížení propustnosti sítě a také v distribuci WEP klíčů. Je možné použít další řešení, jako autorizaci 802.1x nebo VPN. [5]

**Vliv prostředí na šíření signálu –** jaké je prostředí, v němž stavíte bezdrátovou síť a jak se na něm projevují vlivy již dříve popsané. Musí signál procházet železobetonovými zdmi, nebo jsou přípojné body v čisté přímé viditelnosti? Co odraz signálu? [4]

**Finance, plánování a nákup –** zde už záleží na zvyklostech každé firmy nebo jednotlivce. Některé firmy požadují výrobky určitých dodavatelů, někdy vyplynou dodavatelé od požadavků na bezpečnost a jednoduchost řešení. Jednotlivci naopak sáhnou po nejvýhodnějším poměru cena – výkon a vzhledem k jejich požadavkům tedy i k nejlevnějším komponentům. Důležité a často opomíjené je plánování projektu – pokud je třeba instalovat složitější síť, už se bez harmonogramu kroků neobejdete, aby bylo možno trefit se do termínů. [10]

**Jakou zvolit anténu a zisk antény?**

Při výběru antény je zapotřebí mít na zřeteli několik parametrů. Ten nejčastěji uváděný je zisk antény, který udává, s jakou intenzitou anténa vyzařuje signál v požadovaném směru. Zisk antény musíte mít na zřeteli, když plánujete parametry přenosové trasy, zejména délku spoje a případné překážce na trase. Zisk antény je závislý na směrovostí a účinností antény. [14]

**Přizpůsobení antény**

Ještě důležitější, ale často přehlížený parametr, je „napěťový činitel stojatého vlnění“ neboli „přizpůsobení“ antény a celé signálové trasy. Přizpůsobení (SWR, VSWR, PSV) udává, jaké množství vysílacího výkonu aktivního prvku je vyzářeno a kolik ho anténa odráží zpět do vysílače. Odražený signál následně degraduje signál, který anténa přijme od vzdáleného vysílače. Přizpůsobení je poměrová veličina, u Wi-Fi antén se většinou udává ve tvaru 1:XX. Například přizpůsobení 1:1,1 znamená útlum –26dB, takže méně než 0,2 % vyzářeného výkonu se odráží zpět a 99,8 % je vyzářeno. Další důležité hodnoty jsou SWR 1:1,2 (-21dB, 1 % odraženého signálu), což je hodnota která se na českých technických univerzitách vyučuje jako mezní pro datové antény a SWR 1:1,5 (-14dB, 4 % odraženého signálu), od kteréžto hodnoty je anténa v podstatě nepoužitelná. Na celkovém přizpůsobení anténní trasy má kromě antény vliv také každý další nehomogenní prvek na anténním rozvodu, tj. každý konektor.

Zásadní rozdíl mezi ziskem a přizpůsobením spočívá v odlišnostech, kterými se projevují. Pakliže bude mít kabelový rozvod větší útlum, je možné použít výkonnější anténu a celkový zisk anténní soustavy zůstane zachován. Špatné přizpůsobení má za následek, že do přijímače vašeho aktivního prvku bude přicházet velké množství odraženého signálu (výtečný link, silný signál), ale přenosové parametry budou špatné. To, jakým způsobem se přizpůsobení projeví záleží také na tom, jak si s odraženým signálem poradí aktivní komponenty. Abyste se vyvarovali problémů s přizpůsobením, je zapotřebí zvolit kvalitní anténu a konektory, nejlépe s protokolem, který uvádí přesně změřené

hodnoty zisku a přizpůsobení. Na rozdíl od útlumu není možné přizpůsobení nijak „dodatečně“ korigovat. [4]

**Rušení**

Doposud jsme hovořili o spojení v ideální situaci, kdy jediné „problémy na cestě“ vytvářelo samo prostředí, ve kterém se šíří signál a kvalita antény a anténního vedení. V praxi se ale často objevuje další činitel, který má vliv na kvalitu datových přenosů. Jedná se o rušení, tj. o situaci, kdy anténa přijímá kromě žádaného ještě další, rušivý signál. Nemusí se bezpodmínečně jednat o jiný Wi-Fi vysílač, „dostatečným“ zdrojem rušení je i špatně odstíněná mikrovlnná trouba (elektromagnetické vlnění o frekvenci 2,4GHz způsobuje rezonanci/ohřev molekul vody). [6]

Jediným způsobem, jak potlačit rušení je použít vhodnou anténu, která bude účinně přijímat požadovaný signál a zároveň bude necitlivá k rušivým signálům z ostatních směrů. Tyto vlastnosti lze rovněž částečně korigovat vhodnou volbou polarizace. Podle vykrývaného prostoru lze antény rozdělit následujícím způsobem:

***Typy antén podle směru vyzařování***

| | |
|---|---|
| Všesměrové | Vykrývají 360 horizontálně, ideální pro použití jako centrální AP v oblastech bez rušení |
| Sektorové | Vyzařují asymetrický paprsek o šířce několik desítek procent. Ideální jako anténa k centrálnímu AP, kterou je možné nasměrovat do oblasti k výskytu klientů. |
| Směrové | Vyzařují symetrický paprsek, na rozdíl od předchozích antén lze jejich pootočením změnit polarizaci vysílání. Jsou ideální jako klientské antény, pro budování spojů bod-bod a antény s širším vyzařovacím úhlem mohou nahradit sektorové antény. |

Při volbě antény je rovněž často zapotřebí brát zřetel na estetické požadavky, ne každému vyhovuje mít na domě parabolu o průměru 110 cm, i když má skvělé parametry….

***Typy antén podle provedení***

| | |
|---|---|
| Tyčové antény | Všesměrové antény; do této skupiny spadají všechny antény od nejmenších „pendreků“ dodávaných s aktivními prvky až po outdoorové antény se ziskem přes 10dBi. |
| Panelové antény | Antény ve tvaru panelu, podle vyzařovací charakteristiky bývají buďto sektorové nebo směrové. |
| YAGI antény | Vývojově nejstarší typ antény, tyč s mnoha „fousky“. V současnosti obvykle bývají uzavřeny ve vodotěsném pouzdru. Z hlediska rušení je nepříjemná přítomnost tzv. vedlejších vyzařovacích laloků. |
| Síta (Grid antény) | Směrové antény, díky provedení jsou méně náchylné na poškození větrem, ale mají vyšší šumové číslo. |
| Paraboly | Směrové antény s nejlepšími parametry, vzhledem k plnému kovovému talíři jsou náchylné na vychýlení větrem. |

**Důraz na kvalitu**

Nejkvalitnější antény pro pásmo 2,4GHz dosahují přizpůsobení 1:1,1 (-22dB) a pro pásmo 5GHz 1:1,2. Je možné ale narazit i na antény, které oficiálně udávají 1:2! Při měření pak můžete zjistit, že parametry jsou často ještě mnohem horší. Všechny naše antény jsou průběžně přeměřovány a našim zákazníkům dodáváme pouze ty, které vyhoví přísným požadavkům na kvalitu. Mnoho zákazníků je velmi překvapeno když zjistí, že ty „lacinější“ součásti

bezdrátových sítí mají na funkčnost a spolehlivost datových přenosů často větší vliv, než samotné aktivní prvky. [4]

## Výpočet kvality radiového spoje

Aby zejména spojení na větší vzdálenost bylo dostatečně kvalitní a fungovalo spolehlivě po celý rok, je potřeba věnovat dostatek prostoru jeho pečlivému naplánování. Díky propočtení ziskovosti a ztrátovosti jednotlivých komponent sítě a analýze trasy, kterou signál putuje, se můžeme vyhnout leckterým překvapením a dalším výdajům.

Kvalitu radiového spojení určují následující kritéria:

♦ **Efektivní vysílací výkon** – jde o součet vysílacího výkonu Wi-Fi zařízení a zisku antény, od kterého se odečte ztráta na kabelu a konektorech.

♦ **Ztráta při přenosu** – jde o ztráty na signálu ve volném prostoru a ztráty vlivem zásahu do První Fresnelovy zóny .

♦ **Efektivní citlivost přijímače** – jde o součet zisku antény a citlivosti přijímače s odečtem ztrát na kabelu a konektorech.

Celkový vzorec, podle něhož bychom se měli při propočtu přenosové trasy orientovat, zní:

$$\mathbf{P_r = P_t – L_p + G_t + G_r – L_t - L_r}$$

$P_t$ = vysílací výkon vysílače (v dBm nebo dBW, stejná jednotka jako u $P_r$)

$L_p$ = ztráty signálu přenosu (v dB)

$G_t$ = zisk antény vysílače (dBi)

$G_r$ = zisk antény přijímače (dBi)

$L_t$ = útlum (ztráty) mezi vysílačem a anténou vysílače (kabely + konektory) (dB)

$L_r$ = útlum (ztráty) mezi přijímačem a anténou přijímače (kabely + konektory) (dB)

**Výsledek $P_r$ je požadovaná citlivost přijímače** v dBm nebo dBW (shodně s $P_t$). Tuto požadovanou citlivost porovnáme s parametry přijímače a zjistíme, jakou rychlostí či zda vůbec vypočtená trasa bude fungovat. Celý výpočet a jeho vyhodnocení si ukážeme poté, co budeme schopni vypočítat všechny proměnné, tedy především ztráty při přenosu.

Zatímco zisk antény a vysílací výkon vysílače i ztráty na kabelu a konektorech máme udávány výrobcem nebo je již umíme spočíst,neznámou do tohoto vzorečku pro nás zůstává ztráta signálu ve volném prostoru. Výsledkem tohoto vzorečku je očekávaná úroveň signálu na přijímači. Tato úroveň nám určí, zda jsme schopni signál vůbec na přijímači použít a pokud ano, jakou rychlostí se budou přenášet data tímto Wi-Fi spojem. [4]

**Ztráty signálu při přenosu**

Ztráta signálu při přenosu se v radiové praxi rozděluje do tří hlavních skupin podle svého druhu a příčiny.

1) **Refrakce (lom)** o zemskou atmosféru. Horní vrstvy zemské atmosféry změní dráhu radiového signálu lomem. U frekvence 2,4GHz a vysílacího výkonu, jímž Wi-Fi disponuje, se netřeba lomu o zemskou atmosféru obávat, tak daleko signál nedoletí.

2) **Difrakce (ohyb)** o předměty v blízkosti trasy signálu. Toto je již podstatnější problém. Propočet podmnožiny difrakce, tedy První Fresnelovy zóny. Pokud objekt zasahuje zcela do Fresnelovy zóny, není trasa použitelná a není potřeba ohyb vůbec uvažovat.

3) **Reflexe (odraz)** o zem. Vzhledem k charakteristice signálu 2,4 GHz představuje odraz signálu na delší vzdálenosti vážný problém, jenže vzhledem k tomu, že dlouhé trasy v metropolitních oblastech spíše zatěžuje difrakce, uvažuje se spíše v případě, když jde o delší trasy nad 4 km, které jsou vedeny nad rovným terénem nebo nad vodní hladinou. [4]

### Ztráty ve volném prostoru

Samostatnou a pochopitelnou skupinou jsou ztráty ve volném prostoru, tedy ztráty, k nimž dochází průchodem atmosférou, volným prostorem zcela bez překážek a výše uvedených vlivů refrakce, difrakce či reflexe. K těmto ztrátám dochází vždy a je potřeba je fixně započítat. [4]

Použijeme k tomu Fresnelovu formuli, která nám po dosazení radiové frekvence a vzdálenosti vyčíslí ztrátu v decibelech:

**Ztráta ve volné prostoru:**

$Lp\ (dB) = 92{,}45 + 20\log_{10} F + 20\ LOG_{10}\ d$

Kde:

Lp = ztráta ve volném prostoru (dB)

F = frekvence v GHz

dB = decibely

d = vzdálenost v kilometrech

Ve vzorečku nemusíme přesně uvažovat frekvenci kanálu, který používáme - tato změna se projeví až za desetinou čárkou, a tedy nemá smysl ji uvažovat, vzoreček uvádíme s možností dosazení frekvence spíše pro případ, že byste potřebovali vypočítat ztrátu při přenosu dle standardu 802.11 a v pásmu 5 GHz (nebo v jakémkoliv jiném případě). [4]

### Difrakce, ohyb signálu

Zatímco lom o zemskou atmosféru jsme již z našich úvah o šíření signálu 2,4 GHz vynechali, můžeme se podívat na problém difrakce, tedy ohybu signálu.

Trocha teorie: ohyb vlnění je dosti složitý jev a lze ho vysvětlit podle Huygensova principu. Každý bod tělesa, do něhož dospělo vlnění (tzv. primární vlnění) v určitém časovém okamžiku, se stává elementárním zdrojem vlnění (sekundární vlnění) – působením primární vlny se těleso polarizuje (je-li dielektrické) anebo se na jeho povrchu indukují proudy, je-li vodivé. V dalším časovém okamžiku je toto těleso obalovou křivkou všech elementárních

vlnoploch. Výsledná intenzita pole kdekoli v okolí tělesa (i za ním) je součtem intenzity primární a sekundární vlny.

Vlnění se tedy podle tohoto principu může dostat i za překážky, kde dochází k interferenci vlnění, což se **projevuje jako difrakce neboli ohyb.**

Ohyb souvisí jak s rozměry překážky, tak s vlnovou délkou vlnění, které na překážku dopadá. Obecně platí, že ohyb je při určitém rozměru překážky a pozorovatele tím výraznější, čím větší je vlnová délka vlnění. Směr šíření se označuje paprskem. Směr šíření vlnění je ovlivněn ohybem vlnění na překážkách. Tento vliv je však tím větší, čím větší je vlnová délka vlnění.

**Ztráta způsobená difrakcí:**

$v = h \sqrt{(2(d1 + d2) / (\lambda\ d1\ d2)}$

$Ld\ (dB) = 20 \log (0{,}225/v)\ /\ \log (10)$

Kde:

h = výška mezi vrcholem antény a vrcholem překážky v metrech

d1 = vzdálenost od antény 1 k překážce v metrech

d2 = vzdálenost od antény 2 k překážce v metrech

$\lambda$ = vlnová délka v metrech zde dosadíme 0,12 pro pásmo 2,4 GHz

Výsledkem mezivýpočtu je difrakční parametr v, který dosadíme do druhého vzorce, abychom získali Ld, ztrátu způsobenou difrakcí. [4]

**Výhrady k výpočtu:**

♦ Výsledek difrakce u obousměrných přenosů je stejný, ať prohodíme d1 ad2.

♦ Výpočet bude správný pouze tehdy, pokud vzdálenost d1 a d2 jsou významně větší než výška h.

♦ Výsledek připočteme ke ztrátě ve volném prostoru.

**Korekce vlivu zalesnění**

Pokud nestojí v cestě signálu dům, ale přírodní útvar, můžeme počítat s tím, že je zalesněný. Stromy představují další ztrátu – jednak proto, že samy o sobě jsou vysoké a jejich výška není do výšky kopce v mapách zahrnuta, dále také proto, že úspěšně elektromagnetické vlnění pohlcují. Proto bychom v případě zalesněného kopce měli ještě provést korekci vlivu zalesnění. [4]

K tomu použijeme empirický vzorec ITU-R pro korekci zalesnění:

$L_{leaf} = 0{,}2\ (f / 10^6)^{0{,}3}\ df^{0{,}6}$

Kde:

f = frekvence v Hz

df = výška stromů v metrech

Výslednou hodnotu **Lleaf** pro frekvenci **f** můžeme dále korigovat pro odhad procenta zalesnění, pokud tedy odhadujeme zalesnění na 50 %, vynásobíme hodnotu Lleaf 0,5, abychom získali korekci útlumu pro padesátiprocentní zalesnění kopce. [4]

**Příklad:** frekvence 2,45 GH, výška stromů 20 metrů představují útlum 12,5 dB. Pokud bychom uvažovali poloviční zalesnění kopce, hovořili bychom o 6,3 dBm (zaokrouhlení na jedno desetinné místo postačuje).

**Výpočet parametrů bezdrátového spoje**

Dosah jakéhokoliv rádiového spojení je založen v podstatě na jediné věci: úroveň signálu, který vyjde z výstupu vysílače, může po cestě poklesnout jen natolik, aby byla na vstupu přijímače vyšší, než je jeho citlivost (tedy schopnost ho ještě zpracovat). Úmyslně nyní ignorujeme parametry rušení a přizpůsobení.

Pro snazší práci se všechny hodnoty udávají v dB, tj. poměrových jednotkách (podobně jako procenta). To sice zní složitě, ale v praxi to přináší samé výhody. Důležité je si ještě zapamatovat, že změna –3dB odpovídá snížení

na polovinu, +3dB zvýšení na dvojnásobek a že výkon aktivního prvku je udáván v poměru k 1 mW (0 dB).

Z výše uvedených informací se dá snadno odvodit následující tabulka:

**Převod vysílacího výkonu v mW a dBi**

| | |
|---|---|
| 3dBm | 2mW |
| 6dBm | 4mW |
| 9dBm | 8mW |
| 12dBm | 16mW |
| 15dBm | 32mW |
| 18dBm | 64mW |

Obligátních 20dBi odpovídá vysílacímu výkonu 100mW, což je limit stanovený ČTU, VO-R/12/08.2005-34. K vysílači s výkonem 20dBi můžete připojit anténu o zisku 0dBi a výsledná sestavu bude vyhovovat požadavků ČTU.

Anténu se ziskem 0dBi budete hledat v nabídce obchodů marně. Taková anténa by totiž musela šířit signál homogenně všemi směry, byla by ideálně všesměrová. Výrobci antén ale většinou usilují o to, aby jejich výrobek vyzařoval (a přijímal) signál ve směru, který potřebují a naopak byl necitlivý v ostatních směrech. Tím, že se pozmění vyzařovací charakteristika antény, získá tato anténa v některém směru vyšší citlivost, než zmiňovaná „ideální všesměrová anténa“. Tento „zisk“ v konkrétním směru je přesně ten parametr, který je běžně udáván u antén. Zároveň bývá uveden vyzařovací úhel, který popisuje v jakém rozsahu neklesá zisk antény pod 3dBi (50%) maximální hodnoty.

Pakliže Vás přijde kontrolovat ČTU, nebude zvažovat jak směrovou anténu používáte. Ve VO je totiž uvedený maximální vyzářený výkon E.I.R.P., tzn. uvažuje, jako byste používali anténu se ziskem 0dBi. Jestliže tedy použijete anténu s větším ziskem, musíte odpovídajícím způsobem snížit vysílací výkon aktivního prvku, tak aby výkon celé soustavy (v nejziskovějším směru) nepřesáhl 20dBi.

Při výpočtu vyzářeného výkonu byste rovněž měli počítat s tím, že koaxiální kabely a jednotlivé konektory mají vlastní útlum, který naleznete v jejich datasheetech (technických listech).

Elektromagnetické záření, které se šíří volným prostorem je také „tlumeno“. Tento útlum trasy je závislý na vzdálenosti a momentálních klimatických podmínkách, pro základní plánování by Vám měla postačit následující tabulka.

| **Vzdálenost** | **Útlum pro 2,4GHz** | **Útlum pro 5GHz** |
|---|---|---|
| 50 m | -74dB | -81dB |
| 100 m | -80dB | -87dB |
| 200 m | -86dB | -94dB |
| 300 m | -90dB | -97dB |
| 500 m | -94dB | -101dB |
| 750 m | -96dB | -105dB |
| 1000 m | -100dB | -107dB |
| 1500 m | -104dB | -111dB |
| 2000 m | -106dB | -114dB |
| 5000 m | -114dB | -121dB |
| 10000 m | -120dB | -128dB |

Poslední parametr, který potřebujete znát pro výpočet bezdrátového spoje je citlivost aktivního prvku. Platí, že čím silnější signál, tím vyšší přenosové rychlosti lze dosáhnout. Například oblíbená karta Zcomax XI-626 má následující parametry:

-85 dBm (11 MBit)

-88 dBm (5,5 MBit)

-89 dBm (2 MBit)

-92 dBm (1 MBit)

Díky využití poměrových jednotek je nyní výpočet parametrů bezdrátového spoje velice jednoduchý. Pro ukázku si spočítáme spoj na vzdálenost 1000 m s využitím XI-626 a 14-ti dBi antén.

Na každé straně spoje je koaxiální vedení, jehož celkový útlum činí –3dB (kabely + konektory). Aby byly dodrženy podmínky ČTU, musí být vysílací výkon karty snížen na 9dBm (9dB karta –3dB kabeláž + 14dB anténa = 20dB celkový vysílací výkon). Na výstupu z antény m tedy signál sílu 20dB, útlum prostředí činí –100dB, takže k druhému bodu dorazí signál o síle –80dB. Díky zisku antény 14dBi a ztrátě 3dB na koaxiálním vedení bude mít signál na vstupu

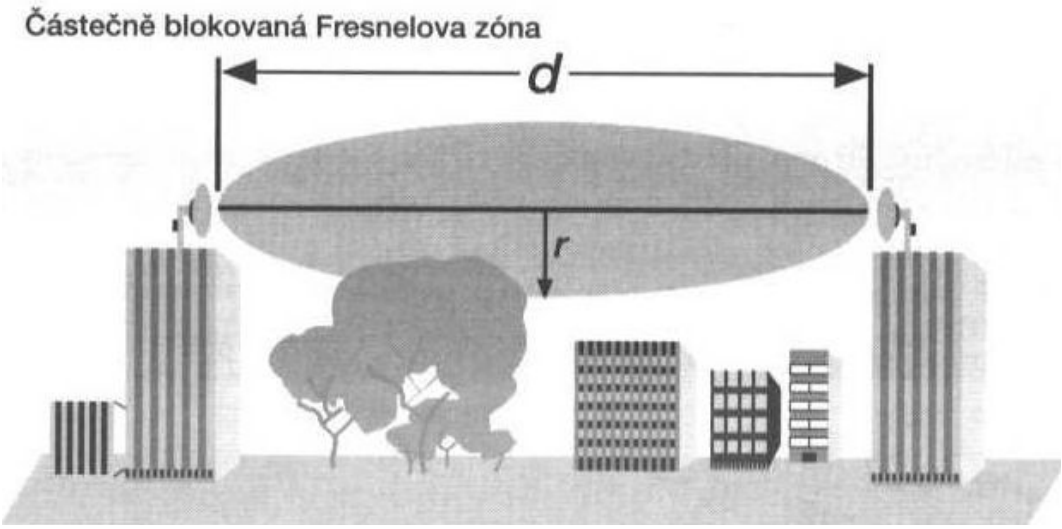
do druhé karty sílu –69dB, což je zcela dostatečné pro plnou rychlost 11MBit a s doporučovanou rezervou 20dB dostačuje pro rychlost 2MBit. Z výpočtu je jasně vidět, že použitím ziskovější antény v kombinaci se snížením vysílacího výkonu aktivního prvku lze realizovat spojení na delší vzdálenost. V případě, že použijete různou konfiguraci zařízení na obou koncích rádiového spoje, je zapotřebí provést si tento výpočet pro oba směry. Pro přenosovou rychlost je pochopitelně limitující ten horší výsledek.

Na závěr je nezbytné připomenout, že nikde v tomto výpočtu není uvažována účinnosti antén a přizpůsobení jednotlivých prvků koaxiálního vedení a samotné antény. Účinnost antény nemá rušivý vliv na kvalitu signálu, pouze ho zeslabuje (podobně jako útlum). Naopak přizpůsobení (SWR) způsobuje, že vlastní odražený signál se mísí se signálem přijatým ze vzdáleného vysílače a degraduje ho. Z hlediska datových přenosů je SWR mnohem důležitější parametr než zisk a útlum. [14]

## První Fresnelova zóna a její vliv na praktický dosah

První Fresnelova zóna je jedním z jevů, jemuž můžeme připisovat velkou část názorů na to, že šíření signálu v pásmu 2,4GHz je duchařina. Ačkoliv pojem Fresnelovy zóny je mezi radioamatéry a lidmi znalými antén známe pojem akceptovaný, v mnoha knihách informujících o Wi-Fi o něm zmínku nenalezneme, nebo jen velmi nevýraznou. Přitom právě zásahem do Fresnelovy zóny se snadno můžeme nadít toho, že teoreticky čistě viditelný spoj na teoreticky bezproblémovou vzdálenost nebude prakticky použitelný.

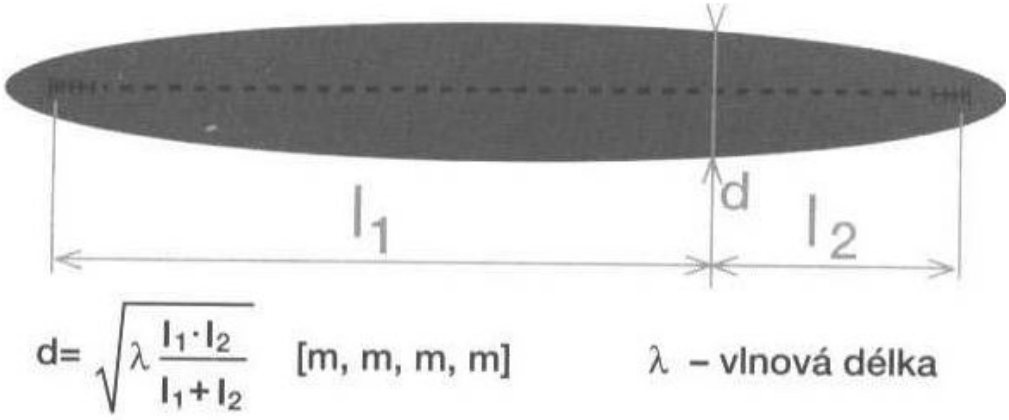
Elektromagnetická vlna se sice šíří po přímce, ale protože je to vlnění, podléhá dalším fyzikálním zákonům (Huygensův princip). Proto je převážná část energie vlny nesena v prostoru okolo přímky spojující vysílací a přijímací antény. Tento prostor má tvar pomyslného doutníku, elipsoidu, s největším průměrem uprostřed trasy. Tato doutníkovitá oblast, kde se přenáší cca 90 % energie, se nazývá **První Fresnelova zóna.** [4]




*Obr .4: Částečně blokovaná Fresnelova zóna[4]*

Na obrázku vidíte, jak taková Fresnelova zóna vypadá a jak se projevuje vliv stromu, který do ní zasahuje. Ačkoliv spoj je na první pohled v přímé viditelnosti, vlivem stínění ve Fresnelově zóně bude potřeba použít kvalitnější antény a kabely, nebo antény posunout výše.

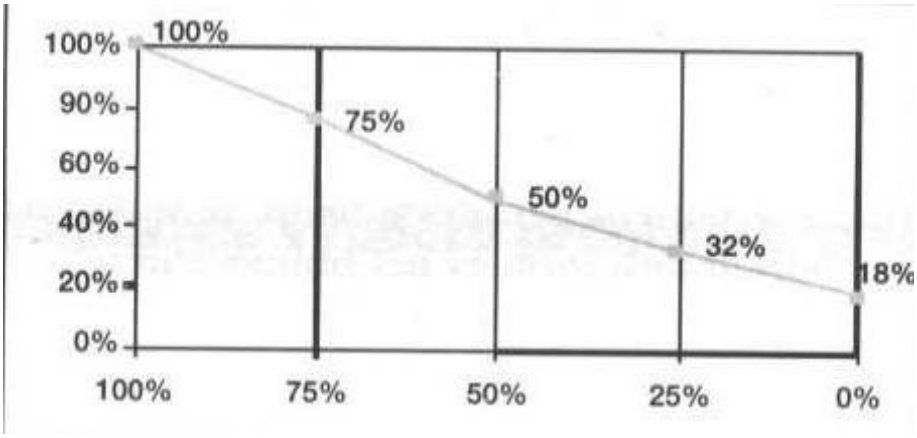
Pro vzdálenost 1 km činí poloměr První Fresnelovy zóny cca 5 m, pro vzdálenost 7 km již cca 13 m. Pro výpočet poloměru První Fresnelovy zóny můžeme použít následující vzoreček.




*Obr. 5: Výpočet Fresnelovy zóny[4]*

**Pro pásmo 2,4 GHz uvažujeme vlnovou délku 12,48 cm, vzoreček pro výpočet je uveden. Do vzorce tedy za λ dosadíme 0,1248 metru.**

Pro rychlý odhad můžete použít následující graf. Vodorovná osa vznačuje procento porušení Fresnelovy zóny, svislá osa snížení teoretického dosahu.

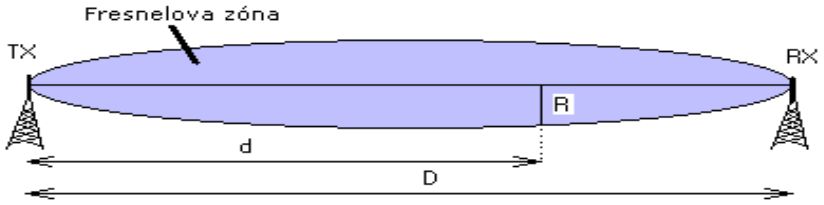



*Graf 4: Procento porušení Fresnelovy zóny[4]*

Např. pokud se přímá spojnice antén dotýká vrcholků mezilehlých objektů (budov), jedná se o 100%ní porušení 1. Fresnelovy zóny. Skutečný dosah se redukuje podle grafu na pouhých 18 % teoretické hodnoty. Při spojení na 1 km stačí umístit antény o 5 m výše (poloměr 1. Fresnelovy zóny na 1 km) a spoj bez problémů dosáhne teoretických parametrů. [4]

**Fresnelova zóna**

Při budování bezdrátového spoje je zpravidla uváděno, že jednou z nutných podmínek (v kmitočtových pásmech 2,4GHz a 5GHz) je přímá viditelnost mezi přijímací a vysílací anténou. To ale není podmínka postačující! Pro kvalitní přenos musí být volná (bez překážek) ještě tzv. Fresnelova (čti frenelova) zóna, tedy určitý prostor kolem spojnice (přímky) mezi vysílací a přijímací anténou. Fresnelova zóna má doutníkovitý tvar (elipsoid) s nejširším průměrem uprostřed vzdálenosti mezi anténami. [14]




*Obr. 6: Výpočet velikosti Fresnelovy zóny[14]*

V prostoru uvnitř této zóny by se neměla vyskytovat žádná překážka, ani by do ní neměla třeba částečně zasahovat (např. střecha nějakého domu nebo strom).

Narušená Fresnelova zóna většinou nemá za následek příliš podstatné snížení úrovně signálu. Jelikož ale v případě jejího narušení dochází k rušivým odrazům, snižuje se kvalita přenosu dat (ztráta paketů, nižší dosažitelná rychlost), stejně jako u nevyhovujícího přizpůsobení. Při realizaci každého spoje by se mělo vyvinout maximální úsilí k tomu, aby bylo volných aspoň 60 % uvedeného průměru zóny. Často stačí umístit anténu o kus výš, ale nezapomínejte, že Fresnelova zóna má kruhový průřez, a že její limity tedy platí i do stran. Průměr Fresnelovy zóny v jejím libovolném místě lze vypočítat, na webu naleznete mnoho stránek, které vám umožní vypočíst poloměr Fresnelovy zóny v závislosti na délce spoje, použité frekvenci a vzdálenosti překážky.

Např. maximální průměr Fresnelovy zóny v následující stručné přehledové tabulce. Je sestavena pro různé celkové délky trasy mezi anténami:

**Maximální průměr první Fresnelovy zóny podle vzdálenosti a frekvence**

| Vzdálenost | Pásmo 2,4GHz | Pásmo 5GHz |
|---|---|---|
| 100 m | 1,37 m | 1,22 m |
| 200 m | 1,93 m | 1,73 m |
| 300 m | 2,37 m | 2,12 m |
| 400 m | 2,73 m | 2,44 m |
| 500 m | 3,06 m | 2,73 m |
| 700 m | 3,62 m | 3,23 m |
| 1000 m | 4,32 m | 3,87 m |
| 1200 m | 4,73 m | 4,23 m |
| 1500 m | 5,29 m | 4,73 m |
| 2000 m | 6,11 m | 5,47 m |
| 2500 m | 6,83 m | 6,11 m |
| 3000 m | 7,48 m | 6,69 m |
| 4000 m | 8,64 m | 7,73 m |

**Jak se vyvarovat problémům s 1. Fresnelovou zónou?**

Nepodceňujte nic, co je v okolí přenosové trasy. Nezapomínejte, že 1. Fresnelova zóna má tvar doutníku, nikoliv placky, a tedy že ji ohrožují nejenom tělesa umístěná pod přenosovou trasou, ale také vedle ní (s problémem nad ní se asi nesetkáte). Signál sice teoreticky můžete prostřelit v úzkém průseku mezi stromy nebo mezi panelovými domy, ale v praxi právě díky zásahu těchto objektů do 1. Fresnelovy zóny bude výsledek velmi špatný.

Řešení je přitom většinou docela snadné a stačí dostat obě antény o několik metrů výše. Věnujme chvíli času práci s kalkulačkou a odhadu vzdálenosti, abychom si spočítali, jaký je poloměr Fresnelovy zóny v místě, kde do ní zasahují cizí tělesa a o kolik metrů tedy bude nutné antény posunout. Výroba stožárů nás většinou přijde levněji, než se snažit ztrátu ve Fresnelově zóně dohonit jinak, například dražší anténou či lepším kabelem. [14]

## 5.6. Praktické otestování bezdrátového spoje v provozu

Pro praktické ověření funkčnosti jednotlivého typu spoje pro pásmo 2.4GHz, 5GHz a 10GHz jsem použil stávající spoje bod-bod mezi našimi jednotlivými přístupovými body.

### 5.6.1. Praktické otestování v pásmu 2.4GHz

Nejprve jsem otestoval spoj v kmitočtovém pásmu 2.4GHz. Testování jsem prováděl ve venkovním provozu, aby se ukázaly případné atmosférické vlivy nebo rušení. K testování jsem použil bezdrátovou kartu Z-COM 626 a celé měření jsem provedl na platformě PC s operačním systémem Linux, včetně výstupních grafů. Testování jsem prováděl dvě. První bylo bez zatížení spoje a druhé bylo při plném zatížení. Vždy se jednalo o zjištění délky odezvy (ping) a maximální reálné propustné rychlosti.

Testovaný spoj se skládá z:

- 2x PC s naším upraveným systémem LinRete
- 2x karta Z-COM 626 …. *obr. č. 2* viz Přílohy

- 2x směrová anténa Andrew 18 dBi *obr. č. 3* viz Přílohy
- 30 m kabelu RLA 10 (s útlumem 0,2dBi/m)
- 6x konektor N
- 2x bleskojistka
- 2x pigtail N -> SMA

Vše je koncipováno tak, aby nebyl překročen povolený vysílací výkon, který je povolen ČTU. [12]

Měření bylo prováděno na vzdálenost 856 m … mapa na *obr. č. 4* viz Přílohy

Nejprve jsem si musel připravit jednotlivé konfigurace na jednotlivých počítačích.

Na testovaných kartách byl následující firmware

*AP_KRASLICE2: -root-*
*# hostap_diag wlan2*
*Host AP driver diagnostics information for 'wlan2'*

*NICID: id=0x8013 v1.0.0 (PRISM II (2.5) Mini-PCI (SST parallel flash))*
*PRIID: id=0x0015 v1.1.1*
*STAID: id=0x001f v1.8.0 (station firmware)*

Pro konfiguraci je nutné mít nainstalován Wireless Extensions. V mém případě se jedná o verzi 18. Dále musí být nainstalován ovladač Hostap.

Nastavení interface na straně vysílacího AP:

*AP_KRASLICE2: -root-*

*modprobe hostap_pci*
*iwconfig wlan2 mode master*
*iwconfig wlan2 essid "SP_KRASLICE4"*
*iwconfig wlan2 channel 8*
*ip addr add 80.188.19.65/29 dev wlan2*
*ip link wlan2 up*

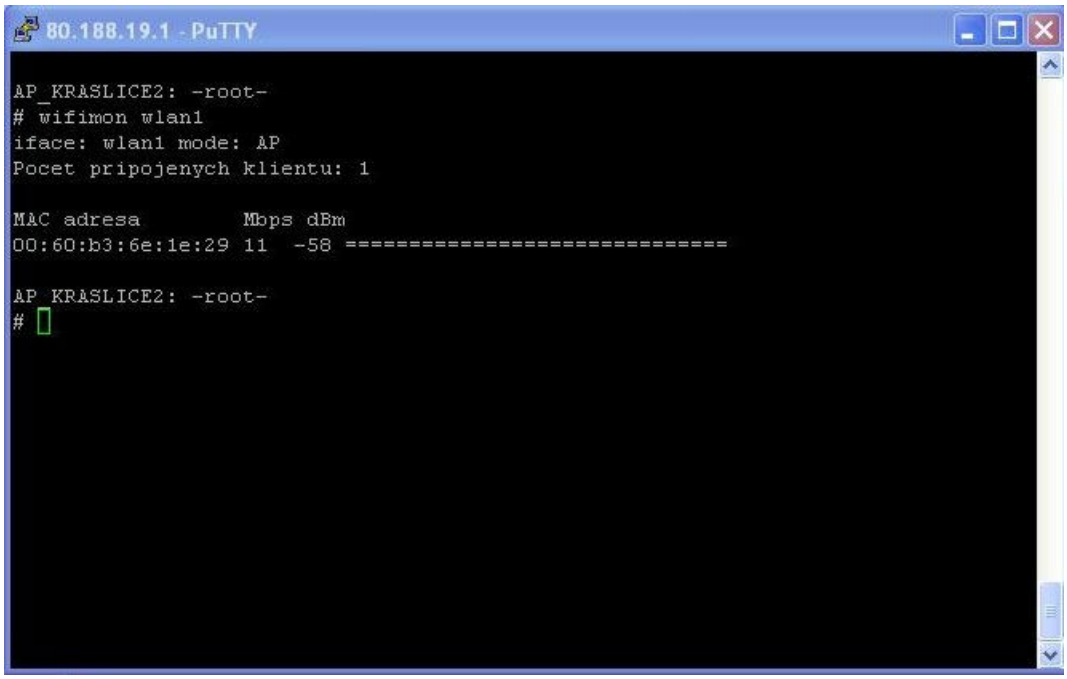
Nastavení interface na straně přijímacího AP:

*AP_KRASLICE4: -root-*

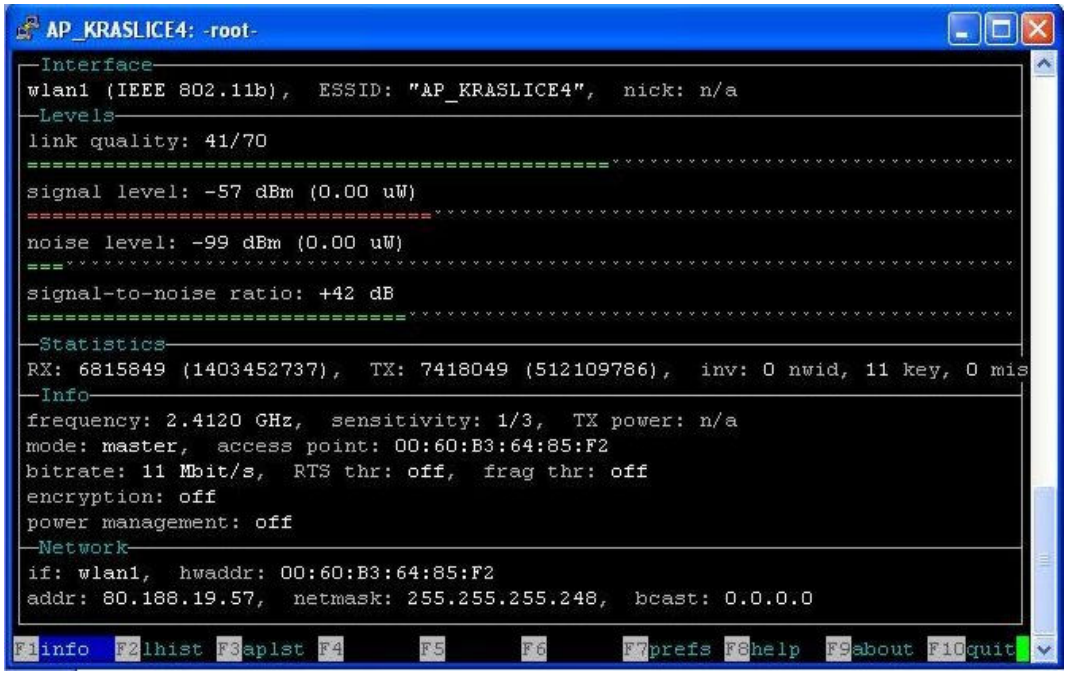
*modprobe hostap_pci*

*iwconfig wlan0 mode managed*
*iwconfig wlan0 essid "SP_KRASLICE4"*
*ip addr add 80.188.19.66/29 dev wlan2*
*route add default gw 80.188.19.65*
*ip link wlan0 up*

Jednotlivá AP se spojila. Jako důkaz přikládám obrázky zobrazující sílu signálu.




*Obr. 7: Síla signálu na straně AP*




*Obr. 8: Síla signálu na straně klienta*

Nyní se již můžu pustit do samotného testování. Výsledek testů jsem zhodnotil v tabulce a provedl k ní příslušné grafy. Reálná rychlost přenosu byla spoje 6 MBit half-duplex.

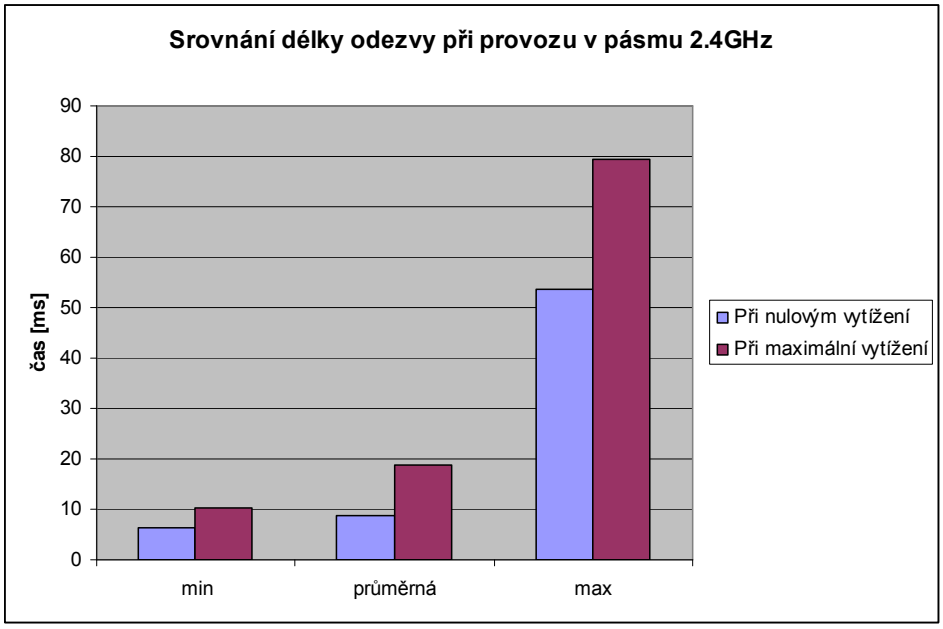
**Při nulovém vytížení**

| Odezva | Čas (ms) |
|---|---|
| min | 6,286 |
| průměrná | 8,783 |
| max | 53,635 |

**Při maximálním vytížení**

| Odezva | Čas (ms) |
|---|---|
| min | 10,365 |
| průměrná | 18,861 |
| max | 79,283 |

*Tab.9: Výsledky testů měření*




*Graf 5: Srovnání délky odezvy*

### 5.6.2. Praktické otestování v pásmu 5Ghz

Další testování jsem prováděl v kmitočtovém pásmu 5GHz. Testování jsem prováděl ve venkovním provozu, aby se ukázaly případné atmosférické vlivy nebo rušení. K testování jsem použil bezdrátovou kartu CM9 obsahující chip ATheros 5212 a celé měření jsem provedl na platformě WRAP s operačním systémem Linux, včetně výstupních grafů. Testování jsem prováděl dvě. První bylo bez zatížení spoje a druhé bylo při plném zatížení. Vždy se jednalo o zjištění délky odezvy (ping) a maximální reálné propustné rychlosti.

Testovaný spoj se skládá z:

- 2x WRAP s naším upraveným systémem LinRete …. *obr. č. 5* viz Přílohy
- 2x karta CM9 …. *obr. č. 6* viz Přílohy
- 2x směrová anténa JRC-24 dBi *obr. č. 7* viz Přílohy
- 12 m kabelu RLA 10 (s útlumem 0,6dBi/m)
- 8x konektor N
- 2x bleskojistka

Vše je koncipováno tak, aby nebyl překročen povolený vysílací výkon, který je povolen ČTU.

Měření bylo prováděno na vzdálenost 792 m … mapa na *obr. č. 8* viz Přílohy

Nejprve jsem si musel připravit jednotlivé konfigurace na jednotlivých počítačích.

Na testovaných kartách byl následující firmware

*AP_KRASLICE2: -root-*
*# hostap_diag wlan2*
*Host AP driver diagnostics information for 'wlan2'*

*NICID: id=0x8013 v1.0.0 (PRISM II (2.5) Mini-PCI (SST parallel flash))*
*PRIID: id=0x0015 v1.1.1*
*STAID: id=0x001f v1.8.0 (station firmware)*

Pro konfiguraci je nutné mít nainstalován Wireless Extensions. V mém případě se jedná o verzi 18. Dále musí být nainstalován ovladač MadWi-Fi.

Nastavení interface na straně vysílacího AP:

*AP_KRA_SEVER2: -root-*

*/usr/local/bin/wlanconfig ath1 destroy*
*/usr/local/bin/wlanconfig ath1 create wlandev wifi1 wlanmode ap*
*/sbin/ip addr add "88.103.208.181/30 dev ath1*
*/sbin/iwconfig ath1 essid "SP_VLEK"*
*/sbin/iwpriv ath1 mode 1*
*/sbin/iwconfig ath1 channel 100*
*/sbin/iwconfig ath1 rate 18M*
*/usr/local/sbin/athctrl ath1 -d 800 # nastavení vzdálenosti*
*sleep 10s*
*/sbin/iwconfig ath1 channel 100*

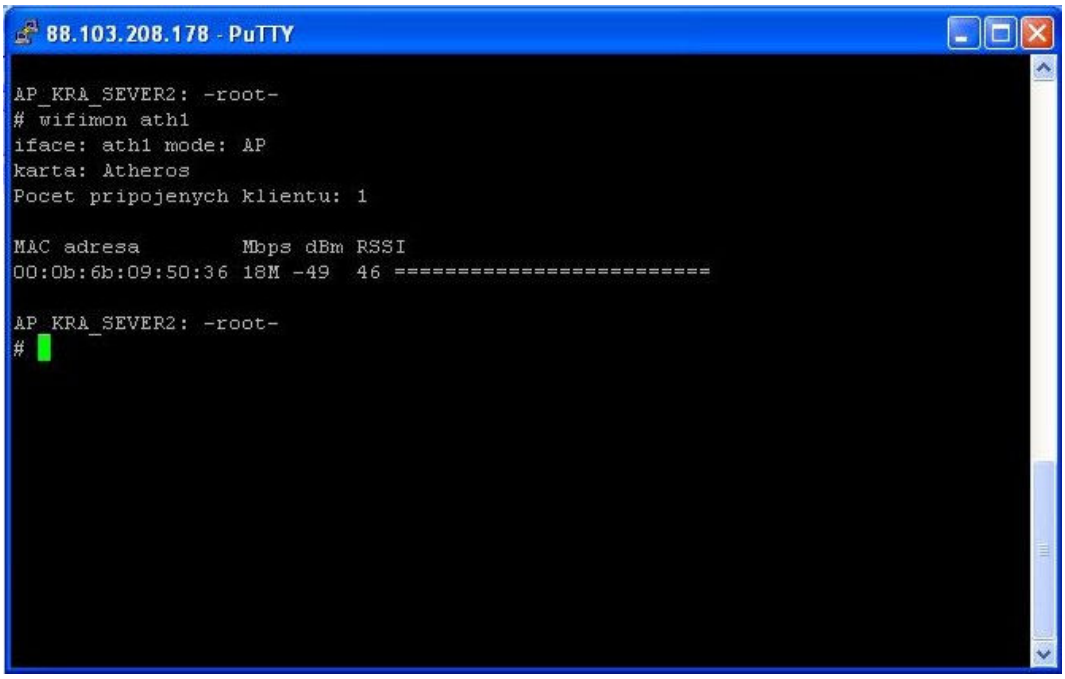
Nastavení interface na straně přijímacího AP:

*AP_VLEK: -root-*

*/usr/local/bin/wlanconfig ath0 destroy*
*/usr/local/bin/wlanconfig ath0 create wlandev wifi0 wlanmode sta*
*/sbin/ip addr add "88.103.208.182/30 dev ath1*

*/sbin/iwconfig ath0 essid "SP_VLEK"*
*/sbin/iwpriv ath0 mode 1*
*/sbin/iwconfig ath0 channel 100*
*/sbin/iwconfig ath0 rate 18M*
*/usr/local/sbin/athctrl ath0 -d 800  # nastavení vzdálenosti*
*sleep 10s*
*/sbin/iwconfig ath0 channel 100*

Jednotlivá AP se spojila. Jako důkaz přikládám obrázek zobrazující sílu signálu.




*Obr. 9: Síla signálu na straně AP*

Výsledky testů jsem opět zpracoval do tabulky a vytvořil z ní příslušný graf.

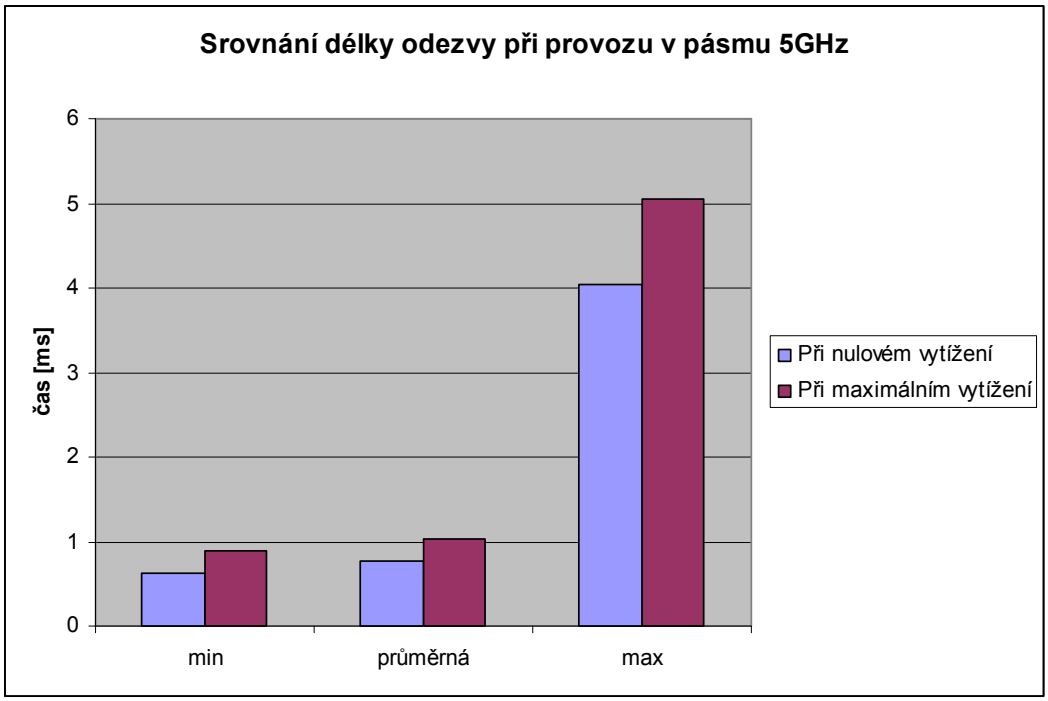
**Při nulovém vytížení**

| Odezva | Čas (ms) |
|---|---|
| min | 0,634 |
| průměrná | 0,765 |
| max | 4,035 |

**Při maximálním vytížení**

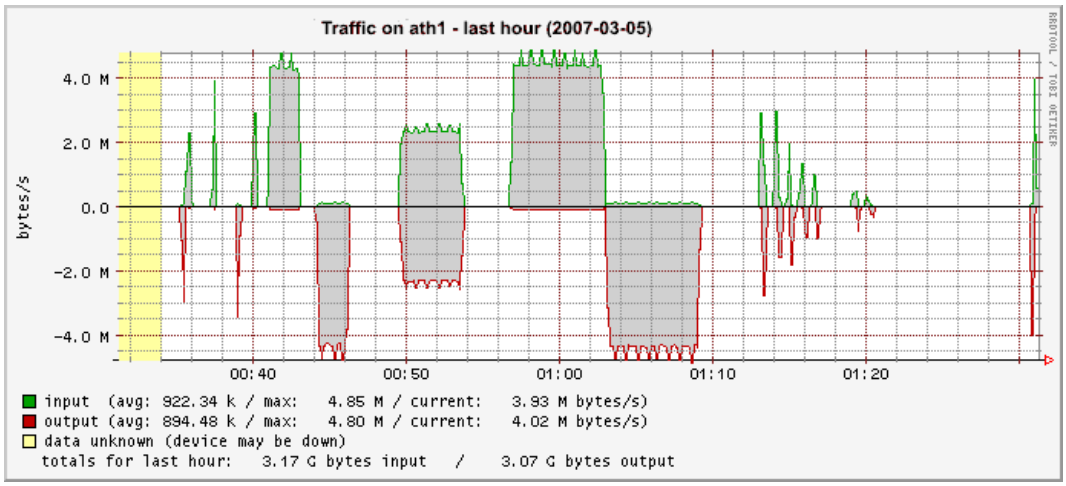
| Odezva | Čas (ms) |
|---|---|
| min | 0,892 |
| průměrná | 1,023 |
| max | 5,048 |

*Tab. 10: Výsledky testů měření*




*Graf 6. Srovnání délky odezvy*

Reálná přenosová rychlost v mém případě se pohybovala kolem 10 MBit half-duplex. Test jsem provedl v odpoledních hodinách, kdy může v okolí působit nějaké rušení od ostatních přístrojů. Přikládám výstupní graf z měřícího AP.



### 5.6.3. Praktické otestování v pásmu 10Ghz

Jako třetí testovaný spoj, bylo zařízení pracující na frekvenci 10 GHz. K testování jsem použil jednotky AL10F s přenosovou rychlostí 155MBit. Testování jsem prováděl na trase dlouhé 2 km s dostatečně velkou Fresnelovou zónou. Velikost parabol je na obou stranách 60 cm. Při přípravě spoje jsem musel nejdříve použít výpočty, abych věděl jaké velikosti antén použít při rezervě na únik 20 dB. Naše jednotka měla prahovou citlivost -71 dBm. Testování jsem prováděl dvě. První bylo bez zatížení spoje a druhé bylo při plném zatížení. Vždy se jednalo o zjištění délky odezvy (ping) a maximální reálné propustné rychlosti.

Testovaný spoj se skládá z:

- 2x jednotka AL10F …. *obr. č. 16* viz Přílohy
- 2x směrová anténa 0,65m – 34 dB…. *obr. č. 6* viz Přílohy
- 30 m kabelu H1000 (s útlumem 0,6dB/m)
- 8x konektor N
- 2x bleskojistka

Vše je koncipováno tak, aby nebyl překročen povolený vysílací výkon, který je povolen ČTU.

Měření bylo prováděno na vzdálenost 1744 m … mapa na *obr. č. 8* viz Přílohy

Nejprve jsem si provedl výpočet, abych zvolil vhodnou velikost antén a následně vhodně nastavil základní jednotky podle přiložené dokumentace.

| Zisk parabol pro pásma 10,3 - 10,6 GHz | | | | |
|---|---|---|---|---|
| průměr Dp | 0,35 m | G = | 28 | dB |
| | 0,65 m | G = | 34 | dB |
| | 1,2 m | G = | 40 | dB |
| | 0,9 m | G = | 37 | dB |

| Výpočet rezervy na únik pro určitou délku skoku: | | |
|---|---|---|
| Výkon Pout | /dBm/ | 3 |
| Prahová citlivost přijímače Pinp | /dBm/ | -71 |
| Útlum na 1 km Ap | /dB/ | 112,8 |
| Útlum celé trasy Ac | /dB/ | 118,8 |
| Zisk konvertoru | /dB/ | 25 |
| Délka trasy d0 | /km/ | 2 |
| Zisk vysílací antény Gav | /dB/ | 34 |
| Zisk přijímací antény Gap | /dB/ | 34 |
| Rezerva na únik | /dB/ | 23,2 |
| Úroveň signálu za konvertorem | /dBm/ | -22,8406 |
| Pměř[dBμV] = PIF-RX[dBm] + 108,75. | /dBμV/ | 86,0794 |

| | | |
|---|---|---|
| útlum volného prostředí. | A0[dB] | 118,8406 |
| úroveň na výstupu přijímací antény, | Pin[dBm] = | -48,8406 |

| |
|---|
| KONSTANTY |
| PROMĚNNÉ |
| VÝPOČTY |

Minimální hodnota stanovená pro rezervu na únik je 20 dB, takže v případě větších atmosférických vlivů mám ještě rezervu.

Výsledky testů jsem opět zpracoval do tabulky a vytvořil z ní příslušný graf.

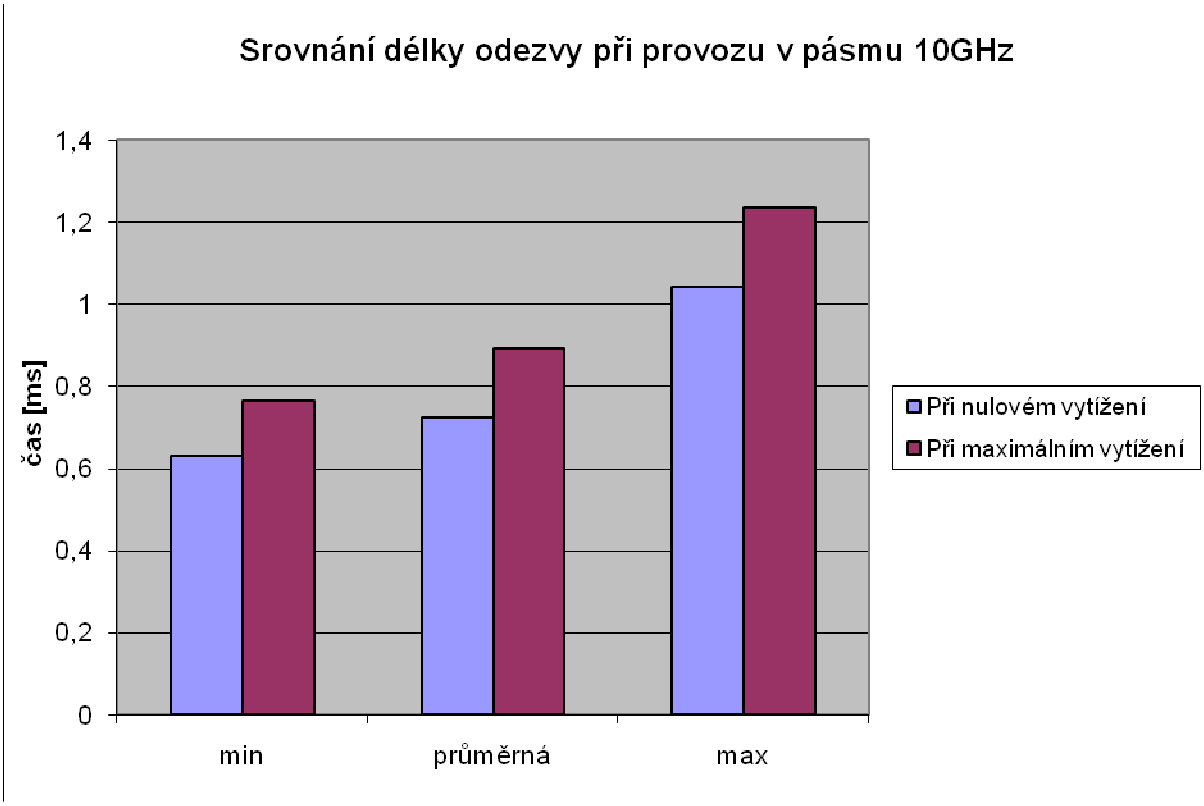
**Při nulovém vytížení**

| Odezva | Čas (ms) |
|---|---|
| min | 0,63 |
| průměrná | 0,722 |
| max | 1,042 |

**Při maximálním vytížení**

| Odezva | Čas (ms) |
|---|---|
| min | 0,765 |
| průměrná | 0,891 |
| max | 1,234 |

*Tab.11: Výsledky testů měření*




*Graf 7. Srovnání délky odezvy*

Testování reálné přenosové rychlosti jsem provedl pomocí utility iperf. Na jednom routeru jsem si pomocí příkazu *iperf –s* pustil server a z druhého routeru jsem prováděl měření. Propustnost spoje byla 148MBit.

# 6. Závěr

V dnešní době jsou bezdrátové sítě velmi významnou komunikační složkou, bez které bych si mnohá technická řešení ani neuměl představit. Dnes už dokonce ani v obyčejných domácnostech nejsou Wi-Fi sítě žádným překvapením.

Je pravdou, že volné frekvenční pásmo 2.4 GHz, ještě před uvolněním frekvenčního kmitočtového pásma 5 GHz, čemuž se stalo v září roku 2005, nešlo v některých oblastech z důvodu velkého zarušení používat.

Bezdrátové sítě se začaly používat nejen pro komerční využití. V mnoha městech například vznikla sdružení, založená určitou skupinou obyvatel, jež začala ve svých volných chvílích budovat malé sítě. Postupem času tyto spojili dohromady a vytvořili tak fungující metropolitní sítě. Mezi takovouto sortu obyvatel se řadím též já a spolu s dalšími, jsem postupně vybudoval dnes již kvalitně fungující metropolitní síť na Sokolovsku. V současné době ji využívá přibližně 1500 domácností, společností a organizací.

Bezdrátovou síť je ovšem nutné velmi dobře zabezpečit a zabránit tak přístupu nežádoucích "návštěvníků" - v opačném případě se můžeme dočkat řady nemilých problémů, z nichž je však pouhé zneužití internetového připojení tou nejmenší záležitostí. V mnoha případech se na toto bezpečnostní riziko opravdu zapomíná a lidé ho podceňují. Podle průzkumu je nejvíce nezabezpečených sítí v Praze. Zabezpečeno je 52% sítí z celkového počtu 876 přístupových bodů.

Dále je důležité zhodnotit kvalitu a přenosovou rychlost jednotlivých pásem. Spoje 5 GHz masivně nahrazují předešlé spoje postavené v kmitočtovém pásmu 2.4 GHz. Přenosová rychlost v pásmu 5 GHz je daleko větší než v pásmu 2.4 GHz. Někdo by mohl říci, že pokud použiji 802.11g (standard), mohl bych dosáhnout stejných přenosových rychlostí. To ano, ale v pásmu 2.4 GHz jsou pouze 3 kanály z celkového počtu 13, které se nepřekrývají, čímž samy sebe nezarušují. Vlivem zarušení přenosová rychlost rapidně klesá a zvyšuje se odezva až na několik desítek či stovek milisekund. Naproti tomu v pásmu 5 GHz nám zůstává odezva i při plném zatížení stejná. Pásmo 10 GHz bych použil tam, kde je opravdu velký požadavek na vysokou rychlost a stabilitu.

Cenové náklady jednotlivých spojů pro obě technologie v pásmu 2,4 GHz a 5 GHz jsou téměř totožné. Přestože jsou samotné bezdrátové jednotky pro pásmo 2.4 GHz o více než 1/3 levnější než pro pásmo 5 GHz, každý raději sáhne při budování nějakého páteřního spoje po zařízení pracujícím v pásmu 5GHz. Ceny 10 GHz spojů jsou 20x – 30x vyšší než u předchozích technologií spojů.

Na základě všech uvedených skutečností, ověřených již několikaletou praxí, bych v současné době doporučil všem tvůrcům bezdrátového připojení využít pro vybudování jakékoli nové metropolitní sítě pásmo 5 GHz.

# 7. Seznam použité literatury

**[1]** **Pužmanová, R.**: Širokopásmový internet. CPress, 2004

**[2]** **Pužmanová, R.**: Bezpečnost bezdrátové komunikace. CPress, 2005

**[3]** **Zandl, P.**: Bezdrátové sítě. CPress, 2003

**[4]** **Zandl, P.**: Bezdrátové sítě Wi-Fi – praktický průvodce. CPress, 2003

**[5]** **Šindelář, J**.: Bezpečnost Wi-Fi sítí v Praze je tragická (on-line). cit. 2008-10-12. Dostupné z < http://www.zive.cz/h/Uzivatel/AR.asp?ARI=126053>

**[6]** **Odvárka, P**.: Jaká je skutečná propustnost bezdrátových sítí (on-line). Cit. 2005-01-29. Dostupné z < http://www.svetsiti.cz/Tipy.asp?ClanekID=96>

**[7]** **Kefurt, P**.: Rozvoj Wi-Fi nabývá v Česku na tempu (on-line). Cit. 2009-03-10. Dostupné z < http://www.isdn.cz/clanek.php?cid=5129>

**[8]** **Řehák, J**.: Jak na ochranu a zabezpečení Wi-Fi sítí (on-line). Cit. 2009-03-14. Dostupné z < http://www.hw.cz/Produkty/Ethernet/ART918-Jak-na-ochranu-a-zabezpeceni-WiFi-siti.html>

**[9]** **Lampa**: Wi-Fi síť (on-line). Cit. 2009-02-21. Dostupné z < http://www.fit.vutbr.cz/CVT/net/wifi.html.cs>

**[10]** **Merunka, M**.: Novinky ze světa Wi-Fi a bezdrátového internetu. Cit. 2008-12-15. Dostupné z

< http://www.isdn.cz/clanek.php?cid=5891>

**[11]** **Hlavenka, J**.: Wi-Fi roaming: a začne to být opravdu zajímavé4 (on-line). Cit. 2004-07-28.Dostupné z < http://www.zive.cz/h/Byznys/AR.asp?ARI=117603>

**[12]** Generální licence VO-R/12/08.2005-34 vydaná ČTU

**[13]** Anonym: IEEE_802.11 (on-line). Cit. 2009-02-21. Dostupné z < http://cs.wikipedia.org/wiki/IEEE_802.11>

**[14]** Anonym: Fresnelova zóna. Cit. 2009-01-10. Dostupné z < http://www.zcomax.cz/Fresnelova_zona.aspx>

**[15]** Anonym: Výpočet parametrů bezdrátového spoje (on-line). Cit. 2008-01-10. Dostupné z < http://www.zcomax.cz/Vypocetwifispoje.aspx>

**[16]** ATHEROS (online) Cit. 2009-02-10. Dostupné z <http://www.atheros.com/>

**[17]** Petr Šimandl (online) Cit. 2008-12-10. Dostupné z <http://www.simandl.cz/>

**[18]** RETE internet s.r.o. (online) Cit. 2009-03-10. Dostupné z <http://www.rete.cz/>

**[19]** Vanco s.r.o. (online) Cit. 2009-02-11. Dostupné z <http://www.wifishop.cz/>

**[20]** Compex (online) Cit. 2008-02-10. Dostupné z <http://www.cpx.cz/>

**[21]** Mikroservis (online) Cit. 2009-02-10. Dostupné z <http://www.mikroservis.cz/>

**[22]** Abclinuxu (online) Cit. 2008-12-26. Dostupné z <http://www.abclinuxu.cz/>

**[23]** ROOT.CZ (online) Cit. 2008-11-23. Dostupné z <http://www.root.cz/>

**[24]** Jirous (online) Cit. 2008-12-10. Dostupné z <http://www.jirous.com/>

**[25]** Alcoma (online) Cit. 2009-01-13. Dostupné z <http://www.alcoma.cz/>

**[26]** Konwes (online) Cit. 2009-01-12. Dostupné z <http://www.konwes.cz/>

**[27]** Wikipedia (online) Cit. 2009-01-13. Dostupné z <http://www.wikipedia.cz/>

**[28]** **Michal Peterka:** Fenomén bezdrátových sítí v Česku aneb éra 10GHz spojů! (online) Cit. 2009-01-13. Dostupné z <www.internetprovsechny.cz/clanek.php?cid=198>

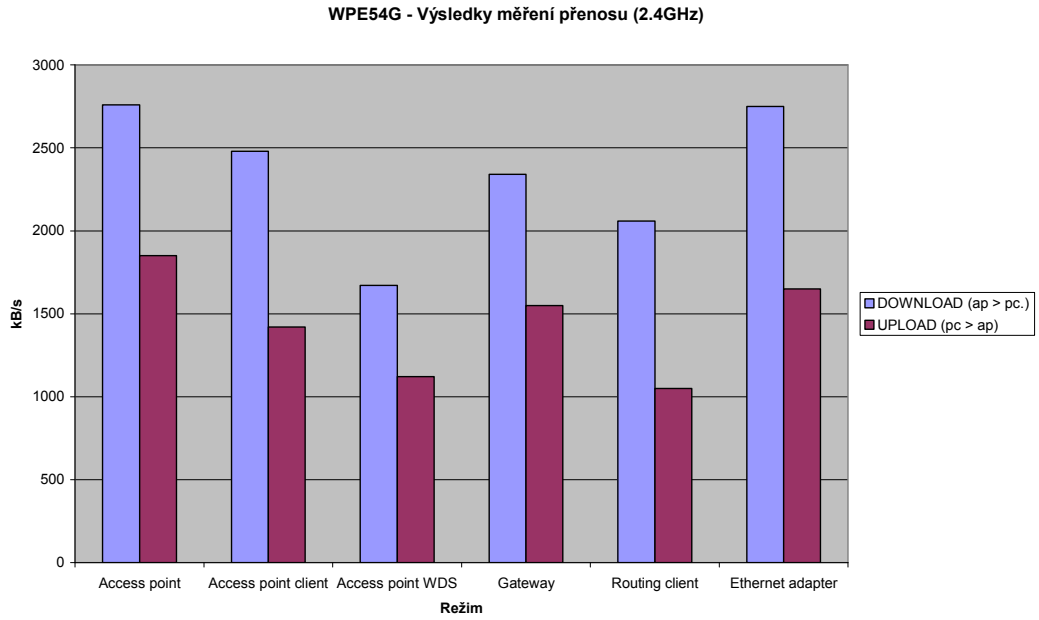
Seznam obrázků:



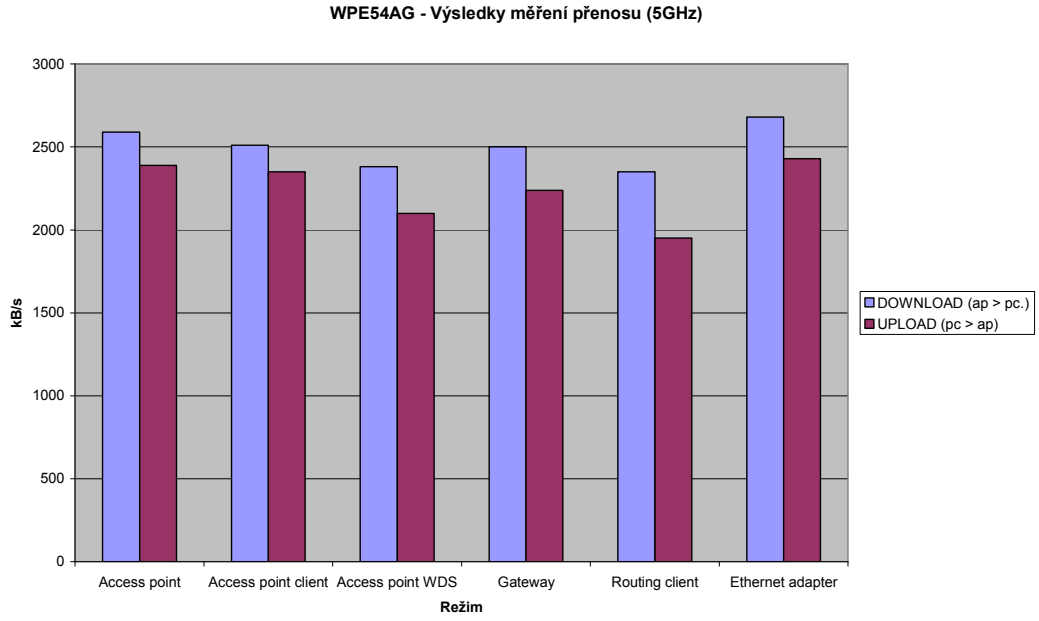
Seznam tabulek:

Seznam grafů:

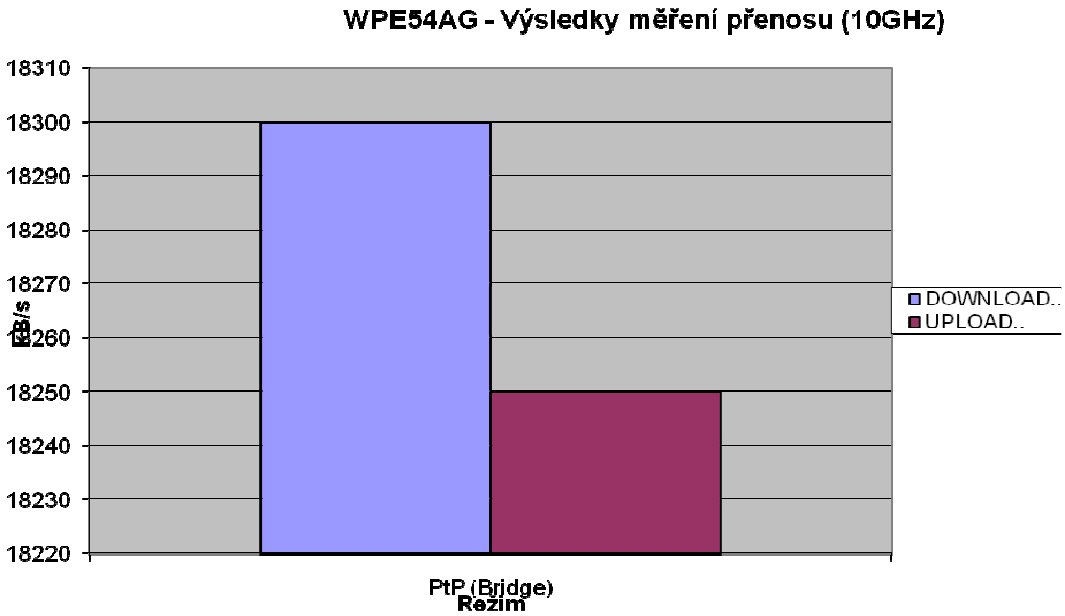
# 8. Přílohy




Graf 1: WPE54G - Výsledky měření přenosu (2.4 GHz)



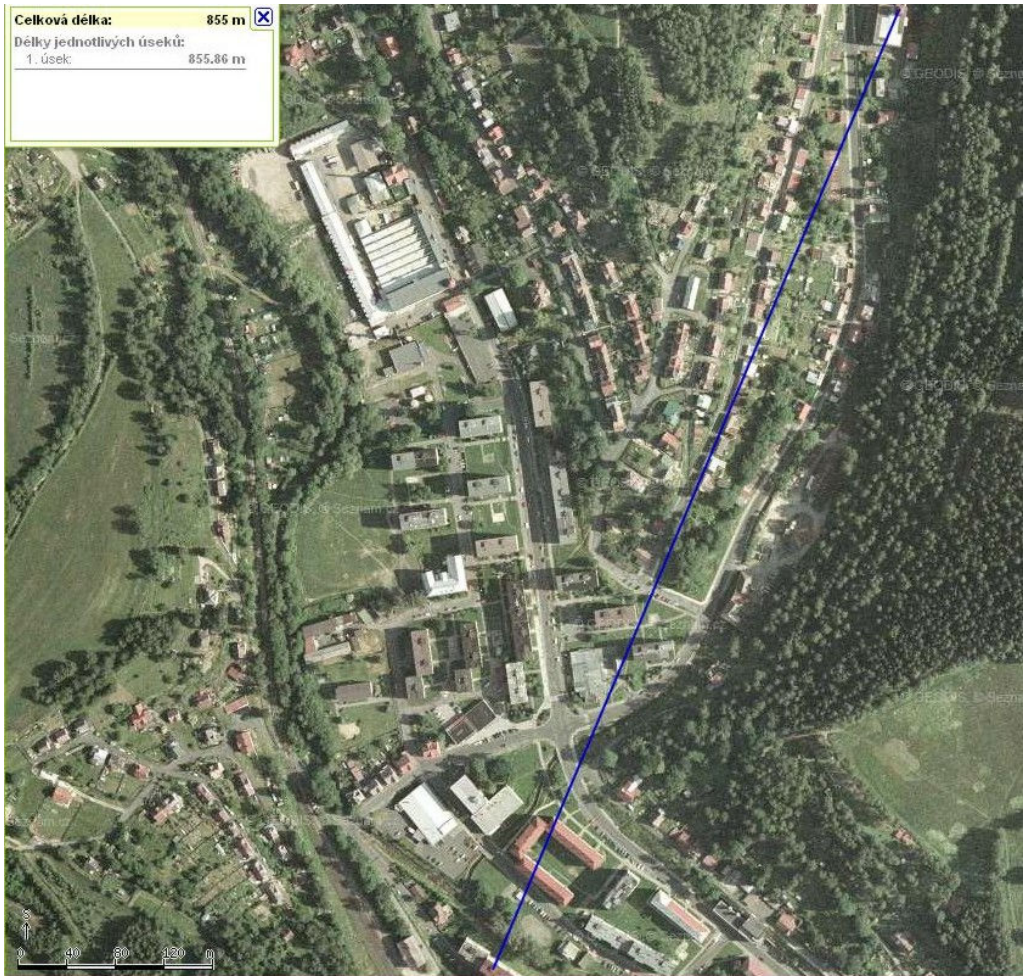

Graf. 2: WPE54G - Výsledky měření přenosu (5 GHz)




Graf. 3: AL10F - Výsledky měření přenosu (10 GHz)

Obr. 2: Bezdrátová karta Z-COM 626 [19]

Obr. 10: Směrová anténa Andrew 18 dBi [19]




Obr. 11: Mapa umístění testovaného spoje 2.4GHz

Obr. 12: Bezdrátové zařízení WRAP 2E [19]

Obr. 13: Bezdrátová karta CM9 [19]

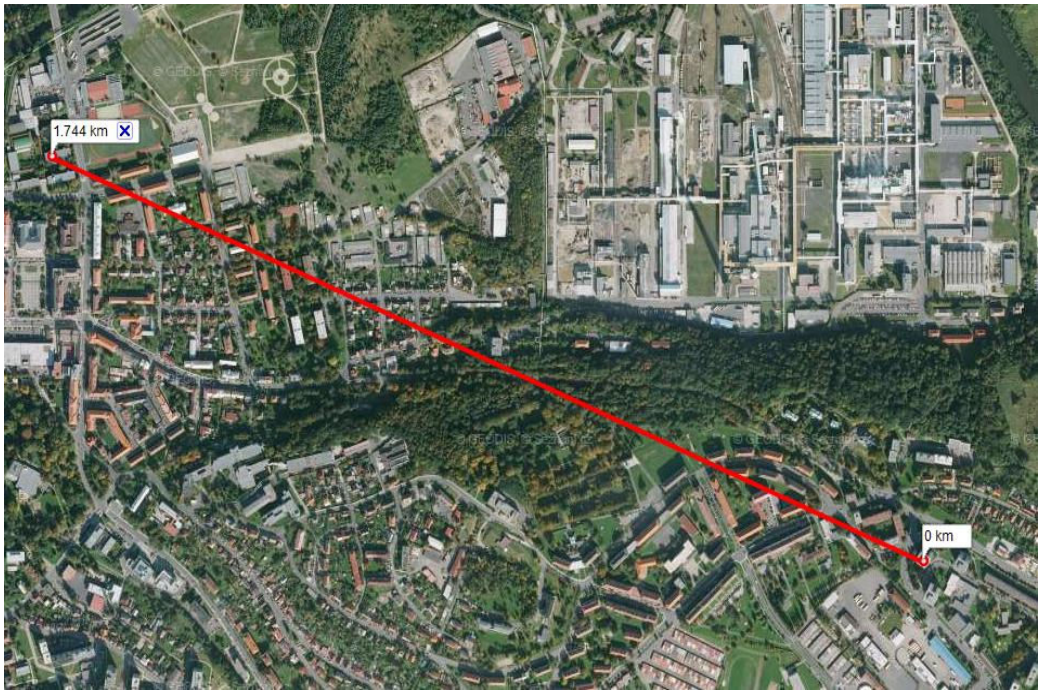
Obr. 14: Směrová anténa JRC-24 dBi [24]


Obr. 15: Mapa umístění testovaného spoje 5 GHz

Obr. 16: Jednotka ALCOMA AL10F [25]


Obr. 17: Parabola 34 dB ALCOMA AL10F


Obr. 18: Venkovní jednotka ALCOMA AL10F




Obr. 19: Mapa umístění testovaného spoje 10 GHz