Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Analýza zpoždění bezdrátové komunikace a jeho závislosti na velikosti dat

Miloš Samek

Bakalářská práce
2016

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Miloš Samek**
Osobní číslo:	**I13217**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza zpoždění bezdrátové komunikace a jeho závislosti na velikosti dat**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je provést analýzu vzniku latence a jeho závislosti na velikosti zasílaných dat. Autor v teoretické části práce vysvětlí principy bezdrátové komunikace s důrazem na Fresnelovi zóny, polarizaci, specifikaci využitelného hardware a používaných protokolů. V praktické části se autor bude věnovat statistickému zpracování naměřených dat získaných z měření na prvcích Mikrotik. Na základě naměřených dat autor provede analýzu vzniku a velikosti latence při komunikaci v závislosti na přenášeném obejmu dat a počtu prvků zapojených do komunikace.

Rozsah grafických prací:

Rozsah pracovní zprávy: **50**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Vyd. 1. Brno: Computer Press, 2011, 478 s. Samostudium. ISBN 978-80-251-2884-8.

GAST, Matthew. 802.11 wireless networks: the definitive guide. 2nd ed. Farnham: O'Reilly, 2005, xxi, 630 p. ISBN 0596100523.

GEIER, Jim. Designing and deploying 802.11 wireless networks: a practical guide to implementing 802.11n and 802.11ac wireless networks for enterprise-based applications. 2nd edition. Indianapolis, IN: Cisco Press, 2015, pages cm. ISBN 9781587144301.

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2015**
Termín odevzdání bakalářské práce: **13. května 2016**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2016

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 11. 5. 2016

Miloš Samek

Poděkování

Tímto bych rád poděkoval Mgr. Josefu Horálkovi Ph.D. za poskytnutí cenných rad a připomínek v průběhu vypracování této práce. Také bych chtěl poděkovat svým rodičům za podporu, kterou mi během mého studia věnovali.

ANOTACE

Tato práce se zabývá analýzou vzniku a velikosti latence v bezdrátové komunikaci. V teoretické části jsou popsány základní principy bezdrátových sítí, druhy standardů. Dále je představena Fresnelova zóna a polarizace. V praktické časti práce je provedeno měření na fyzických zařízeních pro zjištění, do jaké úrovně je latence závislá na velikosti odesílaných dat a počtů zařízení v síti.

KLÍČOVÁ SLOVA

IEEE 802.11, WLAN, latence, bezdrátové sítě, měření latence

TITLE

Analysis of latency in wireless communication and dependency on data size

ANNOTATION

This thesis deals with the analysis of formation and size of latency at wireless communication. In the theoretical part, basic principles of wireless networks and kinds of standards are described. Furthermore, the Fresnel zone and polarization is presented. In the practical part, there will be conducted a measurement of physical devices to detect to what level is the latency dependent on the size of send data and number of devices in the network.

KEYWORDS

IEEE 802.11, WLAN, latency, wireless network, Wi-Fi

OBSAH

SEZNAM TABULEK A ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

AP	Access Point
ARQ	Automatic Repeat-reQuest
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRS	Dynamic Routing System
ETSI	European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IFS	Interframe Spacing
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet service provider
LLC	Logical Link Control
MAC	Media Access Control
MIMO	Multiple-input multiple-output
NAT	Network Address Translation
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PLF	Polarization Loss Factor
QoS	Quality of Service
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol

VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

ÚVOD

Wi-Fi technologie je určená pro bezdrátový přenos dat lokální sítě, je přímo kompatibilní s ethernetem a řeší přenos dat pomocí ethernetových rámců vzduchem. Technologii bezdrátových sítí popisuje rodina norem IEEE 802.11. Normu popisují různé označení na konci za označením normy. Tyto písmena řeší různé dílčí oblasti, nebo popisují různé varianty modulace bezdrátové technologie. Původní účel technologie Wi-Fi bylo rozvést lokální síť v místnosti, nebo budově bez použití kabelů. Následně tento účel byl rozšířen také do exteriéru.

Cílem bakalářské práce je zjištění vzniku a velikosti latence při komunikaci v závislosti na přenášeném objemu dat a počtu prvků zapojených do komunikace. Aby byly splněny cíle, je bakalářská práce rozdělena na dvě stěžejní části a to teoretickou a praktickou.

V teoretické části bakalářské práce budou ukázány principy, stavební kameny a protokoly bezdrátových sítí. V první kapitole budou představeny principy bezdrátových sítí a standardy bezdrátové komunikace. V následující kapitole budou představeny Fresnelovy zóny a polarizace, které slouží ke správnému určení tvaru, či velikosti bezdrátové sítě. Ve třetí kapitole bude představen ISO/OSI model a jednotka pro přenos dat, takzvaný rámec. V posledních dvou kapitolách teoretické části bakalářské práce bude popsán využívaný hardware v bezdrátových sítích, zprvu bude popsán obecně a poté konkrétně od litevské společnosti MikroTik.

V praktické části bakalářské práce se budeme věnovat statistickému zpracování naměřených dat pro analýzu zpoždění bezdrátové komunikace. Komunikaci budeme měřit na síťových prvcích Mikrotik. Na základě naměřených dat bude provedena analýza vzniku a velikosti latence při komunikaci v závislosti na přenášeném objemu dat a počtu prvků zapojených do komunikace.

1 REŠERŠE

Tato kapitola se snaží popsat a shrnout obsah teoretické části bakalářské práce na téma Analýza zpoždění bezdrátové komunikace a jeho závislosti na velikosti dat. Většina základních termínů a postupu analýzy zpoždění bezdrátové komunikace bude popsána v následujících kapitolách.

V bezdrátových sítích je používáno velké spektrum různých prvků, stavebních kamenů, operačních systému apod. je dobré, mít přehled používané terminologie (Goggi, 2014). Pokud máme začít od úplného začátku tak stavební kámen bezdrátových (802.11) sítí jsou přístupové body neboli Access pointy. Architektura bezdrátových sítí na zařízení od firmy Cisco byla popsána například Brandonem James Carrollem (Carroll, 2011).

Bezdrátové sítě jsou tu relativně krátkou dobu, ale Francouzský fyzik Augustin Jean Fresnel narozen v roce 1788 přinesl téma polarizace již v 18. Století. Zachovat jen přímou viditelnost totiž není vždy pro účinné spojení dostačující. Pokud vezmeme příklad dvou antén, které propojuje spojnice, zjistíme, že v ideálních podmínkách musí být kolem této spojnice volný prostor, který vymezují takzvané Fresnelovy zóny. Zjednodušeně řečeno tyto zóny mají tvar podobný doutníku nebo ragbyovému míči. Vymezují oblast, ve které je přenášena většina signálu, pokud se v této oblasti nachází jakákoliv překážka, dochází k útlumu přenosu. Základní principy a vzorce jsou popsány ve výukovém materiálu z Vysoké školy Báňské (Vysoká škola Baňská, 2014).

Mezinárodní neziskový institut Institute of Electrical and Electronics Engineers funguje již od roku 1963. Tato organizace usiluje o vzestup technologie související s elektrotechnikou. My budeme rozebírat převážně jejich standard 802.11, který byl původně vydán již v roce 1997. Přehled a základní vlastnosti některých vybraných protokolů popisuje Brandon James Caroll (Carroll, 2011). Podrobněji jsou všechny standardy popsány právě institutem IEEE (IEEE Computer Society, 2012). Se standardy také přichází nové druhy zabezpečení bezdrátových sítí, které budou v následujících kapitolách.

Protože rámce pracují na druhé vrstvě ISO/OSI modelu, bylo by vhodné si nejprve představit právě ISO/OSI model. ISO/OSI model je referenční model, který byl vypracován se snahou standardizace počítačových sítí. Tento model obsahuje základních 7 vrstev od fyzické až po aplikační vrstvu. Definován a popsán byl například firmou Microsoft v roce 2014 (Microsoft, 2014). My se ale převážně budeme zajímat právě o první dvě vrstvy ISO/OSI modelu

takzvané fyzické a linkové vrstvě. Linková vrstva uspořádává data z fyzické vrstvy logických celků, již zmíněných rámců (Kozierok, 2005).

V bezdrátových sítích se vyskytují 3 základní typy rámců (Rámce pro správu, řídící a datové), jejichž základní strukturu popisuje například Matthew Gast (Gast, 2002). Víme že, bezdrátové sítě běží v režimu poloviční duplexu, pokud by současně vysílalo více než jednou zařízení, dojde ke kolizi. Analýzu pravděpodobnosti kolize zmiňují ve výukových materiálech Fakulty Českého vysokého učení technického (České vysoké učení technické v Praze, 2008).

V praktické části práce, bude zkoumána analýza zpoždění bezdrátové komunikace. Prvky, které budou využívané pro znázornění, jsou právě od firmy Mikrotik. Firma byla založena v roce 1995 se záměrem vývoje a prodeje bezdrátových systémů. Základní konfiguraci a příkazy pro Mikrotik RouterOS poskytují na jejich webové prezentaci (Mikrotik, 2011).

2 ZÁKLADNÍ PRINCIPY A POJMY 802.11 SÍTI A STANDARDY

V této kapitole budou představeny parametry bezdrátových sítí. Bude popsán signál a jeho úrovně. Taktéž bude rozebrán výkon sítě a přehledem specifikací nejpoužívanějších standardů.

2.1 PARAMETRY POČÍTAČOVÝCH SÍTÍ

Mezi ideální a reálnou sítí existuje mnoho technických rozdílů, které tyto sítě rozlišují. V ideální síti jsou všechna spojení realizované metodou point-to-point, přenosová rychlost je neomezená a neexistuje žádná latence, žádné chyby. Reálná síť se ale chová podstatně jinak a z toho důvodu si v následující podkapitole představíme parametry počítačových síti.

Propustnost je veličina, která říká, jaké množství dat je možné sítí přenést za jednotku času. V reálném provozu sítě se propustnost může měnit a síť musí na tyto změny reagovat. Cílem směrování je obvykle doručení paketů co nejrychleji na místo určení a právě propustnost je důležitou vlastností směrování. Udává se běžně v Mbps a v bezdrátových sítích je běžná propustnost 54 Mbps.

Chybovost či spolehlivost, nám označuje jaká je vzdálenost (v objemu či čase) mezi dvěma porušenými pakety. V reálné sítí nikdy nedosáhneme nulové chybovosti, z důvodů existence šumu, výpadku či chyb.

Rozptyl udává rozdíl mezi maximální a minimální odezvou na požadavek. Pokud chceme dosáhnout optimálního využití sítě, je potřeba rozptyl neustále sledovat a hlídat.

Route, neboli cesta označuje použitou cestu zapsanou v routovací tabulce. Vypočítává se pomocí adresy směrovače, přes které se paket dostal od vysílače až do cílové stanice.

Vytíženost linky udává, jaká část z maximální kapacity linky je využita. Existují 3 různé druhy vytíženosti aktuální, špičková a průměrná hodnota. U lokálních sítí se pravidelně přibližujeme k 100% vytíženosti, ale u páteřních sítí je kritická úroveň již pokud vytíženost dosahuje 80%. Pokud je vytíženost větší, je potřeba hledat nové možnosti pro směrování nebo se musí zvýšit kapacita linky.

Šířka pásma je pojem, který má několik souvisejících významů. Ze strany digitální komunikace rozumíme šířce pásma jako množství dat, která mohou být přenesena za jednotku času. Šířka pásma, taktéž může udávat propustnost, která se vyjadřuje pomocí dostupné šířky pásma nebo kapacity.

Parametry signálu obsahují intenzitu pole, vstupní úrovně užitečných a nežádoucího signálu, poté jejich úrovně ve vývodkách, úrovně šumu a interference způsobené přijímači. Aktuální impedance jednotlivých součásti vybavení, či parametry zesilovačů, společně se spolehlivostí komponent a mnoho dalších parametrů. Celkově tohle vše ovlivňuje kvalitu anténního systému.

Na závěr podkapitoly, si představíme pojem latence, která bude zkoumána v praktické části bakalářské práce.

Zpoždění neboli latence, je potřebná doba odeslání zprávy, nebo paketu z místa odeslání do cílového místa. Toto je jednoduchá a užitečná definice, ale skrývá mnoho užitečných informací. Každá síť, či systém obsahuje různé zdroje nebo komponenty, které zvyšují celkový čas potřebný ke zpracování zprávy (Vaňková, 2012).

Celková latence mezi klientem a serverem se skládá z následujících zpoždění:

- **Propagation delay** je potřebná doba pro doručení zprávy od odesílatele k příjemci, která je funkcí vzdáleností nad rychlostí, s níž se signál šíří.
- **Transmission delay** je množství času, ve kterém je nutné přenést všechny bity paketu do spojení, které je závislé na velikosti paketu a propustnosti spojení
- **Processing delay** je množství času potřebné ke zpracování hlavičky paketu, zkontrolování bitových chyb a určení cíle cesty paketu.
- **Queing delay** je doba, po kterou příchozí paket čeká ve frontě, dokud není zpracováván

Doba šíření je dána vzdáleností a prostředkem, jehož prostřednictvím je signál šířen. Obvykle je rychlost šíření rovna rychlosti světla. Na druhou stranu, přenosové zpoždění (Transmission delay) je dán k možnostem dostupné přenosové rychlosti vysílající linky a nemá nic společného se vzdáleností mezí klientem a serverem (Grigorik, 2013).

2.2 STANDARDY

V bezdrátových sítích se využívá větší počet standardů. Konkrétně v oblasti bezdrátových sítí vytvořila organizace IEEE různé protokoly z kategorie 802.11. Každý z těchto standardů popisuje jiné modulační schéma a jinou šířku pásma, se kterou pracuje. Všechny standardy však sdílí koncept kanálů, který odděluje jednu sadu spojení od ostatních. Původní překonaný protokol 802.11 taktéž nazývaný „legacy mode“, nalezneme v současnosti jen zřídka. Byl založen na technologii FHSS a z toho důvodu jeho přenosová rychlost dosahuje pouze 1 Mb/s a 2 Mb/s (Malířová, 2014).

Protokol 802.11a byl schválen v roce 1999. Vysílá radiový signál ve spektru 5GHz a používá modulaci OFDM. Z hlediska interferencí je to výrazné zlepšení z důvodu toho, že na této frekvenci nepracuje tolik zařízení. Není kompatibilní s protokoly 802.11 / b / g, ale zároveň není rušen těmito zařízeními, spolu s mikrovlnnými troubami, či bluetooth přenosem. Umožňuje přenášet data do rychlosti 54 Mb/s. V dnešní době není nasazován tak často, například z důvodů toho, že obsahuje neodpovídající zabezpečení přenosu QoS (Quality of Service). QoS slouží k přidělování datového pásma v technologiích VoIP nebo HTTP (IEEE Computer Society, 2012).

Protokol 802.11b představuje doplněk protokolu 802.11. Musíme si uvědomit, že technologie se mění rychleji než standardy. Z toho důvodu protokol 802.11 rychle zastaral, protože kabelové sítě nabídly rychlost až 10 Mb/s oproti 2 Mb/s. Protokol poskytuje přenosové rychlosti až do 11 Mb/s a k tomu podporuje zpětnou kompatibilitu k rychlostem 1 Mb/s a 2 Mb/s. K dispozici má v Evropě 13 kanálu, které definuje organizace ETSI. Umožňuje, aby klienti metodou DRS (dynamic rate shifting) snižovali přenosové rychlosti při rostoucí vzdálenosti a při zvyšovali, pokud přijdou blíže. Je to jeden z nejčastěji implementovaných standardů (IEEE Computer Society, 2012).

Protokol 802.11g byl ratifikován v roce 2003, kde ke stávajícím čtyřem přenosovým rychlostem od protokolů 802.11 a 802.11b přibylo 8 dalších. Protokol se díky přenosové rychlosti dat, která činí 54 Mb/s dostává na stejnou rychlostní úroveň jako 802.11a, nýbrž zůstává ve frekvenčním rozsahu 2,4 Ghz. V nižších přenosových rychlostech je protokol nadále kompatibilní se standardem 802.11b a používá stejné kódování i modulaci. K dosažení vyšších rychlostí protokol používá metodu OFDM (orthogonal frequency division multiplexing), stejně jako standard 802.11a. Můžeme o něm tvrdit, že se jedná o nejrozšířenější protokol bezdrátových sítí (IEEE Computer Society, 2012).

Protokol 802.11n je nejnovějším protokolem sady standardů IEEE. Jeho největším přínosem je, že ve výhradním použití v síti lze získat přenosovou rychlost až 300 Mb/s. V dokumentaci bývá uváděné, že dosahuje přenosové rychlostí okolo 100 Mb/s. Nižší přenosová rychlost je způsobena využíváním různých protokolů v jedné síti. Zpětná kompatibilita do standardů b/g/a je dána použitím více antén a technologie MIMO (Multiple-Input, Multiple-Output). Technologie MIMO je abstraktní matematický model pro multi-anténní komunikační systémy (EPRIN spol. s r.o., 2015). Umožňuje odesílat a přijímat pomocí více antén, což zvyšuje propustnost a dovoluje dosáhnout lepšího duplexního provozu (EPRIN spol. s r.o., 2015).

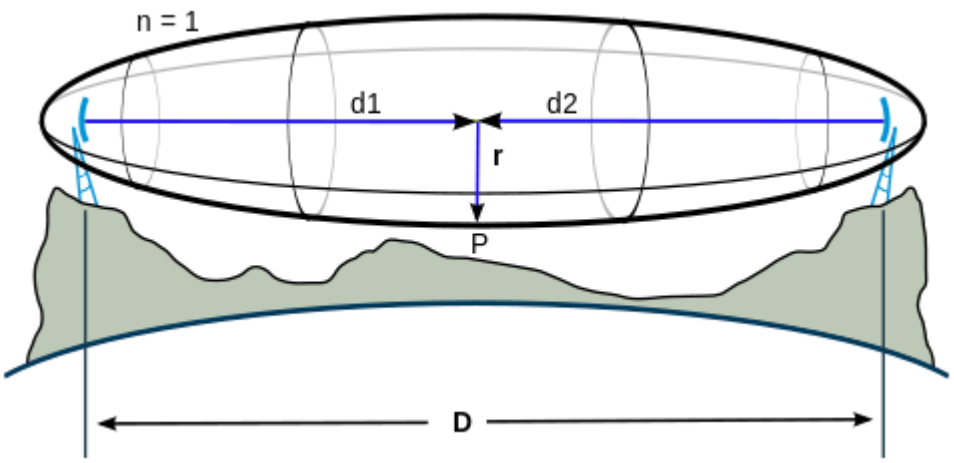
Toto byl pouze přehled nejdůležitějších protokolů od firmy IEEE, existuje spousta literatury či webových zdrojů, která dopodrobna popisuje funkčnost, informace či výhody různých protokolů (Sosinsky, 2010).

3 FRESNELOVY ZÓNY A POLARIZACE

S rozvojem radiokomunikace se objevily problémy na přenosových vlnách signálu, které se na nižších kmitočtových pásmech prakticky nevyskytovaly. K řešení problému šíření vln přispěla teorie od francouzského fyzika A. J. Fresnela. Fresnelovy zóny a jeho elipsy v šíření signálu si rozebereme v následující podkapitole.

3.1 FRESNELOVY ZÓNY

Zachovat přímou viditelnost mezi dvěma anténami, ve všech případech nemusí být dostačující. Představme si dva body, kterou spojuje spojnice. Kolem myšlené spojnice musí být volný prostor, který ohraničují takzvané Fresnelovy zóny. Pro lepší představu si můžeme představit tuto zónu jako elipsu, která je na obrázku č. 1. Tato elipsa vymezuje oblast, ve které se přenáší většina výkonu.



Obrázek 1 – Fresnelova zóna, zdroj: (Kohanbash, 2014)

Fresnelovy zóny se dělí do 3 různých úrovní. O první Fresnelově zóně je známo, že musí alespoň 60% zóny být prázdné, bez objektů. Každá překážka v této oblasti způsobuje útlum přenosu, rušivé odrazy a snižuje se kvalita přenosu dat (ztráta paketů, nižší rychlost). Čím více rušení, tím kvalitnější antény či kabely musí být použity. Nejmenší přípustnou vzdálenost překážky od přímé spojnice komunikujících zařízení lze určit podle vztahu

$$r_1 = \sqrt{\frac{\lambda d_1 d_2}{D}}$$

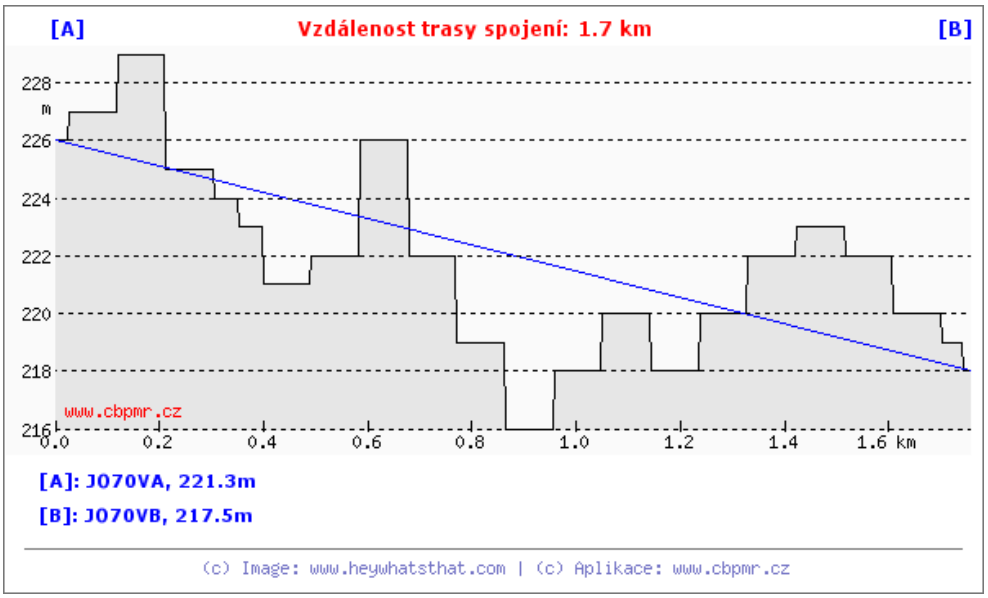
kde r_1 značí poloměr Fresnelovy zóny, λ je vlnová délka, d_1 a d_2 jsou vzdálenosti překážky od přijímače či vysílače, poslední označení je D a to značí vzdálenost mezi přijímačem a vysílačem (Vysoká škola Baňská, 2014).

K výpočtu poloměru volných Fresnelových zón jsou k dispozici různé kalkulátory na internetových stránkách, které nahradily starší grafické pomůcky (např. spojnicový nomogram pro určení 1. Fresnelovy zóny). Ke kalkulátorům jsou obvykle připojeny další funkce například útlum tras směrových spojů, radiovou dohlednost popřípadě energetickou bilanci celého spoje. Problémem většiny těchto kalkulátorů je, že řeší pouze 2D prostor a k zastínění zóny může dojít i mimo 2D prostor (crk.cz). Pro lepší představu, pokud známe vzdálenost mezi komunikačními body, můžeme určit, jaký největší průměr může dosahovat Fresnelova zóna (Macoun, 2014). Základní přehled maximálních průměrů první Fresnelovy zóny v pásmu 2,4 a 5Ghz v následující Tabulce č. 1.

Tabulka 1- Maximální průměr první Fresnelovy zóny podle vzdálenosti a frekvence.

Vzdálenost	**Pásmo 2,4Ghz**	**Pásmo 5Ghz**
100m	1,37m	1,22m
200m	1,93m	1,73m
300m	2,37m	2,12m
400m	2,73m	2,44m
500m	3,06m	2,73m
700m	3,62m	3,23m
1000m	4,32m	3,87m
1200m	4,73m	4,23m
1500m	5,29m	4,73m
2000m	6,11m	5,47m

Při výpočtu Fresnelových zón je důležité znát reálný terénní profil mezi anténami. Dříve k jeho sestavení bylo využíváno topografických map s hustou sítí vrstevnic, které umožnily odečet výškopisu podél uvažované oblasti. Dnes v době digitalizace, jsou dostupné počítačové programy, které vypočtou a znázorní přesný profil zadané oblasti. Na internetových stránkách českého radioklubu doporučují výškopis (obr. 2) od společnosti cbpmr (citizen band – personal mobile radio), který je využíván jako nástroj pro ověřování viditelnosti mezi různými stanovišti radiostanic.



Obrázek 2 – Výškopis trasy mezi kolejemi a fakultou

Na obrázku znázorňuji trasu mezi fakultou Elektrotechniky Pardubice (bod A) a kolejemi A (bod B), které jsou v hlavním kampusu Univerzity Pardubice.

3.2 HORIZONTÁLNÍ A VERTIKÁLNÍ POLARIZACE

Polarizace, taktéž nazývaná vlnová polarizace, je orientace vektoru elektrického pole prostorem se šířícího elektromagnetického záření. Polarizace je obvykle popisována pomocí polarizační elipsy, zejména podle excentricity a její hlavní poloosy. Běžně se popisuje pomocí úhlu mezi osou x a hlavní poloosou.

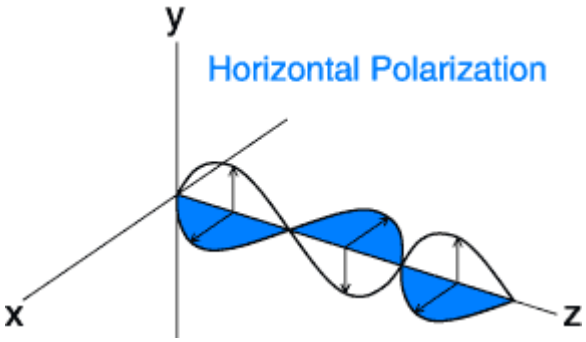
Při šíření vlny ve volném prostředí může existovat polarizace **lineární**, do které patří horizontální a vertikální polarizace nebo **eliptická polarizace**. Vlna je lineárně polarizovaná, když vektor E má během celé periody stále stejný směr. Pokud si představíme vektor okamžité hodnoty, pak se její délka mění během půlperiody od nuly do maxima a zpět, během druhé půl periody se opakuje totéž s opačnou orientací.

Elipticky polarizovaná vlna, která je využívána v kruhových anténách mění svůj vektor intenzity elektrického pole po dobu celé periody. Šipka, znázorňující okamžitou hodnotu intenzity pole se během periody otáčí a současně mění svou délku tak, že její koncový bod se pohybuje po elipse. Existuje i možnost, že koncový bod se pohybuje po kružnici (kruhová polarizace). Eliptická (kruhová) polarizace může být pravotočivá nebo levotočivá. Smysl otáčení se posuzuje při pohledu ve směru šíření. Elipticky polarizovanou vlnu lze považovat za superpozici dvou koherentních lineárně polarizovaných vln, jejichž vektory E kmitají v různých směrech a s určitým nenulovým vzájemným posuvem (Zbyněk Raida, 2010).

Polarizace ze strany bezdrátových sítí je důležitá z důvodu orientace antény.

Horizontální Antény

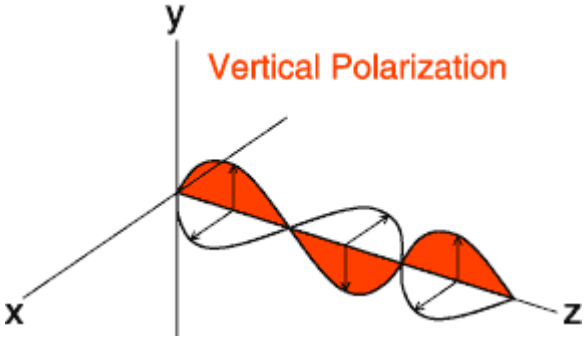
Horizontálně polarizované antény mají své elektrické pole paralelně k zemskému povrchu. Signál osciluje zleva doprava. Protože země se chová jako dobrý vodič při nízkých frekvencích, tak některé frekvence jsou zkracovány. Znázornění horizontální polarizace na obrázku č. 3.



Obrázek 3 – Horizontální polarizace, zdroj: (Service, 2012)

Vertikální antény

Vertikálně polarizované antény mají své elektrické pole kolmé k zemskému povrchu. Signály oscilují od shora dolu. Průběh signálu je ukázán na obrázku č. 4. Signály jsou přenášeny ve všech směrech, a proto se vertikální polarizace používá pro přenos „ground-wave“ vln. Z tohoto důvodu je možné posílat rádiové vlny na značnou vzdálenost podél povrchu země s minimálním útlumem.



Obrázek 4 – Vertikální polarizace, zdroj: (Service, 2012)

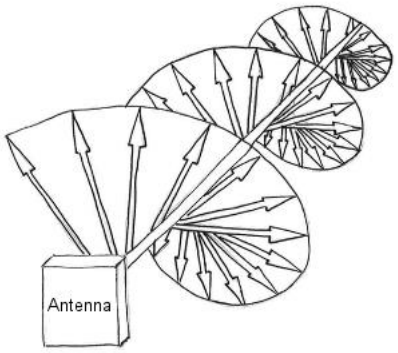
Pokud antény v bezdrátových sítích nejsou orientovaný stejnou polarizaci, dochází ke ztrátě výkonu. Neshoda polarizace je definována „Polarization Loss Factorem“ (Bevelacqua, 2009).

$$PLF = cos^2\phi$$

Kruhové antény

Kruhově polarizované antény (obr. 5) vyzařují elektromagnetické pole v podobě vývrtky. Z technického hlediska kruhové antény vysílají elektromagnetické vlny ve dvou rovinách tvořících jednu periodu v jedné vlnové délce.

Ve srovnání s lineárně polarizovanými anténami, kruhově polarizované antény ztrácí asi 3 dB síly, protože signál je rozdělen do dvou různých oddělených rovin (Armstrong, 2013).



Obrázek 5 – Eliptická polarizace, zdroj: (Bevelacqua, 2009)

4 RÁMCE A ISO/OSI MODEL

Jak už vyplívá z názvu kapitoly, budeme se zabývat teoretickým představením ISO/OSI modelu a rámců. Postupně si představíme základní informace o ISO/OSI modelu a poté přejdeme k rozebrání rámců. Na závěr OSI modelu si podrobněji představíme fyzickou vrstvu, na které dochází k fyzickému přenosu dat a linkovou vrstvu, která předává informace pomocí rámců.

4.1 ISO /OSI MODEL

OSI model, neboli Open Systems Interconnection Basic Reference Model, byl popsán již před více než 30 lety mezinárodní společností ISO. Společnost ISO je nezávislá, nevládní organizace, která spojuje více než 162 zemí světa. Prostřednictvím svých členů sdílí znalosti a snaží se vyvinout mezinárodní normy, které podporují inovace a poskytují řešení globálních výzev (International Organization for Standardization, 2016).

Jedná se o abstraktní popis síťové komunikace a protokolů používaných pro komunikaci v počítačové síti. Model byl rozdělen do sedmi vrstev, které komunikují pomocí zapouzdření – encapsulate na straně odesílatele a rozbalováním na straně příjemce (Malířová, 2014). Účelem referenčního modelu je standardizování komunikace pro různé výrobce hardwaru i softwaru.

Hlavní výhodou tohoto modelu je, že dochází ke standardizování komunikace, ale s výhodami taktéž přichází i nevýhody. Dvě základní nevýhody jsou, že i nevyužité vrstvy musí být obsaženy v komunikaci a vrstvy mohou komunikovat pouze přímo. Pokud vrstva číslo 5 chce předat informace vrstvě číslo 7, musí být v komunikaci zahrnuta i vrstva číslo 6. Tento postup vytváří zbytečné kroky a dochází ke zbytečné časové a datové náročnosti.

V tabulce č.2 je možné nalézt přehled jednotlivých vrstev modelu včetně jejich základních funkcí.

Tabulka 2 - Přehled vrstev ISO/OSI modelu zdroj: (Malířová, 2014)

Číslo vrstvy	Anglický název	Český název	Jednotka	Funkce	Služby
7	Application	Aplikační	data	Poskytnutí aplikacím přístup ke komunikačnímu systému z důvodu umožnění jejich spolupráce	FTP, SSH
6	Presentation	Prezentační	data	Transformace dat do podoby (tvaru), ve kterém je použitelná aplikacemi	Telnet, TLS
5	Session	Relační	data	Organizace a synchronizace dialogu mezi relačními vrstvami komunikujících systému.	NFS, NetBIOS
4	Transport	Transportní	segmenty	Přenos dat mezi koncovými uzly	TCP, UDP
3	Network	Síťová	pakety	Poskytuje spojení mezi systémy, které spolu přímo nesousedí.	ICMP, IPX
2	Data Link	Linková	rámce	Poskytuje spojení mezi dvěma sousedními systémy. Uspořádává data z fyzické vrstvy do rámců	PPP, Ethernet
1	Physical	Fyzická	bity	Specifikuje fyzickou komunikaci. Aktivuje, udržuje a deaktivuje fyzické spoje mezi koncovými systémy	Wi-Fi, ISDN, DSL, CAN bus

OSI model není jediný síťový model, který je možný využít. Taktéž existuje TCP/IP model, o kterém můžeme říci, že vychází z OSI modelu, ale upravuje jej, aby byl více flexibilní. Obvykle označení TCP/IP je chápáno jako označení dvou přenosových protokolů používaných v počítačové sítí. Ve skutečnosti TCP/IP seskupuje celou řadu protokolů. Na rozdíl od OSI modelu, který zajišťuje spolehlivost přenosů, TCP/IP protokol takovou spolehlivost nezajišťuje. Tvůrci předpokládají, že zajištění spolehlivosti je na straně koncových účastníků komunikace, tzn., mělo by být řešeno až na úrovní transportní vrstvy (Meyer, 1990).

Na rozdíl od ISO/OSI modelu, který mu 7 funkčních vrstev, Architektura TCP/IP je pouze čtyřvrstvá. V následující tabulce jsou tyto architektury porovnány.

Tabulka 3- Porovnání TCP/IP a OSI modelu, zdroj: (Malířová, 2014)

TCP/IP	OSI
Aplikační	Aplikační
	Prezentační
	Relační
Transportní	Transportní
Síťová	Síťová
Vrstva síťového rozhraní	Linková
	Fyzická

Nyní si představíme z pohledu TCP/IP protokolu vrstvu síťového rozhraní, která obsahuje fyzickou vrstvu a vrstvu linkovou. Další vrstvy si podrobněji popisovat nebudeme, protože pro účel této bakalářské práce nejsou potřebné.

4.1.1 FYZICKÁ VRSTVA

Fyzická vrstva, je nejnižší vrstva OSI modelu. O fyzické vrstvě, je možné říci, že se jedná o hardwarovou vrstvu, která jako jediná v referenčním modelu ISO/OSI podporuje fyzickou komunikaci dat mezi systémy. Někteří mohou vidět fyzickou vrstvu pouze jako síťové karty a kabely, to ale není pravda. Fyzická vrstva definuje počet síťových funkcí.

Hlavním úkolem této vrstvy je tedy zajištění bitového přenosu z jednoho zařízení na druhé prostřednictvím fyzického média, která tato vrstva bezprostředně ovládá.

Dokáže detekovat chybové stavy a tyto stavy oznamuje vyšší vrstvě OSI modelu (Linkové vrstvě). Fyzická vrstva dále zajišťuje kódování přenosu, kde dochází k upravování digitálního vzorku signálu (jedničky a nuly), tak aby odpovídal charakteristice konkrétního fyzického média a napomáhal synchronizaci bitů a rámců. Taktéž zajišťuje synchronizaci komunikací a časový multiplex. Fyzická vrstva definuje napěťovou úroveň, kterou bude v přenosu reprezentována logická jednička a logická nula. Dále specifikuje technické parametry kabelu, tvar konektoru kabelu, počet kontaktů a délku trvání jednoho bitu (Microsoft, 2014).

Pro znázornění na fyzické vrstvě pracují nejjednodušší síťové prvky opakovače, konvenční huby a transceivery. Tyto zařízení nemají žádnou znalost o obsahu přenášené zprávy, pouze berou vstupní bity a odesílají je jako výstupní. Na rozdíl od těchto zařízení např. směrovače a přepínače musí pracovat na vyšších vrstvách, protože chtějí znát obsah přenášených zpráv.

Technologie, které poskytují služby fyzické vrstvy, jsou například Etherloop, ISDN, CAN bus a jiné (Carroll, 2011).

4.1.2 LINKOVÁ VRSTVA

Data Link neboli linková, taktéž někdy překládána jako spojová je druhá vrstva ISO/OSI modelu, která poskytuje bezchybný přenos datových rámců z jednoho uzlu do druhého prostřednictvím fyzické vrstvy. Obvykle je tato vrstva dělena do dvou různých sub vrstev: Logical Link control (LLC) a Media Access Control (MAC). Toto rozdělení je

založené na architektuře IEE 802 a dochází ke spolupráci různých síťových technologii (Kozierok, 2005).

4.1.2.1 Logical Link Control (LLC)

V českém překladu Řízení logického spoje je horní podvrstva linkové vrstvy. Dříve zajišťovala řízení toku dat a mechanismus automatického opakování přenosu (ARQ), který označuje různé metody detekce a korekce chyb používané při přenosu dat. V dnešních sítích se však o řízení toku dat nestará, obvykle se o to starají protokoly transportní či aplikační vrstvy, které zabezpečují end-to-end přenos. Nynější funkcí této podvrstvy je ale poskytování mechanismu multiplexování, které umožňují používání různých síťových protokolů v jedné síti současně. Například IP, IPv6, AppleTalk.

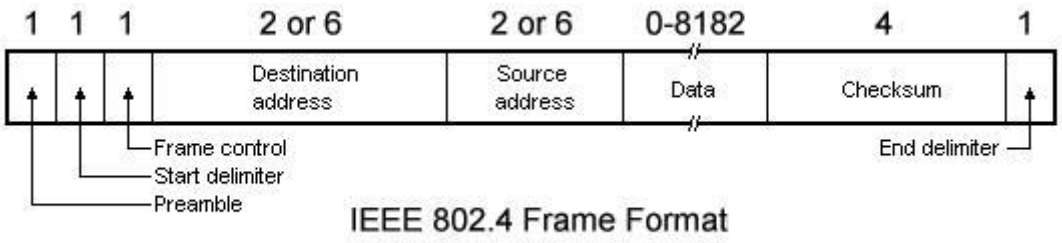
4.1.2.2 Media Acces Control (MAC)

Media Access Control podvrstva se chová jako rozhraní mezi LLC podvrstvou a síťovou vrstvou. Tato vrstva je hardwarově závislá a zajišťuje fyzické adresování a řízení přístupu k médiu. Vrstva emuluje full-duplexový logický komunikační kanál do multi-point sítě. Díky emulaci kanál poskytuje unicastovou, multicastovou či broadcastovou komunikaci.

Linková vrstva je zodpovědná za konečné zapouzdření zpráv do rámců, které jsou odesílány po síti na fyzické vrstvě.

4.2 RÁMCE

V počítačových sítích je rámec označení pro jednotku přenosu na linkové vrstvě modelu OSI. Rámec, který je ilustrován na obrázku č. 6, začíná synchronizační sekvencí, poté následuje hlavička, která obsahuje údaje nutné pro přenos rámce, tělo které obsahuje data a ukončen je patičkou. V patičce se nachází kontrolní součet, který umožní rozpoznat poškozený rámec. Pokud je při přenášení zjištěno, že rámec je poškozený, dochází k zahození rámce.



Obrázek 6 – Struktura rámce, (Gast, 2002)

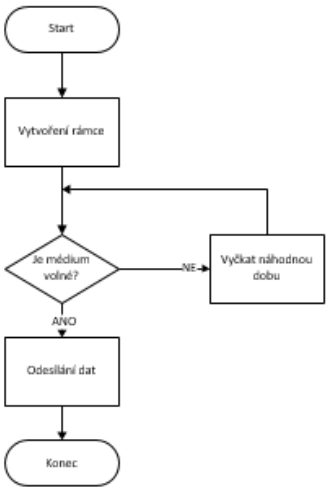
Odesílání rámců v bezdrátových sítích probíhá s polovičním duplexem. Pokud by současně vysílalo více než jedno zařízení, došlo by ke kolizi. Jestliže nastane kolize, data rámců jsou poškozena, stávají se nečitelnými a musí být odeslána znovu. Dochází k plýtvání času a prostředků, z tohoto důvodu je aplikována metoda CSMA/CA, která bude popsána v následující podkapitole (Carroll, 2011).

Nejedná se pouze o kolize, každá stanice musí taktéž dodržovat IFS. IFS představuje dobu čekání, předtím než může stanice začít odesílat. Interval zaručuje dostupnost média, pomocí rozestupu mezi odesíláním rámců, aby nedošlo k jejich nesprávné interpretaci. Existují 3 obdoby IFS. Přičemž každý z těchto obdob, má definován konkrétní účel podle standardu IEEE.

- **SIFS(short interframe space) –** používá se pro zprávy ACK
- **PIFS(point-coordination inteframe space) –** použití, jakmile přístupový bod řídí síť
- **DIFS(distributed-coordination interframe space) –** využíván při datových rámcích

4.2.1 CSMA/CA

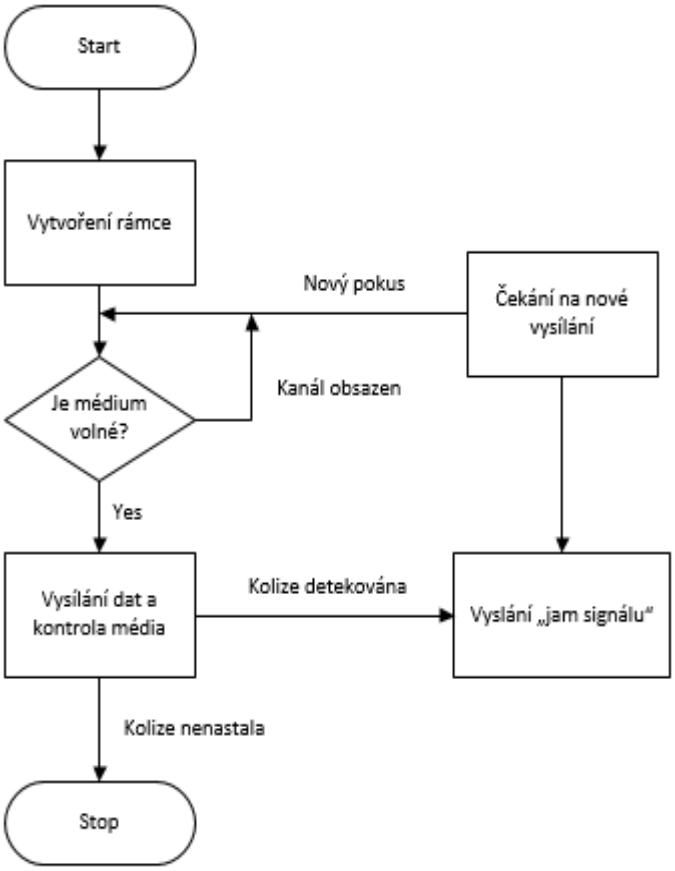
Carrier Sense Multiple Access with Collision Avoidance patří do skupiny protokolů označovaný jako metody s vícenásobným přístupem. Jedná se o modifikaci čistého CSMA. Protokol předchází kolizím a slouží k zvýšení přenosového výkonu. Část termínu *carrier sense* znamená, že stanice musí určit, zda nevysílá kdokoliv jiný. K tomu slouží metoda CCA (clear channel assessment), ve které dochází k prostému naslouchání. Druhá část *Collision avoidance* zajišťuje, exponenciální čekání pro uvolnění komunikačního kanálu. Pokud zjistíme, že přenosové médium je volné můžeme zahájit vysílání. V opačném případně čekáme na konec probíhajícího vysílání (Malířová, 2014). Ukázka zjednodušeného algoritmu je na obrázku č. 7.



Obrázek 7 – Algoritmus CSMA/CA

4.2.2 CSMA/CD

Stejně jako protokol CSMA/CA patří protokol CSMA/CD do třídy s vícenásobným přístupem. Pojem CSMA již byl rozebrán v podkapitole o protokolu CSMA/CA, proto se podíváme pouze po části CD(Collision detection). Stanice při svém vysílání kontroluje přenosové médium, zda nezachytí jiné vysílání, které by mohlo kolidovat s jejím. Jestliže stanice zjistí kolizi, vysílání je zastaveno a stanice čeká náhodnou dobu, než stanice svůj pokus znovu opakuje. CSMA/CD je efektivnější než samotné CSMA či CSMA/CA, z toho důvodu že v těchto protokolech se kolize nezjišťují a zbytečně se odesílá celý datový rámec, který se musí, pokud dojde ke kolizi odesílat znovu. (Learn-Networking.com Team, 2008) Na obrázku č. 8 si ukážeme zjednodušený algoritmus pro protokol CSMA/CD.



Obrázek 8 – Algoritmus CSMA/CD

4.2.3 TYPY BEZDRÁTOVÝCH RÁMCŮ

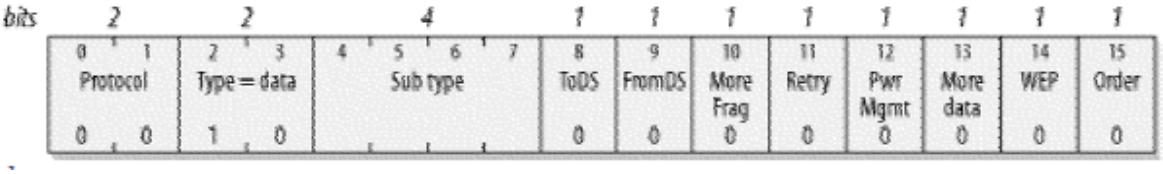
V bezdrátových sítích se vyskytují 3 základní typy rámců. Jsou jimi rámce pro správu, řídící a datové rámce. Tyto rámce mají zpravidla stejný typ hlavičky. Rozdíly spočívají v tělu rámce, které je specifičtější a určuje, jakou roli rámec plní. Tabulka č. 4 shrnuje některé typy rámců (Carroll, 2011).

Tabulka 4 – Tabulka typů rámců, zdroj: (Carroll, 2011)

Pro správu	Řídící	Datový
Maják	Požadavek pro odeslání	Prostá data
Sondovací požadavek	Povolení odeslání	Nulový funkční rámec
Odpověď na sondování	Potvrzení	Data+CF-ACK
Požadavek na přidružení	Power-save-poll	Data+CF-Poll
Odpověď na přidružení	Contention free end	Data+CF-Ack
Autentizační požadavek	Contention free end + potvrzení	Ack+CF-Poll
Autentizační odpověď	CF-ACK	
Deautentizační zpráva	CF-ACK+CF-Poll	
Odpověď opakovaného Přidružení		
ATIM		

4.2.3.1 Řídící rámce

Řídící rámce pomáhají doručení datových rámců mezi stanicemi. ACK řídící rámce umožňují potvrzení příjmu datových rámců. Další řídicí rámce jsou například. RTS, CTS. Na obrázku č. 9 je znázorněna struktura řídícího rámce, která je společná pro všechny druhy.



Obrázek 9 – Struktura řídícího rámce, zdroj: (Gast, 2002)

Protocol – Na obrázku je znázorněna verze protokolu 0. Jiná verze v tuto chvíli neexistuje.

Type – Všechny řídící rámce používají stejný typ označení „01“.

Subtype – Označuje druh konkrétního řídícího rámce (RTS,ACK,CTS).

ToDS & FromDS – Distribuční systém neposílá ani nepřijme řídící rámce, obě hodnoty vždy 0.

More frag – Neboli More Fragments bit je vždy na hodnotě 0, protože řídící rámce nejsou rozdělovány.

Retry bit – Vždy na hodnotě 0 protože řídící rámce nejsou tázány pro přeposlání.

Power Management bit – Označuje stav řízení spotřeby odesílatele po odeslání rámce.

More Data bit – Taktéž na hodnotě 0, využíván pouze v řídících a datových rámcích.

WEP – Řídicí rámce nejsou šifrované, hodnota bitu na 0.

Order – Dochází k atomické výměně operací, pořadí nemůže být měněno, hodnota bitu 0.

4.2.3.1.1 Přehled řídících rámců

Request to Send (RTS)- Funkce RTS snižuje rámcové kolize, pokud skryté stanice mají spojení se stejnými přístupovými body. Stanice předtím než odešle datový rámec na jinou stanici, vyšle RTS rámec, po kterém dochází k oboustrannému potvrzení.

Clear to Send (CTS) – Slouží jako odpověď na RTS rámec. CTS obsahuje časovou hodnotu, pro kterou ostatní stanice mají zadržet komunikaci. Díky tomu dochází k snižování kolizí a dochází k větší propustnosti sítě.

Acknowledgment (ACK) – Po obdržení a zkontrolování datového rámce, přijímací stanice odesílá ACK rámec odesílající stanici. Pokud odesílající stanice neobdrží potvrzení pomocí ACK, dochází k přeposlaní datového rámce.

4.2.3.2 Datové rámce

Datové rámce přenášejí data vyšších protokolů. Na obrázku č. 10 je znázorněn obecný tvar rámce. Všechny části na obrázku, nemusí být použity. Datové rámce mohou být rozděleny pomocí jejich funkce. První druh rozdělení je pomocí jejich služeb tzn. contention-based service a contention-free service. Další rozdělení je pomocí toho jestli obsahují data, nebo vykonávají řídící funkce.

Obrázek 10 – Struktura datového rámce, zdroj: (Gast, 2002)

Frame control – Bity obsažené v této části, mohou ovlivňovat interpretaci ostatních polí v MAC hlavičce. Převážně pak určují adresní pole hlavičky, která závisí na hodnotě ToDSand a FromDSbits.

Duration – Duration nese hodnotu takzvaného Network Allocation Vectoru (NAV), která určuje povolenou dobu přístupu k médiu.

Adressing – Počet a funkci adres v hlavičce, závisí na tom, jaká sada systémových bitů je nastavena. Tabulka znázorňuje možné kombinace využití adresních polí v rámcích.

Tabulka 5 – Využití adresního pole v datovém rámci zdroj: (Gast, 2002)

Funkce	ToDS	FromDS	Adresa 1	Adresa 2	Adresa 3	Adresa 4
IBSS	0	0	DA	SA	BSSID	-
To AP	1	0	BSSID	SA	DA	-
From AP	0	1	DA	BSSID	SA	-
WDS	1	1	RA	TA	DA	SA

Obecně adresa 1 označuje přijímač, ve většině případů je to cílová adresa. Není tomu ale vždy, také může obsahovat broadcastovou či multicastovou adresu. Adresa 2 je určena vysílači a je používána k odeslání potvrzení (acknowledgments). Adresa 3 je využívána k filtrování pomocí přístupových bodů či distribuovaných systémů, kde záleží na určitém typu sítě (Gast, 2002).

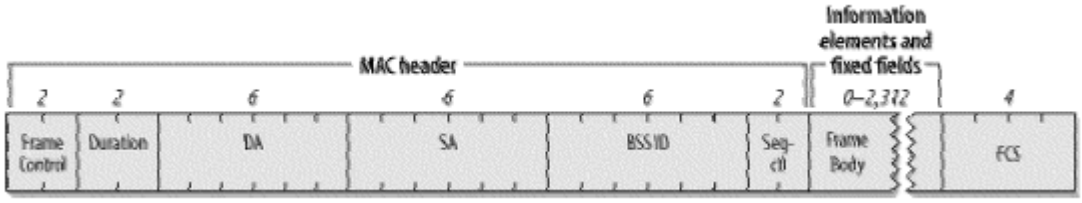
4.2.3.2.1 Přehled datových rámců

Data (prostá data) jsou přenášena pouze během contention-based access period. Jsou to jednoduché rámce s jediným účelem, přenášení těla rámce z jedné stanice na druhou.

Null (Nulový funkční rámec) obsahují MAC hlavičku a FCS patičku. Jsou využívaný pro probuzení přístupových bodů.

4.2.3.1 Rámce pro správu

Jak je již zřejmé, rámce pro správu slouží k správě řízení připojení. Používají se k připojení a opuštění bezdrátové buňky. Při pohledu zachytávání je v rámci - Type uvedeno „managment“ a dílčí typ určuje, o jaký druh rámce pro správu se jedná. Taktéž nedochází k šifrování rámců pro správu a jsou používány pro podpoření autentizace, asociace a synchronizace.



Obrázek 11 – Struktura rámce pro správu, zdroj (Gast, 2002)

Na obrázku č. 11 je znázorněna obecná struktura managment rámce. Hlavička je stejná pro všechny managment rámce. Některé rámce pro správu používají tělo rámce, pro převod specifických informací.

Adresace – stejně jako u ostatních rámců, první adresa slouží k určení cíle a druhá adresa k označení odesílatele.

Frame body – Řídící rámce jsou poměrně různorodé. Většina dat uložených v těle rámce používá statickou délku pole a jsou nazývány *fixed fields* . Dynamické části pole jsou označovány jako *information elements,* které obsahují skupiny dat různé velikosti. Každá skupina dat je označena číslem a velikostí.

4.2.3.1.1 Druhy řídících rámců

Beacon – Do češtiny volně přeloženo majáky, slouží k zjištění existence sítě. Taktéž jsou používány k většině úkolů síťové údržby a jsou přenášeny v pravidelných intervalech. V bezdrátových sítích zodpovědnost za odeslání majáků mají přístupové prvky.

Probe Request neboli sondovací požadavek slouží k určení oblasti existující 802.11 sítě. Nejdůležitější části tohoto rámce jsou SSID a poměry podporované stanicí. Stanice využívají tento rámec k zjištění, jestli uživatel může či nemůže vstoupit do sítě.

Probe Response je odpověď na sondování, pokud sondovací požadavek narazil na síť s požadovanými parametry, síť odešle odpověď. Stanice, která odeslala poslední maják, je zodpovědná za odeslání odpovědi příchozím sondám.

Disassociation and Deauthentication – Disassociation rámce jsou používány pro ukončení vztahu sdružení a Deauthentizační zpráva je používaná pro ukončení vztahu ověřování. Oba rámce obsahují jednotné pole „Reason Code“.

Assocation Request, Reassociation Request – Jakmile přenosná stanice zjistí a ověří kompatibilní síť, pokusí se připojit do sítě pomocí požadavku na přidružení. Pokud mobilní stanice opustí dočasně pokrytou oblast přístupového bodu a chce se znovu připojit, posílá požadavek pro opakované přidružení.

Authentication – Pro ověření přístupového bodu si stanice vyměňují Autentizační rámce. Existují různé druhy algoritmů pro ověření. Pole „Authentication Algorithm Number“ označuje výběr algoritmu (Gast, 2002).

5 PRVKY A TOPOLOGIE BEZDRÁTOVÝCH SÍTÍ

V této kapitole budou představeny základní stavební kameny bezdrátových sítí přístupové body, mosty a jiné. Taktéž bude představena základní architektura.

5.1 PRVKY BEZDRÁTOVÝCH SÍTÍ

Bezdrátový přístupový bod alias **AP** (Access Point) je zařízení, které kombinuje vysílač a přijímač. Zároveň je také uzlem bezdrátové sítě a navíc dokáže propojit kabelovou síť s bezdrátovou. Dá se říct, že se jedná o most mezi kabelovou a bezdrátovou sítí. Samozřejmě je tu i možnost propojení dvou přístupových bodů mezi sebou a tím dochází k rozšíření bezdrátové sítě. Většina přístupových bodů má zabudované omezení na podsíť o velikosti 255 klientů. Zařízení AP mohou podporovat standardy 802.11a/b/g nebo se dokonce objevují různé kombinace obvykle dvou nebo tří z výše uvedených protokolů.

Existují také bezdrátové přístupové body, které disponují technologii WISP, která dokáže z přístupového bodu udělat odchozí bránu k ISP, aniž by poskytovatel musel zadávat všechna zařízení. Wi-Fi modul přístupového bodu je změněn na klienta, který se tváří jako jeden PC a zároveň přeposílá Wi-Fi signál ve vnitřní síti. Vnitřní přeposílaná síť je izolovaná, což zvyšuje její bezpečnost a umožňuje vlastní adresaci (Srb, 2012) (Airdump, 2010) .

V domácích sítích bývají **bezdrátové brány** součástí spojení do Internetu. Bezdrátové brány mají funkci přemostění externí sítě WAN do vnitřní sítě, ať už bezdrátové či kabelové. Jediné rozdíly mezi bránou a přístupovým bodem jsou v tom, jaké služby poskytují. Brány obvykle nabízí následující služby:

- Bezdrátové připojení 802.11
- Servery DHCP, DNS
- Zabezpečení
- Asociaci zařízení, nastavení a konfigurace
- Vlastnosti směrovače podle 802.3 a technologii NAT traversal
- Objevování zařízení, Diagnostiku
- UPnP (Universtal Plug and Play) (Sosinsky, 2010).

Opakovače (repeater) jsou aktivní síťové prvky, které rozšiřují dosah bezdrátové sítě. Je to tedy zařízení, které příjme signál a posílá jej dále zesíleně. Jejich výhodou je, že mají stejné nastavení jako zařízení, od kterého signál přijímají a z toho důvodu složitost bezdrátové sítě nijak nezvyšují. Umisťují se nejčastěji na hranici dosahu přístupového bodu. Taktéž již

některé zmíněné přístupové body (AP) mají možnost konfigurace na režim opakovače (Sosinsky, 2010).

Most (bridge) je sítové zařízení, sloužící k propojení dvou či více sítí nebo jejich segmentů, které jsou fyzicky nebo logicky odděleny. Mosty pracují na druhé (linkové) vrstvě ISO/OSI modelu. Nejznámější topologie funkce bezdrátových mostů jsou například **Point-to-point** (jedna ku jedné), **point-to-multipoint** (jedna ku více) a **redundantní multipoint**(koncové body tvoří duplikované páry) (Sosinsky, 2010).

5.2 TOPOLOGIE BEZDRATOVÝCH SITÍ

Bezdrátové sítě mohou mít podobu mnoha různých topologií. V následující kapitole si porovnáme 4 druhy topologií sítí pomocí jejich zaměření, či využití bezdrátových technologii.

5.2.1 WPAN

Tuto topologii sítě využíváme v situacích, kdy se potřebujeme bezdrátově připojit k něčemu, co je od nás velmi blízko, obvykle do 10 metrů. Reálné využití je připojení například bezdrátových sluchátek, či dokonce i myši.

Osobní sítě WPAN jsou přímo určené k provozu v dosahu 6 metrů. Nejčastější technologie, které využíváme v osobních sítích, jsou IrDa a Bluetooth. Tato síť může obsahovat nejvíce osm aktivních zařízení, neaktivní zařízení nejsou nijak omezena. Obvykle spadají do nelicencovaného pásma 2,4 GHz a jejich standardy popisuje pracovní skupina IEEE 802.15.

5.2.2 WLAN

Druhý typ, který bude představen, je topologie, se kterou se v reálném provozu setkáme nejčastěji. Sítě WLAN můžeme provozovat v prostředí od malých kanceláří až po velké podnikové sítě. Zařízení v této kategorii jsou většinou využívána v seskupení, označované jako infrastrukturní sítě, ovšem můžou fungovat i v režimu ad-hoc. Sítě WLAN mají následující charakteristiky.

- Frekvenční pásmo 2,4Ghz nebo 5Ghz
- Dosah až 100 metrů
- Pro dosažení větší vzdálenosti je potřeba vyšší vysílací výkon
- Zpravidla obsahuje více klientů (Nejedná se o osobní sítě) (Malířová, 2014).

Produkty, které jsou využívány v sítích WLAN používající standard 802.11, jsou zaregistrované pod obchodní značkou Wi-Fi. Kromě bezdrátových uživatelů jsou zde také bezdrátové tiskové servery, prezentační servery a záznamová zařízení.

5.2.3 WMAN

Wireless Metropolitan Area network je bezdrátová metropolitní síť, která spojuje několik bezdrátových lokálních sítí. Sítě WMAN jsou používány jako páteřní sítě, či dvoubodová spojení (point-to-point), nebo i jako vícebodová připojení (point-to-multipoint). Většina WMAN sítí používá licencované frekvenční pásmo, ale najdou se i takové, které používají nelicencované a může tak docházet k rušení od jiných sítí. Další charakteristiky jsou například:

- Nejznámější je pod označením WiMax
- Její rychlost je blízká spíše širokopásmovému připojení než ethernetu

5.2.4 WWAN

Wireless Wide Area Network je rozsáhlá bezdrátová síť. Sítě WWAN využívají pouze technologií síťové infrastruktury mobilních operátorů, kterých je na českém trhu oproti ISP využívajících WMAN jen hrstka. Tento druh bezdrátového připojení, je možné udržovat v rozsáhlých geografických oblastech, proto je tato technologie označována, jako technologie druhé generace (2G). Výhodou WWAN je v pokrytí, které může být celostátní nebo celosvětové, a také vyšší zabezpečení (Kysela, 2010). Nevýhodami jsou například

- Nízká přenosová rychlost
- Platba za používání
- Vysoké náklady na provozování

6 PRVKY MIKROTIK

Firma MikroTik je společnost sídlící v Litvě a byla založena v roce 1996, byla založena za účelem rozvoje směrovačů a bezdrátových systému ISP. Nyní firma poskytuje hardware a software pro připojení k internetu ve většině zemí po celém světě.

6.1 PRODUKTY

RouterBOARD je plně funkční systém. Firma MikroTik poskytuje různé verze sytému. Základní verze je pouze odhalená základní deska. Ke správné funkčnosti desky je potřeba ji osadit alespoň anténou. Základní verzi lze rozšířit o Daughterboard, či rozšiřující moduly např. Ethernet porty či miniPCI sloty. Druhou verzí jsou takzvané hotové sestavy, které stačí zapojit a nastavit. V neposlední řadě nabízí MikroTik venkovní jednotky, které obsahují v jednom těle jak RouterBOARD, tak anténu. Takové výrobky mají jištění proti vniknutí vody, prachu a také proti UV záření. Zařízení takového charakteru jsou zpravidla napájena přes POE (RouterBOARD, 2015).

Operační systém **RouterOS** je vestavěný systém určený zejména pro produkt od stejné společnosti **RouterBOARD**, ale lze jej instalovat i na platformu i386. Celý systém je založen na linuxovém jádru a je navržený pro spolehlivost a rychlost provozu sítě. Operační systém je kompaktní a nezabírá více jak 64 MB. Nabízí velké množství funkcí pro chod sítě, a to od základních, jako např. správce vstupů, pevné nastavení cest, DHCP server až po složité: VPN (IPsec), dynamické směrování (OSPF, BGD), nástroje pro analýzu sítě (ping, bandwidth test) (MikroTik, 2015).

Posledním systémem, který je určený pro přepínače je **SwitchOS**. Jednoduchý operační systém, který nám dává možnost nastavit základní vlastnosti přepínače, ale také složitější funkcionalitu jako např. virtualní sítě, filtry mac adres nebo sledování provozu.

6.2 MOŽNOSTI KONFIGURACE

Pro nastavení operačního systému RouterOS lze použít 3 typy připojení:

- Přes webové rozhraní
- Aplikace Winbox
- Vzdálené připojení ke konzoli (telnet,ssh)

V základní konfiguraci jsou povoleny všechny 3 možnosti přístupu. V rámci zabezpečení je vhodné omezit nebo zastavit nezabezpečené služby jako telnet a rozhraní pro úpravu pomocí

internetového prohlížeče. Operační systém nabízí možnost omezení přístupu na tyto služby na pouze některé adresy IP. Také je zde možnost změnit porty, na kterých bude naslouchat systém.

Winbox je vizuální aplikace od firmy MikroTik pro snadnou a rychlou konfiguraci systému RouterOS. Aplikace je kompatibilní pouze se systémem Windows, ale může být pomocí emulátoru Wine spuštěna na Linuxu a Mac OSX.

Některé rozšířené možnosti a systémově kritické změny přes aplikaci Winbox nejsou povoleny například změna MAC adresy na WAN/LAN portu.

7 ANALÝZA LATENCE BEZDRÁTOVÉ KOMUNIKACE

V této kapitole bude provedena analýza měření latence v bezdrátové komunikaci. Cílem analýzy je, zjistit do jaké úrovně, je vznik latence závislý na velikosti zasílaných dat a počtu prvků v bezdrátové síti.

7.1 ÚVOD DO ANALÝZY

Analýza byla provedena v laboratorní místnosti NET101. V analýze byly použity prvky od dvou různých firem. První druh prvků byl od firmy MikroTik a to řada produktu RouterBoard 493G. Představení produktů a možnosti konfigurace jsou popsány v 6. kapitole. Druhý byl od firmy TP-LINK konkrétně řada TL-WR843ND z důvodu možnosti takzvaného WISP módu, který nám dovoluje zároveň vysílat i přijímat bezdrátovou síť.

7.2 POSTUP PROVÁDĚNÍ METODIKY

Cílem bakalářské práce je zjistit, do jaké úrovně je latence závislá na velikosti odesílaných dat a počtu prvků v síti. Pro zjištění latence v provozu sítě nám poslouží traffic generator od firmy MikroTik, který nám pomůže s analýzou latence. Nastavení nástroje pro generování toku dat bude popsáno v následující podkapitole.

Prvním krokem bylo určení rozsahu odesílání velikosti dat paketu. Maximální velikostí je ohraničena pomocí tzv. L2MTU. L2 MTU označuje maximální velikost paketu bez MAC hlavičky, které může být odesláno přes určité rozhraní. Maximální velikostí na zařízeních firmy MikroTik 493G je 1600 byte. Jako Nejmenší velikost odesílaného paketu jsem určil velikost 200 byte. Krok posunu velikosti paketu jsem určil na 200 a z toho nám vychází, že pro každou topologii jsem opakoval 8 různých měření s různými velikostmi. Pro každé z těchto měření, bylo měření latence opakováno 40x. Každé měření, které bylo vyhodnoceno přes nástroj „traffic generator“ odeslalo 10 paketů. Z toho nám vyplívá, že pro jednu velikost bylo odesláno 400 paketů, ze kterých poté byla počítána výsledná průměrná latence.

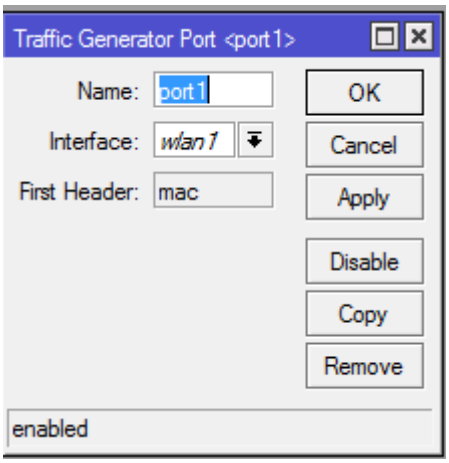
Následujícím krokem experimentu, bylo zjištění, jestli počet prvků je závislý na vzniku latence v síti. K experimentu byly postaveny 3 různé topologie. Jejich konfigurace, výsledná latence a topologie bude rozebrána v následujících kapitolách.

7.2.1 TRAFFIC GENERATOR

Traffic generátor je nástroj na zařízeních firmy MikroTik pro generování umělého provozu v síti. Nástroj umí vytvářet a odesílat různé velikosti paketů na určitém portu. V našem experimentu byl využíván pro generování v bezdrátové síti. V rámci generátoru je i analýza výsledků, která obsahuje latenci, jiter, počet ztracených a špatných paketů a jiné.

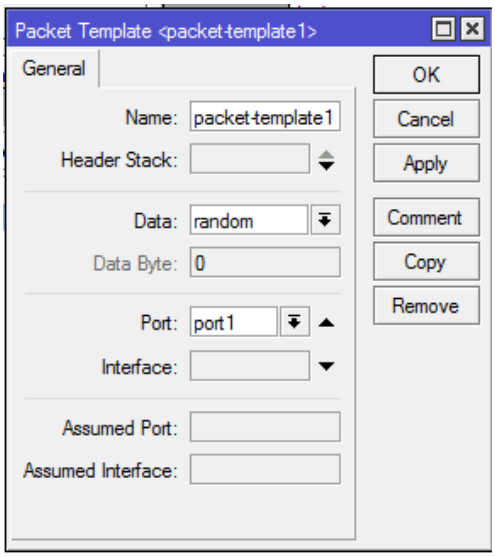
7.2.1.1 Postup nastavení generátoru

První krok při konfiguraci generátoru je vytvoření portu, ve kterém zvolíme, přes které rozhraní poteče generovaný tok dat.



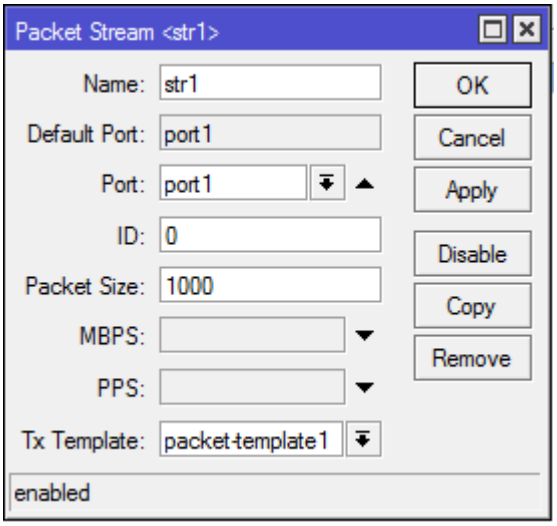
Obrázek 12 – Nastavení portu

Poté co byl určen port, přes který budeme vysílat, nastává vytvoření paketů, které budeme odesílat. Pro naše potřeby nebylo důležité, jaká data byla odesílána, proto jsem zvolil možnost náhodných dat a znovu vybral port.



Obrázek 13 – Tvorba paketu

Posledním krokem, předtím než můžeme začít generovat data do naší sítě, nastává na vytvoření proudu. Generátor dovoluje vytvořit víc proudů, proto si proudy můžeme pojmenovat a zvolit jim patřičné ID. Dále máme možnost vybrání portu, velikosti paketu a šablony již vytvořeného paketu.



Obrázek 14 – Výběr streamu

7.3 TOPOLOGIE 1

Obrázek 15 – Topologie 1

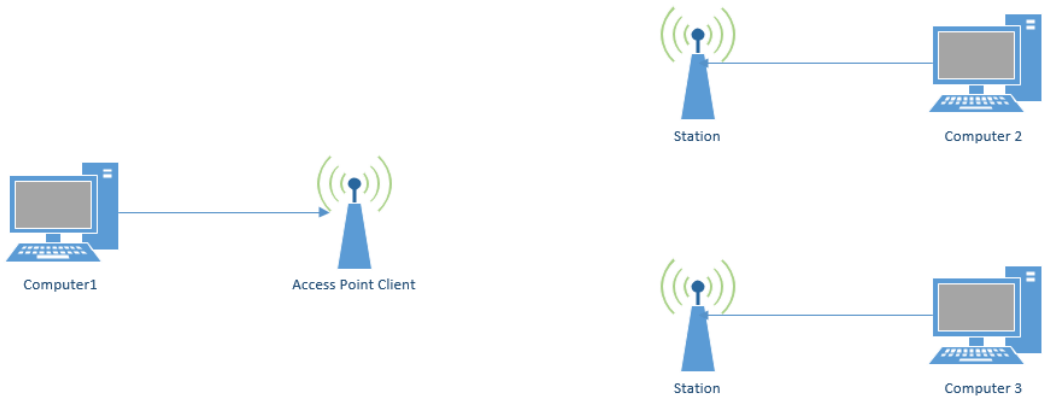
První topologie, která byla použita, byla topologie se dvěma síťovými prvky. První zařízení od firmy MikroTik bylo AP v režimu „AP bridge“, které vysílalo 802.11 síť. Druhé zařízení bylo shodné jako to první, pouze běželo v režimu „Station“. Konektivita byla ověřena pomocí nástroje ping. Na obou zařízeních bylo na fyzický WLAN port nastavena statická IP adresa.

První topologie nám prokázala, že latence je závislá na velikosti odesílaného paketu. Následující tabulka nám shrnuje naměřené hodnoty latence.

Tabulka 6 Latence první topologie

Velikost Paketu (byte)	Průměrná latence (milisekundy)
200	**2,86**
400	**4,99**
600	**6,76**
800	**8,79**
1000	**10,16**
1200	**11,68**
1400	**13,45**
1600	**14,66**

7.4 TOPOLOGIE 2



Obrázek 16 – Topologie 2

Jako druhá byla využita topologie se třemi síťovými prvky. První zařízení od firmy MikroTik bylo AP v režimu „AP bridge“, které vysílalo 802.11 síť. Ostatní zařízení byli shodné jako to první, pouze běželi v režimu „Station“. Konektivita byla ověřena pomocí nástroje ping. Na všech zařízeních bylo na fyzický WLAN port nastavena statická IP adresa.

Druhá topologie nám prokázala, že latence není závislá na počtu přijímacích zařízení v sítí. Následující tabulka nám shrnuje naměřené hodnoty latence.

Tabulka 7 Latence druhé topologie

Velikost Paketu (byte)	Průměrná latence (milisekundy)
200	2,67
400	4,60
600	6,14
800	7,81
1000	9,48
1200	10,93
1400	12,90
1600	14,71

7.5 TOPOLOGIE 3

Obrázek 17– Topologie 3

Třetí topologie, která byla použita, byla topologie se třemi síťovými prvky. První zařízení od firmy MikroTik bylo AP v režimu „AP bridge“, které vysílalo 802.11 síť. Druhé zařízení od firmy TP-Link, bylo zařízení, které zároveň přijímalo a vysílalo bezdrátovou síť. Disponovalo vlastností WISP, které je rozebrána v 5. kapitole teoretické části. Poslední zařízení bylo AP od firmy Mikrotik, které bylo v režimu „station“. Konektivita byla ověřena pomocí nástroje ping.

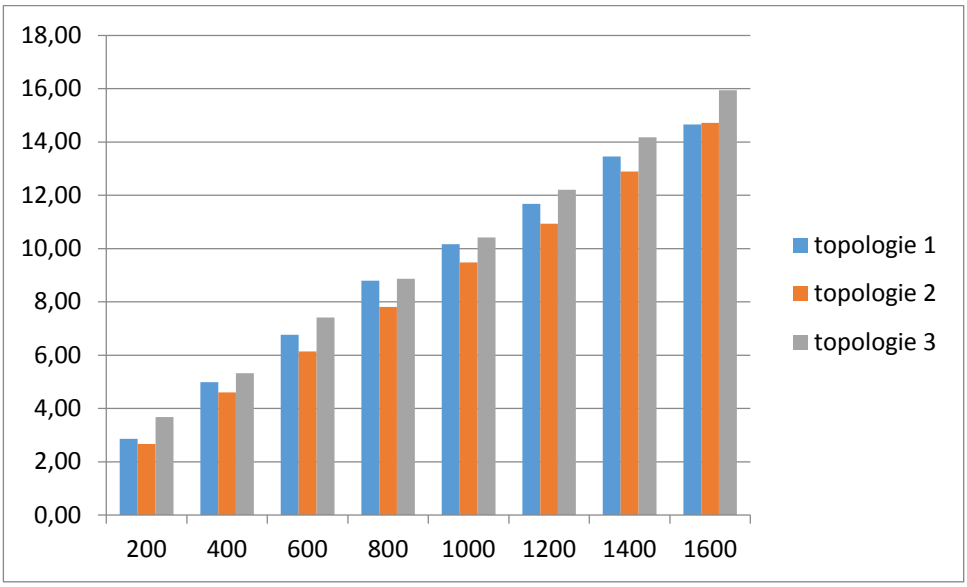
Druhá topologie nám prokázala, že latence je závislá na počtu vysílacích zařízení v sítí. Následující tabulka nám shrnuje naměřené hodnoty latence.

Tabulka 8 – Latence třetí topologie

Velikost Paketu (byte)	Průměrná latence (milisekundy)
200	3,68
400	5,33
600	7,41
800	8,86
1000	10,42
1200	12,20
1400	14,17
1600	15,94

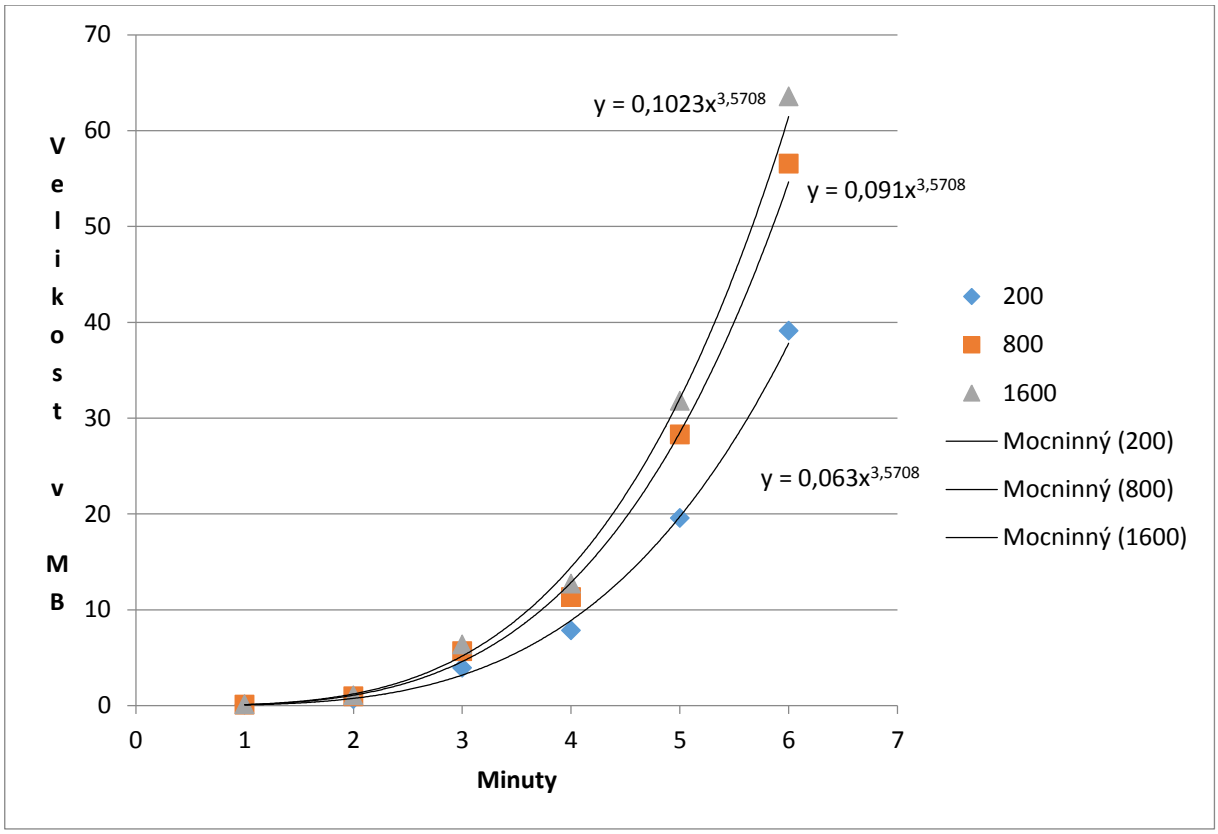
7.6 ANALÝZA VÝSLEDKŮ

Zjištěné výsledky prokazatelně znázorňují, že velikost paketu má značný vliv na latenci. Následující graf č. 1 nám ukazuje porovnání latencí všech ukázkových topologii.



Graf 1 – Porovnání průměrných latencí

Z naměřených výsledků, lze predikovat, pro jaké velikosti souborů je vhodná velikost paketu 200, 800, 1600. Na následující tabulce si ukážeme průběh odesílání paketu za konstantu času.



Graf 2 – Průběh odesílání dat

Průběh odeslání paketu je dán mocninou rovnicí:

$$y = cx^{3,5708}$$

Kdy c je konstanta, která je závislá na velikosti odesílaného paketu.

Z toho vyplívá, že pokud odesíláme data větší než je velikost paketu, je nejúčinnější odesílat maximální velikost L2 MTU.

ZÁVĚR

Cílem bakalářské práce bylo zjištění tvorby latence při bezdrátové komunikaci v závislosti na přenášeném objemu dat a počtu prvků zapojených do komunikace. Práce byla rozdělena na dvě stěžejní části teoretickou a praktickou.

V první části byly představeny základní principy a pojmy s důrazem na bezdrátovou komunikaci. Dále byly představeny nejpoužívanější standardy od americké organizace IEEE.

Problematika určení polohy komunikačních zařízení byla rozebrána pomocí Fresnelových zón a polarizace. Wi-Fi technologie komunikuje na prvních dvou vrstvách ISO/OSI pomocí bezdrátových rámců, z toho důvodu funkčnost prvních dvou vrstev ISO/OSI modelu a struktura rámců byla představena v teoretické části práce.

V praktické části byla zkoumána latence převážně na prvcích od firmy MikroTik. Latence byla zkoumána pomocí nástroje Traffic generator, který poskytuje na svých zařízeních již zmíněná společnost. Byla provedena měření v 3 různých topologiích o různých velikostech.

Z naměřených výsledků je patrné, že latence je závislá na velikosti přenášených dat. Tvorba latence v závislosti na velikost odesílaných dat. Pokud odesíláme soubor větší než je velikost rámce, je vhodné odesílat co největší rámec, který nám druhá vrstva ISO/OSI modelu dovoluje. Z naměřených výsledků nám také vyplívá, čím méně vysílacích zařízení v síti, tím je latence menší.

Žádoucím rozšířením této práce by bylo rozšíření počtu vysílacích zařízení v bezdrátové komunikaci, pro přesnější zjištění do jaké míry je latence závislá na počtu zařízení v síti. Dalším možným rozšířením by bylo otestování provozu sítě pomocí softwarových generátorů například pomocí multiplatformního generátoru Ostinato.

POUŽITÁ LITERATURA

Airdump. 2010. Wiki.Airdump.cz. [Online] 2010. [Citace: 22. 4 2016.] http://wiki.airdump.cz/WISP_Mode.

Armstrong, Shain. 2013. RFIDinsider. [Online] 2013. [Citace: 31. 3 2016.] http://blog.atlasrfidstore.com/circular-polarization-vs-linear-polarization.

Bevelacqua, Peter Joseph. 2009. Polarization - EM Waves and Antennas. [Online] 2009. [Citace: 20. 2 2016.] http://www.antenna-theory.com/basics/polarization.php.

Carroll, Brandon James. 2011. *Bezdrátové sítě Cisco Autorizovaný výukový průvodce.* 1. Brno : Computer press, a.s., 2011. ISBN 978-80-251-2884-8.

České vysoké učení technické v Praze. 2008. Přístupové metody bezdrátových sítí. [Online] 2008. [Citace: 11. 3 2016.] http://access.feld.cvut.cz/view.php?cisloclanku=2008100003.

EPRIN spol. s r.o. 2015. Základní přehled standardů IEEE 802.11. [Online] 2015. [Citace: 11. 3 2016.] http://www.eprin.cz/zakladni-prehled.html.

Gast, Mathew. 2002. *GAST, Matthew. 802.11 wireless networks: the definitive guide.* 2. místo neznámé : O'Reilly, 2002. ISBN 0-596-00183-5.

Goggi, Christina. 2014. TalkTechToMe. [Online] 2014. [Citace: 22. 2 2016.] http://www.gfi.com/blog/wi-fi-glossary-71-terms-you-need-to-know/.

Grigorik, Ilya. 2013. *High Performance Browser Networking.* místo neznámé : O'Reilly Media, 2013. ISBN:978-1-4493-4476-4.

IEEE Computer Society. 2012. *IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* New York : IEEE Computer Society, 2012.

International Organization for Standardization. 2016. ISO. [Online] 2016. [Citace: 2. 27 2016.] http://www.iso.org/iso/home/about.htm.

Kohanbash, David. 2014. Antennas and Amplifiers for Long Distance Wireless Communications. *Robots for robotic.* [Online] 3. 5 2014. [Citace: 3. 5 2016.] http://robotsforroboticists.com/long-distance-wireless-communications-antennas/.

Kozierok, Charles M. 2005. The TCP/IP Guide. [Online] 2005. [Citace: 2. 16 2016.] http://www.tcpipguide.com/free/t_DataLinkLayerLayer2.htm.

Kysela, Jiří. 2010. Internet pro všechny. [Online] 2010. [Citace: 2. 24 2016.] http://www.internetprovsechny.cz/bezdratovy-internet-a-technologie-wi-fi-v-ceske-republice/.

Learn-Networking.com Team. 2008. Learn Networking. [Online] 2008. [Citace: 27. 2 2016.] http://learn-networking.com/network-design/carrier-sense-multiple-access-collision-detect-csmacd-explained.

Macoun, Jindra. 2014. O Fresnelových zónách. [Online] 03 2014. [Citace: 4. 4 2016.] http://www.crk.cz/FILES/VR-ANT/57.%20O%20Fresnelov%C3%BDch%20z%C3%B3n%C3%A1ch.pdf.

Malířová, Aneta. 2014. UPaWiki. [Online] 2014. [Citace: 2. 17 2016.] https://wiki.upce.cz/.

Meyer, Douglas. 1990. *TCP/IP versus OSI.* Missouri University : IEEE, 1990.

Microsoft. 2014. Definice sedmi vrstev modelu OSI a vysvětlení jejich funkcí. [Online] 2014. [Citace: 11. 2 2016.] https://support.microsoft.com/cs-cz/kb/103884.

Mikrotik. 2011. Manual:Initial Configuration. [Online] 2011. [Citace: 20. 1 2016.] http://wiki.mikrotik.com/wiki/Manual:Initial_Configuration.

MikroTik. 2015. MikroTik wiki. [Online] 2015. [Citace: 11. 3 2016.] http://wiki.mikrotik.com/wiki/Manual:RouterOS_features.

RouterBOARD. 2015. Routerboard.sk. [Online] 2015. [Citace: 22. 2 2016.] http://www.routerboard.sk/.

Service, National Weather. 2012. NWS WSR-88D to Receive Dual Polarization Upgrade. *National Weather Service Weather Forecast Office.* [Online] 5. 26 2012. [Citace: 3. 5 2016.] http://www.crh.noaa.gov/.

Sosinsky, Barrie. 2010. *Mistrovství – počítačové sítě.* 1. Brno : Computer Press, 2010. ISBN 978-80-251-3363-7.

Srb, Martin. 2012. IPSvět. [Online] 2012. [Citace: 22. 4 2016.] http://www.ipsvet.cz/wisp-mode-u-access-pointu/.

Vaňková, Jana. 2012. Metodický portál RVP. [Online] 2012. [Citace: 28. 3 2016.] http://clanky.rvp.cz/clanek/a/14721/15061/PARAMETRY-POCITACOVYCH-SITI.html/.

Vysoká škola Baňská. 2014. Výukové materiály Vysoké školy Baňské. [Online] 2014. [Citace: 25. 1 2016.] http://fei1.vsb.cz/kat420/vyuka/FEI/sireni_vln/teze/otazka_09.pdf.

Zbyněk Raida, et al. 2010. *Elektromagnetické vlny Mikrovlnná technika.* Brno : Vysoké učení technické v Brně, 2010.

SEZNAM PŘÍLOH

Příloha A *Tabulky_Topologie_1*

Příloha B *Tabulky_Topologie_2*

Příloha C *Tabulky_Topologie_3*

Příloha D *Tabulky_Vyhodnoceni*