

# Návrh a optimalizace bezdrátového spoje

Bakalářská práce

Vedoucí práce:

Ing. Petr Zach

Tomáš Rumíšek

Brno 2014



Zde bych chtěl poděkovat Ing. Petrovi Zachovi za ochotu a pomoc při vypracování této bakalářské práce. Jeho rady mi byly velkým přínosem při její realizaci. Díky patří také všem, kteří mi pomáhali s instalací zařízení a také těm, kteří mi povolili umístění technického vybavení na jejich nemovitosti.



## **Čestné prohlášení**

Prohlašuji, že jsem tuto práci **Návrh a optimalizace bezdrátového spoje** vypracoval samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb. o vysokých školách ve znění pozdějších předpisů a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací*.

Jsem si vědom, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla a to až do jejich skutečné výše.

V Brně dne 20. prosince 2014

---



## **Abstract**

Rumíšek, T. Design and optimization of wireless link. Bachelor thesis. Brno: Mendel University in Brno, 2014.

The first part of bachelor thesis focuses on the selection of appropriate technology for wireless connection of the type point-point which is then assembled using two best standards. There are also technologies compared from two different manufacturers who use more of their proprietary protocols.

## **Keywords**

wifi, 802.11, MikoTik, Ubiquiti, nstream, NV2, AirMAX, TDMA.

## **Abstrakt**

Rumíšek, T. Návrh a optimalizace bezdrátového spoje. Bakalářská práce. Brno: Mendelova univerzita v Brně, 2014.

První část bakalářské práce se zaměřuje na výběr vhodné technologie pro bezdrátový spoj typu bod-bod, který je následně sestaven pomocí dvou nejvhodnějších standardů. Také je zde porovnána technologie od dvou různých výrobců, kteří používají další své proprietární protokoly.

## **Klíčová slova**

wifi, 802.11, MikoTik, Ubiquiti, nstream, NV2, AirMAX, TDMA.





# Obsah

<b>1</b>	<b>Úvod a cíl práce</b>	<b>13</b>
1.1	Úvod.....	13
1.2	Cíl práce.....	13
<b>2</b>	<b>Bezdrátový přenos</b>	<b>14</b>
2.1	Jednotlivé standardy .....	14
2.1.1	IEEE 802.11b.....	14
2.1.2	IEEE 802.11g.....	14
2.1.3	IEEE 802.11a.....	14
2.1.4	IEEE 802.11n.....	14
2.1.5	IEEE 802.11ac.....	15
2.2	Maximální povolené vysílací výkony .....	16
2.3	DSSS .....	17
2.4	FHSS.....	17
2.5	OFDM.....	17
2.6	Fresnelova zóna .....	18
2.7	SNR.....	18
2.8	Hardware fragmentation threshold.....	18
2.9	Problematika skrytých uzlů .....	19
2.10	WMM.....	19
<b>3</b>	<b>Použité technologie</b>	<b>20</b>
3.1	MikroTik .....	20
3.1.1	Nstream.....	20
3.1.2	NV2 .....	20
3.2	Ubiquiti.....	20
3.2.1	AirMAX .....	21
3.2.2	RTS Treshold.....	21
3.2.3	Aggregation .....	21
<b>4</b>	<b>Rešerše dostupných prací a odborných publikací</b>	<b>22</b>
<b>5</b>	<b>Vlastní práce</b>	<b>27</b>
5.1	Metodika .....	27

5.2	Použitý hardware .....	29
5.3	Lokalita.....	30
5.4	Nastavení programů.....	30
5.4.1	Iperf .....	30
5.4.2	hrPing.....	31
5.5	Výsledky měření všech standardů v domácích podmínkách .....	32
5.6	Výsledky měření vybraných norem ve venkovních podmínkách.....	35
5.6.1	Porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik) .....	35
5.6.2	Porovnání standardu 802.11n NV2 (MikroTik) a 802.11n AirMAX (UBNT) 37	
5.6.3	Porovnání TDMA protokolu AirMAX (ON/OFF) u zařízení UBNT.....	38
5.6.4	Porovnání TDMA protokolu NV2 (ON/OFF) u zařízení MikroTik.....	39
5.6.5	Porovnání nastavení TDMA protokolu (1 ms/2 ms) u zařízení MikroTik.....	40
5.6.6	Porovnání prohození přístupového bodu a klienta (Mikrotik i UBNT)42	
5.6.7	Porovnání funkce Aggregation (ON/OFF) u zařízení UBNT .....	44
<b>6</b>	<b>Závěr</b>	<b>45</b>
6.1	Cenové a praktické srovnání.....	46
6.2	Praktický přínos.....	47
<b>7</b>	<b>Literatura</b>	<b>48</b>
<b>A</b>	<b>Výstup ze skenování dostupných bezdrátových stanic v okolí spoje</b>	<b>52</b>
<b>B</b>	<b>Výstup z měření v domácích podmínkách, standard 802.11n (MikroTik), NV2, TDMA 2 ms, TCP upload</b>	<b>53</b>
<b>C</b>	<b>Výstup z měření v domácích podmínkách, standard 802.11n (MikroTik), NV2, TDMA 2 ms, TCP download</b>	<b>54</b>
<b>D</b>	<b>Zdrojová data pro jednotlivé grafy</b>	<b>55</b>

## Seznam obrázků

Obr. 1	Možnosti kombinací šířky pásma a počtu antén. Zdroj: Blegen, 2013.	16
Obr. 2	Kombinace vysílání dvou stanic na stejném kanálu. Zdroj: Gast, 2005.	17
Obr. 3	Fresnelova zóna Zdroj: Lammler, 2010.	18
Obr. 4	Znázornění funkce Ubiquiti TDMA protokolu. Zdroj: Ubiquiti, 2014a.	21
Obr. 5	Přenosová rychlost při různých nastavení mechanismu RTS/CTS Zdroj: Michalina, 2014.	26
Obr. 6	Průběh spojení s různou prioritou WMM. Zdroj: Michalina, 2014.	26
Obr. 7	Hardwarové zapojení pro všechny testy.	27
Obr. 8	Umístění bezdrátového spoje. Zdroj: Mapy.cz, 2014.	30
Obr. 9	Srovnání jednotlivých standardů a technologií při měření v domácích podmínkách.	33
Obr. 10	Porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik)	36
Obr. 11	Porovnání zařízení firmy MikroTik a UBNT na standardu 802.11n s TDMA.	37
Obr. 12	Porovnání UBNT 802.11n se zapnutou a vypnutou funkcí AirMAX.	39
Obr. 13	Porovnání MikroTik 802.11n se zapnutou a vypnutou funkcí NV2.	39
Obr. 14	Porovnání MikroTik 802.11n s TDMA 1 ms a 2 ms.	41
Obr. 15	Porovnání MikroTik 802.11n NV2 při prohození přístupového bodu a klienta.	42
Obr. 16	Porovnání UBNT 802.11n AirMAX při prohození přístupového bodu a klienta.	43
Obr. 17	Porovnání UBNT 802.11n se zapnutou a vypnutou funkcí Aggregation.	44

## Seznam tabulek

Tab. 1	Maximální povolený vysílací výkon v české republice.	16
Tab. 2	Vliv připojené stanice 802.11b na přenosovou rychlost	23
Tab. 3	Jednotlivé standardy a technologie použité při měření.	33
Tab. 4	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při domácím (indoor) měření.	34
Tab. 5	Konfigurace jednotlivých testů.	35
Tab. 6	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik)	36
Tab. 7	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání zařízení firmy MikroTik a UBNT na standardu 802.11n s TDMA	38
Tab. 8	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání TDMA protokolu AirMAX (ON/OFF) u zařízení UBNT.	38
Tab. 9	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání TDMA protokolu NV2 (ON/OFF) u zařízení MikroTik	40
Tab. 10	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání MikroTik 802.11n s TDMA 1 ms a 2 ms. 41	
Tab. 11	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání MikroTik 802.11n NV2 při prohození přístupového bodu a klienta.	43
Tab. 12	Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání UBNT 802.11n AirMAX při prohození přístupového bodu a klienta.	44

# 1 Úvod a cíl práce

## 1.1 Úvod

V současné době existuje na trhu nepřeberné množství zařízení, které jsou primárně určeny pro bezdrátové spoje bod-bod, nebo pro připojení více zařízení k jednomu přístupovému bodu, tedy typu bod-multibod. Lze si vybrat z více standardů, technologií i výrobců. Také existuje více poskytovatelů bezdrátového připojení nebo domácností využívajících tuto technologii ke sdílení dat, kterým zpravidla nestačí omezené množství bezlicenčních kanálů. Nastává tak situace, kdy na jednom kanálu vysílá více zařízení a vzniká interference, neboli rušení. Je tedy nutné využívat nejkvalitnější hardware a optimální konfigurace bezdrátových zařízení, aby nedocházelo k rušení ostatních stanic a ke snižování propustnosti daných spojů.

## 1.2 Cíl práce

Cílem této práce je vybrat z mnoha možností (parametrů) bezdrátového přenosu (srovnáním v domácích nezarušených podmínkách) tu optimální a ověřit ji praktickým použitím ve venkovních podmínkách a dále optimalizovat. Jedná se o spoje používané menšími poskytovateli internetového připojení na bezlicenčním pásmu 2,4 GHz a 5 GHz. Dále budou porovnána dvě různá zařízení od různých výrobců, kteří mimo oficiální standardy používají i své proprietární technologie.

## 2 Bezdrátový přenos

### 2.1 Jednotlivé standardy

#### 2.1.1 IEEE 802.11b

Standard 802.11b, který byl vydán v roce 1999, je definován v pásmu 2,4 GHz. Komunikační kanál je široký 22 MHz a jsou pro něj definovány přenosové rychlosti 1; 2; 5,5 a 11 Mbit/s. Data jsou modulována pomocí komplementárního kódového klíčování CCK (Complementary Code Keying) a přenášena modulačním systémem HR-DSSS. Jelikož je povoleno bezlicenční pásmo šířky od 2 402 MHz do 2 482 MHz, šířka jednotlivého kanálu je 22 MHz a definováno je 13 kanálů. Jeden kanál se překrývá se dvěma sousedícími na každou stranu. Vyplývá tedy, že na jednom místě lze použít pouze tři kanály tak, aby se vzájemně nerušily. Možnosti jsou tedy 1;6;11, 2;7;12 nebo 3;8;13. V praxi (pro komerční použití) se ale běžně překrývají, někdy dokonce vysílají dvě stanice na stejném kanálu. Proto bylo nutné zpřístupnit další volné kanály (standard 802.11a). (IEEE, 2013)

#### 2.1.2 IEEE 802.11g

Standard 802.11g, který byl vydán v roce 2003, je definován v pásmu 2,4 GHz. Komunikační kanál je široký stejně jako u standardu 802.11b, a to 22 MHz. Použité modulační schéma je OFDM pro rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s, přičemž pro rychlosti 1; 2; 5,5 a 11 Mbit/s je použito stejné schéma jako u standardu 802.11b. Rychlosti se automaticky mění na základě síly přijímaného signálu. Rozmístění kanálů je také stejné jako u standardu IEEE 802.11b. (IEEE, 2013)

#### 2.1.3 IEEE 802.11a

802.11a je standard fyzické vrstvy pro síť WLAN v rádiovém pásmu 5 GHz. Maximální rychlost (data rate) je 54 Mbit/s na kanál. Větší počet kanálů než standard 802.11b/g, které se nepřekrývají (konkrétně 11 kanálů o šířce 20 MHz, povolených platnou legislativou v české republice, viz kapitola 2.2), poskytuje lepší ochranu proti možnému rušení od stanic na vedlejších kanále a vyšší datovou propustnost. Standard byl dokončen v roce 1999 (Ergen, 2002)

#### 2.1.4 IEEE 802.11n

Klíčovým požadavkem, který vede k vývoji normy 802.11n, je schopnost minimální propustnosti 100Mbit/s na MAC (L2) vrstvě s ohledem na to, že reálné propustnosti norem 802.11a/g jsou 25Mbit/s (při data-rate 54Mbit/s). Tento požadavek tak určuje alespoň 4krát vyšší propustnost.

Definováním požadavku propustnosti na MAC vrstvě spíše než datové rychlosti (data-rate) jsou vývojáři nuceni zvládnout obtížný problém, a to zlepšení účinnosti MAC vrstvy. Neschopnost dosáhnout propustnosti 100 Mbit/s si vyžádala podstatné zlepšení MAC vrstvy.

Pro zvýšení data rate se u standardu 802.11n používají dva základní koncepty:

- Použití šířky pásma 40 MHz.
- Použití MIMO technologie (Multiple Input Multiple Output).

Zvýšením z jednoho prostorového toku (jedna anténa na každé straně) na 4 (4 antény na každé straně) se zvyšuje data rate čtyřikrát. Termín prostorový tok (spatial stream) je definován 802.11n standardem jako jeden z několika bitových proudů, které jsou předávány přes více prostorových dimenzí, založených použitím více antén na obou stranách.

Vzhledem k rostoucím nákladům při zvyšování počtu antén jsou režimy používající 3 a 4 antény volitelné. Volitelnost použití šířky kanálu 40 MHz a 20 MHz je povinná z důvodu zajištění interoperability. Nicméně režim s šířkou kanálu 40 MHz se stal základní funkcí vzhledem k nízkým výrobním nákladům, kdy se rychlost zdvojnásobí. (Perahia, 2008)

Počet souběžných datových proudů je omezen minimálním počtem antén na obou stranách spoje. Jednotlivá zařízení dále omezují počet prostorových proudů, které mohou nést jedinečná data.

$A \times b : c$  zápis pomáhá zjistit, čeho je dané zařízení schopno. První číslo (a), je maximální počet vysílacích antén nebo TX RF řetězců, které mohou být použity pomocí zařízení. Druhé číslo (b), je maximální počet přijímacích antén nebo RX RF řetězců, které mohou být použity pomocí zařízení. Třetí číslo (c) je maximální počet datových prostorových toků, které umí zařízení využít. Například zařízení, které může odesílat na dvou anténách a přijímat na třech, ale může pouze odesílat a přijímat dva datové toky by bylo  $2 \times 3 : 2$ .

Standard 802.11n draft umožňuje až  $4 \times 4 : 4$ . Běžné konfigurace 802.11n zařízení jsou  $2 \times 2 : 2$ ,  $2 \times 3 : 2$  a  $3 \times 2 : 2$ . Všechny tři konfigurace mají stejnou maximální propustnost a funkce. Liší se pouze v kombinacích jednotlivých antén. (Intel, 2014)

### 2.1.5 IEEE 802.11ac

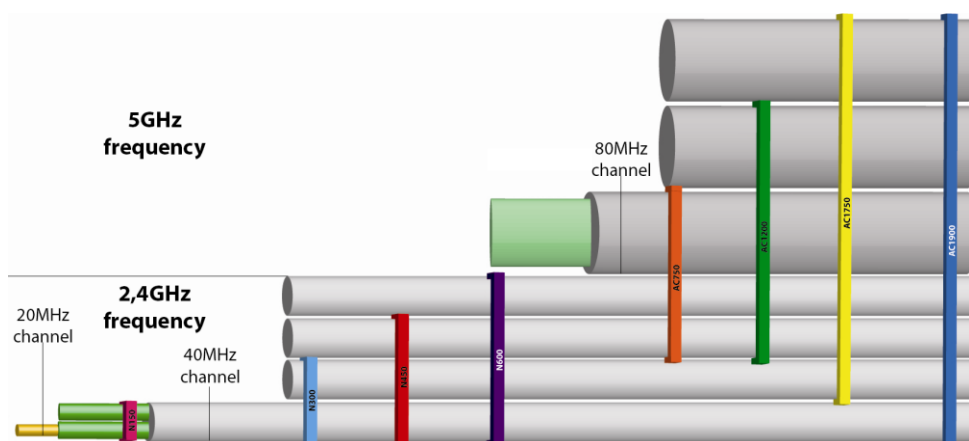
Standard 802.11ac vylepšuje technologické inovace standardu 802.11n s významnými pokroky v kódování, využitím multikanálového a MIMO provozu.

Standard 802.11n podporuje maximálně čtyři prostorové proudy, zatímco standard 802.11ac podporuje dvojnásobek, až osm prostorových proudů. Standard 802.11n je omezen na maximální šířku kanálu 40 MHz, zatímco 802.11ac umožňuje šířku kanálu 80 MHz a 160 MHz.

V závislosti na schopnosti přístupového bodu nebo routeru existuje více variací standardu 802.11ac. V současné době existují zařízení, která jsou označena podle maximální teoretické propustnosti 433 Mbit/s, 650 Mbit/s, 867 Mbit/s a 1 300 Mbit/s. Zařízení s maximální teoretickou propustností 867 Mbit/s využívají dvou prostorových proudů a šířku kanálu 80 MHz. Zařízení s maximální teoretickou propustností 1300 Mbit/s využívají tři prostorové proudy a šířku kanálu také 80 MHz.

Ve vývoji jsou i zařízení podporující čtyři prostorové proudy (1 733 Mbit/s) a případně s šířkou kanálu 160 MHz pro dosažení rychlosti až 3 466 Mbit/s. Technická specifikace počítá ještě s osmi prostorovými proudy, kde rychlost dosahuje až 6 930 Mbit/s. Reálná rychlost se však o teoretické velmi liší. (Blegen, 2013)

Kombinace více antén a šířek pásma ilustruje obrázek č. 1. Při kombinaci všech čtyř prostorových proudů na frekvenci 2,4 GHz s šířkou pásma 40 MHz lze dosáhnout maximální teoretické rychlosti 600 Mbit/s (označení N600). Postupným přidáváním prostorových proudů na frekvenci 5 GHz se šířkou pásma 80 MHz lze při kombinaci čtyř proudů na frekvenci 2,4 GHz a tří proudů na frekvenci 5 GHz dosáhnout maximální teoretické rychlosti 1 900 Mbit/s (označení AC1900).



Obr. 1 Možnosti kombinací šířky pásma a počtu antén.  
Zdroj: Blegen, 2013.

## 2.2 Maximální povolené vysílací výkony

Výrobce/distributor zařízení je povinen v návodu k použití, který musí být v češtině přiložen ke každému zařízení uvést podmínky, za nichž lze zařízení v ČR provozovat v souladu se všeobecným oprávněním č. VO-R/12/09.2010-12. Zejména musí výrobce/distributor uvést, jaký druh nebo typ antény může být u zařízení použit, aby zařízení splňovalo podmínky, za nichž byla posouzena shoda. Provozovatel rádiového zařízení je povinen na základě těchto informací výrobce dodržovat režim vysílání, který odpovídá výše uvedenému všeobecnému oprávnění. Obecně platí, že při použití směrové antény (pokud výrobce/distributor tento druh antény připouští) musí provozovatel snížit výkon zařízení tak, aby vyzářený výkon byl v souladu s všeobecným oprávněním. Maximální povolené vysílací výkony jsou uvedeny v tabulce číslo 1. (ČTÚ, 2014)

Tab. 1 Maximální povolený vysílací výkon v české republice.

Kmitočtové pásmo	Max. povolený výkon	Další podmínky
2400 – 2483,5 MHz	100 mW e.i.r.p.	
5150 – 5250 MHz	200 mW střední e.i.r.p.	Pouze uvnitř budov
5250 – 5350 MHz	200 mW střední e.i.r.p.	Pouze uvnitř budov
5470 – 5725 MHz	1000 mW střední e.i.r.p.	

Zdroj: ČTÚ, 2010.



## 2.3 DSSS

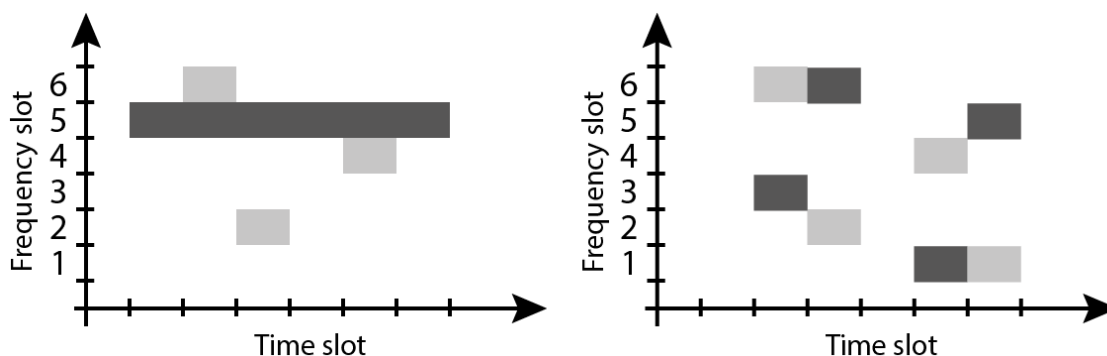
Standard 802.11b využívá modulační metodu DSSS (direct sequence spread spectrum). Technika rozprostření spektra využívá přístup modulace, kde je využita mnohem větší šířka pásma, než je nutné pro přenos konkrétních dat.

Každý bit je nahrazen (rozprostřen) takzvaným „chipem“, což je konkrétní osmibitová kombinace jedniček a nul. Tato modulace má schopnost pracovat i v podmínkách nízkého poměru signálu k šumu (SNR). To má za následek větší odolnost proti rušení. Charakteristickým rysem těchto kódů je, že i když by přijímači chybělo několik bitů, bude stále schopen určit, jestli byl „chip“ zamýšlen jako 1 nebo 0. Pokud by tedy existovalo rušení, mohl by přenos dat fungovat bez ztráty dat nebo snížení propustnosti. (Dafne Di Rocco, 2009)

## 2.4 FHSS

FHSS (frequency hopping spread spectrum) závisí na rychle se měnící frekvenci vysílače podle předem určeného vzoru.

Frekvenční přeskokování umožňuje, aby se zabránilo rušení od primárního uživatele přiřazeného na stejném frekvenčním pásmu. Mohou nastat dva případy, kdy v prvním případě primární stanice vysílá stále na stejné frekvenci (např. metodou DSSS) a sekundární stanice používá frekvenční přeskokování (obrázek č. 2, vlevo), nebo obě stanice vysílají metodou FHSS. V obou případech se stanice budou navzájem rušit jen zlomek vysílaného času. V druhém případě se ale stanice nemusí rušit vůbec, pokud zvolí vhodnou sekvenci přeskoků. Taková frekvence, kde se stanice nepřekrývají, se nazývá ortogonální (obrázek č. 2, vpravo). (Gast, 2005)



Obr. 2 Kombinace vysílání dvou stanic na stejném kanálu.  
Zdroj: Gast, 2005.

## 2.5 OFDM

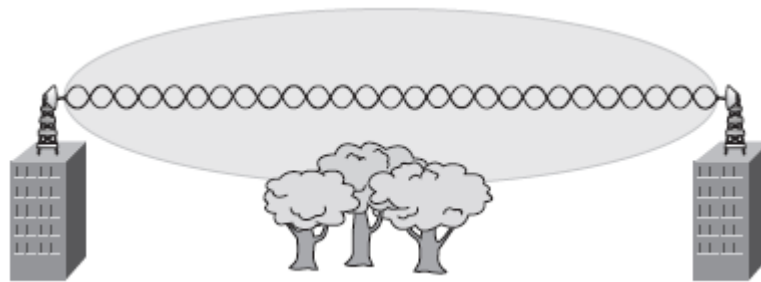
Modulační metoda OFDM (orthogonal frequency division multiplexing) spočívá v použití několika desítek až tisíců nosných kmitočtů. Nosné kmitočty jsou dále modulovány dle potřeby různě robustními modulacemi QPSK nebo M-QAM. Jed-

notlivé nosné kmitočty jsou vzájemně ortogonální (tj. jejich skalární součin je nulový), takže maximum každého nosného kmitočtu by se mělo překrývat s průchody nulou ostatních kmitočtů. Datový tok celého kanálu se tak dělí na stovky dílčích datových toků jednotlivých nosných kmitočtu. Tím, že ve výsledku jsou toky na jednotlivých nosných kmitočtech přenášeny relativně nízkou modulační rychlostí, je OFDM odolná vůči vícecestnému (multipath) šíření. Dále se využívá vkládání ochranného intervalu (času), kdy se nevysílá žádná nová informace. Na přijímací straně je tak možné nerušeně přijmout právě vysílaný symbol. OFDM se tedy vyznačuje vysokou odolností vůči interferencím. (Bumbálek, 2010)

Standardy 802.11a a 802.11g jsou založeny na OFDM modulaci. Standard 802.11n využívá MIMO technologii pro přenos více OFDM datových toků. (Gast, 2012)

## 2.6 Fresnelova zóna

Je elipticky tvarovaná oblast mezi vysílačem a přijímačem, která musí být alespoň ze šedesáti procent bez překážek, aby signál mohl být přijat správně. Na obrázku č. 3 je vidět, že i když existuje vizuální přímá viditelnost, existuje zde překážka v kruhové oblasti kolem středové osy signálu. (Lammle, 2010)



Obr. 3 Fresnelova zóna

Zdroj: Lammler, 2010.

## 2.7 SNR

SNR (Signal to noise ratio) je termín používaný k popisu, o kolik silnější je signál ve srovnání s okolním rušením, který signál kazí.

Pro pochopení předpokládejme, že budeme chodit po přeplněném parku s mnoha křičícími dětmi a mluvit normálním hlasem do telefonu. Je pravděpodobné, že šum bude vysoký a že osoba na druhém konci nebude schopna odlišit slova od hluku kolem, který je rovněž přenášen po telefonu. Pokud jsou tedy vnější vlivy příčinou příliš vysokého hluku, nemusí přijímače rozumět přenosu. (Carroll, 2008)

## 2.8 Hardware fragmentation threshold

Určuje maximální velikost fragmentu v bytech při přenosu přes bezdrátové médium. Standardní paketová fragmentace umožňuje pakety fragmentovat před vysláním přes Wi-Fi připojení pro získání větší pravděpodobnosti úspěšného přenosu (pouze fragmenty nepřenesené správně jsou znovu odeslány). Přenos paketu, kte-

rý je rozdělen na mnoho částí, je ale méně efektivní než odeslání nefragmentovaného balíčku, z důvodu vyšší režie a většího využití vysílacích zdrojů (pásma). (MikroTik, 2014)

## 2.9 Problematika skrytých uzlů

Standard 802.11 poskytuje prostředky k ochraně proti přenosu ostatních stanic pomocí RTS/CTS protokolu. Ochrana pomáhá zejména v boji proti takzvanému „problému skrytého uzlu“. Existuje několik typů ochrany:

- RTS/CTS ochrana – zařízení, které chce vysílat, nejprve pošle RequestToSend rámec a čeká na ClearToSend rámec ze zamýšleného místa určení. Rozpoznáním RTS nebo CTS rámce stanice ví, že někdo se chystá vysílat a tudíž nemají iniciovat přenos sami.
- CTS to self - ochrana založená na odeslání CTS rámce sama sobě. Stejně jako v protokolu RTS/CTS, každé 802.11 kompatibilní zařízení přijímá tento rámec a rozpozná, že nemá vysílat. CTS to self ochrana je založená na menší režii, ale je třeba vzít v úvahu, že tato metoda pouze chrání před zařízeními, která přijímají CTS rámec. (Například pokud existují 2 skryté stanice, není použití CTS to self ochrany možné. V tomto případě je nutné použít RTS/CTS ochrany, takže další stanice se o zákazu vysílání dozví od přístupového bodu.) (MikroTik, 2014)

## 2.10 WMM

WMM funguje tak, že veškerý provoz je rozdělen do čtyř kategorií (background, best effort, video, voice). QoS politika (rozdílná manipulace s různým typem dat) se aplikuje na přenášené pakety a vysílací zařízení zpracovává každý paket s jinou prioritou. V případě zahlcení kapacity přenosového média jsou pakety s nízkou prioritou zahozeny a pakety s vysokou prioritou dostávají přednost. (MikroTik, 2014b)

## 3 Použité technologie

### 3.1 MikroTik

MikroTik je lotyšská společnost, která byla založena v roce 1995 k rozvoji směrovačů a bezdrátových ISP (internet service provider) systémů. MikroTik nyní poskytuje hardware a software pro připojení k internetu ve většině zemí po celém světě.

Zkušenosti s využíváním průmyslových počítačů, hardware a kompletních systémů přispěly v roce 1997 k vytvoření vlastního operačního systému RouterOS, který poskytuje rozsáhlé ovládání, stabilitu a flexibilitu pro všechny druhy datových rozhraní a směrovačů. Primárně je systém určen pro jejich výroby, ale lze jej nahrát i na běžné počítače. V roce 2002 se firma rozhodla, že si vytvoří vlastní hardware, a tak vznikl výrobek nazvaný RouterBOARD, který se prodává ve všech státech světa. (MikroTik, 2014c)

Pro tuto práci jsou důležité zejména jejich proprietární protokoly Nstream a jeho novější verze NV2.

#### 3.1.1 Nstream

K této technologii lze nalézt jen velmi málo informací. MikroTik uvádí pouze tyto hlavní výhody. Funkce „Polling“ zkracuje časy přístupu k přenosovému médium, protože není třeba pokaždé zjišťovat, zda je přenosové médium volné, když je potřeba přenášet data. Nízké zatížení protokolu při přenosu každého rámce zvyšuje přenosovou rychlost. Neexistují implicitní limity pro délku spoje. Také neexistuje implicitní rychlostní omezení na spojích o velké vzdálenosti. (MikroTik, 2012a)

#### 3.1.2 NV2

Bezdrátový protokol založený na technologii TDMA (Time Division Multiple Access). TDMA je způsob sdíleného přístupu ke kanálu pro středně velké sítě. Technologie umožňuje více uživatelům sdílet stejný frekvenční kanál, který je rozdělený do různých časových úseků. Uživatelé mohou přenášet data v rychlém sledu, kdy každý využije svůj časový úsek. To umožňuje více stanicím sdílet stejné přenosové médium (např. kmítočtový kanál) při použití pouze části kapacity tohoto kanálu. TDMA řeší problém skrytého uzlu a zlepšuje využití přenosového kanálu, což má za důsledek zlepšení propustnosti a latence, a to zejména v sítích PtMP (point to multipoint). (MikroTik, 2012a)

### 3.2 Ubiquiti

Firma Ubiquiti, dále jen UBNT, byla založena v červnu roku 2005, aktuálně sídlí v Kalifornii, USA. Na českém trhu prorazila zejména s výrobky označenými Bullet, NanoStation, NanoStation Loco, PicoStation a RouterStation. V roce 2009 uvedla na trh výrobky s proprietární technologií AirMAX, které využívají TDMA protokol. V roce 2010 vydali řadu „M“, která využívá MIMO technologii. (Wispa, 2014)

Pro tuto práci je důležitý zejména jejich proprietární protokol AirMAX, nastavení RTS Threshold a použití agregace.

### 3.2.1 AirMAX

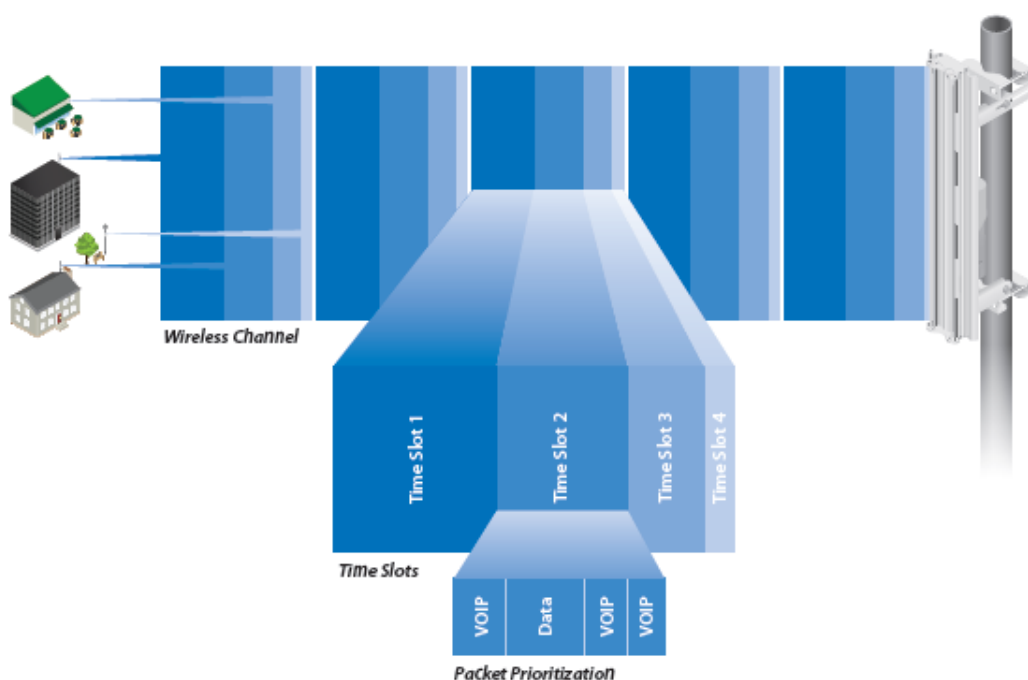
Mezi hlavní vlastnosti patří plánování časových slotů k eliminaci kolizí, maximalizace časové efektivity a přiřazení priorit pro přenos hlasu a videa (viz obrázek č. 4). Protokol TDMA (který technologie AirMAX využívá) dynamicky přiděluje čas pro aktivní klienty a poskytuje větší výkon a odolnost proti rušení ve srovnání s konvenčním 802.11 CSMA/CA. (Ubiquiti, 2014a)

### 3.2.2 RTS Treshold

Určuje, od jaké velikosti paketů je použita metoda RTS/CTS (více v kapitole 2.9) a pomáhá regulovat tok dat skrz přístupový bod. Rozsah je 0 - 2346 bytů. Defaultně je nastavená hodnota 2346, která znamená, že mechanismus RTS je vypnutý. (Ubiquiti, 2014b)

### 3.2.3 Aggregation

Jde o součást standardu 802.11n, která umožňuje zaslání více rámců dohromady při jediném přístupu k přenosovému médium. Větší rámce se vytváří tak, že se zkombinují menší rámce se stejným zdrojem, místem doručení a prioritou (QoS), do jednoho velkého rámce se společným MAC záhlavím. U této funkce lze nastavit počet rámců, které se mohou maximálně zkombinovat a maximální velikost výsledného rámce. (Ubiquiti, 2014b)



Obr. 4 Znázornění funkce Ubiquiti TDMA protokolu.  
Zdroj: Ubiquiti, 2014a.

## 4 Rešerše dostupných prací a odborných publikací

Jako zdroj prací a odborných publikací byl použit internetový portál Theses, kde byly vyhledávány práce s klíčovým slovem „802.11“ od roku 2010. Standard 802.11n byl sice schválen již v roce 2009, ale na trhu nebyly zařízení, které by byly výkonově ani softwarově optimalizované pro tento standard. Z nich byly následně vybrány práce, které se specializují přímo na výstavbu bezdrátových spojů.

Vyhledávání bylo také provedeno přes vyhledávací portál Google, kde klíčovými slovy bylo „wireless throughput“.

Dané téma se dá rozdělit na dílčí části z hlediska jednotlivých technologií, které budou v práci zkoumány. První, ze všech nejstarší je standard označovaný IEEE 802.11b. Informace o testování pouze tohoto standardu můžeme najít v práci LongDistance 802.11b Links: Performance Measurements and Experience (Chebrolu, Raman, Sen, 2006), kde autoři zkoumali zejména tyto faktory:

- Jak velká je ztrátovost paketů u spojů na velkou vzdálenost.
- Jak se liší síla přijímaného signálu.
- Zda existuje vztah mezi paketovou ztrátovostí a délkou spoje.
- Jaký vliv má velikost paketů a přenosová rychlost (modulace) na ztrátovost paketů.
- Jaký vliv má počasí (dešť, mlha) na výkon spoje.
- Jaký vliv na kvalitu má externí a interní rušení spoje.

Měření probíhalo na osmi různých spojkách, kde nejkratší měl délku 1 km a nejdelší 37 km. Spoje byly vytvořeny za použití vysoce výkonných směrových antén, které byly umístěny na střechách vysokých budov nebo anténních vysílačů. Bezdrátové karty byly použity Senao 2511CD plus ext2 PCMCIA, ke kterým byly pomocí pigtail kabelů připojeny antény. Tyto kabely však dosahovaly délek až 45 m, což není z hlediska útlumu kabelu optimální. Závěry z měření:

- Ztrátovost paketů záleží zejména na SNR (viz kapitola 2.7). Existuje okno SNR o velikosti 4 až 6 dB, pod které je chybovost téměř 100% a nad ním je chybovost do jednotek procent.
- Ztrátovost paketů není přímo závislá na délce spoje, ale pouze na přijímané SNR.
- Vliv velikosti paketů na ztrátovost je patrný, ale není významný.
- Je zde určitá závislost ztrátovosti paketů na použité modulaci (data-rate). Závislost naznačuje robustní algoritmus založený na SNR přijímače.
- Na jednom spoji (5 km) byl sledován vliv mlhy a deště, který měl negativní vliv.
- Veškeré vnější vlivy na tyto spoje škodí výkonu.
- Provoz na tzv. nerušících se kanálech (1 a 6 nebo 1 a 11) má pouze drobné rozdíly.

- Jevy jako rušení jiné antény v blízkosti a únik signálu na konektorech mají vliv na sílu přijímaného signálu.

Ve shrnutí je také uvedeno, že bezdrátové spoje na této technologii jde docela dobře dimenzovat na patřičný výkon (přenosovou rychlost). Každý zásah v rámci sítě nebo ze sousedních sítí může způsobit drastické snížení výkonu. Interference může nastat i mezi sousedními spoji. Tato studie je sice zaměřená pouze na testování standardu IEEE 802.11b, ale vzhledem k podobným vlastnostem standardů IEEE 802.11b a IEEE 802.11g předpokládá, že mnoho závěrů bude stejných pro oba standardy.

Dalšími standardy IEEE 802.11b a IEEE 802.11g se zabývá diplomová práce s názvem *Problematika vysokého zatížení bezdrátových sítí standardu 802.11b/g* (Šlinz, 2012). V první části této práce se zkoumá vliv na přenosovou rychlost při připojování více zařízení, které používají tyto dva různé standardy. Měřeny byly tyto 3 stavy:

- připojený klient v „b“ normě je pouze připojen s minimální aktivitou (1).
- připojený klient v „b“ normě provádí přenosy se stejnou intenzitou jako ostatní klienti připojení k přístupovému bodu (2).
- připojený klient v „b“ normě provádí přenosy v plné, jemu dostupné šířce přenosového pásma (3).

Tab. 2 Vliv připojené stanice 802.11b na přenosovou rychlost

Vytížení stanic 802.11b	Maximální rychlost v Mbit/s
1	10,6
2	7,32
3	6,2

Zdroj: Šlinz, 2012.

Výsledky měření jsou zaznamenány v tabulce číslo 2. Závěrem je zde dodáno, že při velmi nízkém zatížení klienty využívající zařízení standardu 802.11b dojde k neúměrnému snížení kapacity přístupového bodu, i když není přenos narušován častými kolizemi se zařízeními používajícími standard 802.11g. Při stejnoměrném nebo vysokém využití kapacity zařízeními používajícími standard 802.11b dochází k přiblížení přenosové rychlosti standardu 802.11b. Je to způsobeno tím, že hlavní složkou přenosu je preamble každého rámce přenášená na rychlosti nejvýše 2 Mbit/s, a to i u zařízení podporujících vyšší data-rate. Následná doba přenosu uživatelských dat u rychlých zařízení tvoří pouze 26 % z celkového času přenosu včetně režijních nákladů. Vypnutím této ochrany lze získat přenosovou kapacitu běžnou pro standard 802.11a a zachovat možnost přenosu i pro starší zařízení. Zařízení standardu 802.11g zvládají v režimu b/g dekodovat data vyslaná starším klientem a prodloužit si NAV vektor (vnitřní proměnná, která na MAC vrstvě udržuje informaci o době přenosu a udržování této informace každou stanicí) o odpovídající čas. Tato vlastnost však není dostupná pro klienty 802.11b, kteří detekují rámce modulované OFDM pouze jako jistou úroveň energie v kanále a odkládají vysílání o náhodný čas.

Celá práce je zakončená simulací, ve které je v programu OPNET Modeler v. 14.5 nasimulována situace, kde jsou 3 druhy klientů (http\_browse, http\_heavy\_load a ftp\_download), kteří mají přesně nastaveno jaké objemy a jak často stahovat (přenášet). Pro http přenos je zde zohledněna i průměrná velikost www stránek. Stanice jsou rozmístěny náhodně v místnosti 50×50 metrů a žádná z nich se během testu nepohybuje. Test se skládal ze dvou částí, kdy jednou byly „stahovači“ a „brouzdaři“ ve srovnatelných podmínkách. Podruhé byl jeden „stahovač“ namodelován do nevýhodné pozice (co se týče kvality přijímaného signálu) a byl tak spárován pouze při rychlosti 6 Mbit/s. Výsledek byl reprezentován takto:

- Při zamezení připojení 802.11b stanice je přenosová rychlost nejrychlejší.
- Při použití algoritmu CTS-to-self (viz kapitola 2.9) je rychlost poloviční.
- Při vysílání pouze standardem 802.11b se rychlost oproti předchozímu případu opět o polovinu sníží a přiblíží se maximální teoretické přenosové rychlosti tohoto standardu.
- Pokud jde o případ, kdy je k síti připojen „stahovač s nevýhodnou pozicí“, ve všech třech variantách se rychlost sníží přibližně o 15 %.

V diplomové práci (Skipala, 2011) se autor zabývá standardem 802.11a. První část je zaměřená na velikost latence při přenosu. Latence je zde testována při různých rychlostech přenosu na bezdrátovém spoji. Naměřené hodnoty ukazují, že blíží-li se rychlost přenosu maximální propustnosti spoje, začíná se to projevovat na zvyšující se latenci. Autor z tohoto měření vyvozuje, že by se mohlo zdát, že odezva spoje roste s množstvím dat, která jsou přes spoj přenášena. Ve skutečnosti spoj jako takový pracuje stále s odezvou 1ms. To, co způsobuje zpoždění, jsou však fronty, které nejsou správně řízeny. Po optimalizaci řízených front se latence snížila i při rychlosti blízké se maximální propustnosti. Při dosažení rychlosti maximální propustnosti se odezva opět zvyšuje. Tuto problematiku autor nadále zkoumá a vysvětluje pomocí tzv. hardwarových front.

Neméně důležitou částí práce je zkoumání vlivu provozu na stejné frekvenci. Z prováděných testů je vidět, že klíčovou roli v degradaci výkonu systému hraje problém skrytého uzlu a nepoužívání mechanismu RTS/CTS. Autor však upozorňuje, že na druhou stranu RTS/CTS může být i nežádoucí faktor pro sítě, které jsou od sebe více vzdálené (všechny stanice i přístupové body jsou od sebe třeba několik kilometrů). Pokud se zařízení slyší navzájem a vysílají-li obě na modulační rychlosti 54 Mbit/s, pak dosažitelné maximum média je 30 Mbit/s, a proto každá stanice bude vysílat průměrnou rychlostí 15 Mbit/s. Tato rychlost bude lehce snížena o čas strávený náhodným čekáním, kdy testy ukázaly rychlost obou stanic okolo 14,5 Mbit/s.

Další příčinou rušení je provoz na přilehlém kanálu (vedlejší frekvenci). Zde autor uvádí důležitý faktor SIR, poměr signálu k rušení (S/I nebo SIR), také známý jako poměr nosné frekvence k rušení (C/I nebo CIR), je podíl mezi průměrem obdržené modulované nosné síly S nebo C a průměrnou přijatou výkonovou mezikanálovou interferencí I, tj. přeslechů od jiných vysílačů.

Také upozorňuje, že mezi provozem na stejné frekvenci a provozem na vedlejší frekvenci je velký rozdíl. Při provozu na stejné frekvenci se stanice snaží sdílet pásmo (ať už zažívají problém skrytého uzlu, či ne), zatímco při provozu na vedlejší frekvenci nedochází ke sdílení pásma. Signál, který z vedlejšího kanálu proniká,



je čistě šumového charakteru a nelze z něj vyčíst žádnou informaci (při provozu na stejném kanálu lze bez problému dekodovat PLCP hlavičku).

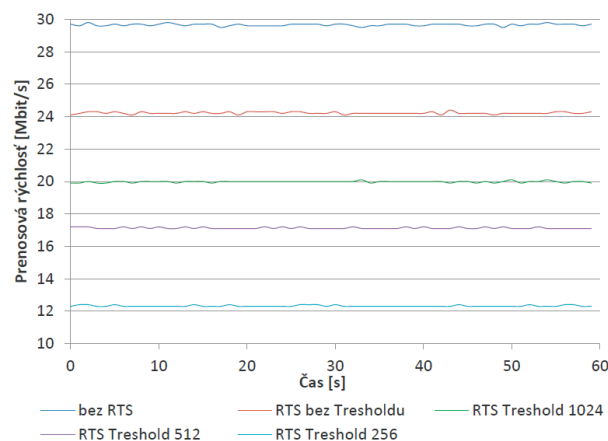
Bakalářská práce Spojení „poslední míle“ na bázi technologie IEEE 802.11 (Buzek, 2010) popisuje možnosti přenosů využívajících frekvenci 10 GHz a 26 GHz. Popisuje také parametry všech dostupných zařízení pro spojení na této frekvenci i jednotek (zejména klientských) na frekvenci 5 GHz. V této práci nejsou provedeny žádné praktické testy pro porovnání jednotlivých zařízení nebo standardů.

Bakalářská práce Reálná propustnost zařízení pracujících na standardu 802.11n (Vágner, 2011), zkoumá propustnost standardu 802.11n se zařízeními MikroTik RB711, Ubiquiti Bullet M5 (pro MIMO 1×1) a MikroTik RB493 s kartami R52n-M, MikroTik RBSXT (pro MIMO 2×2). Při testech jsou také využity proprietární protokoly nstream, nv2, Airmax či metoda agregace. Obsahem této práce jsou také testy propustnosti při šířce kanálu 40 MHz, který se pro venkovní spojení z důvodu platné legislativy nepoužívá.

Autor uvádí, že testy byly provedeny programem iperf, spuštěným na linuxové distribuci debian s generováním TCP přenosu. V této práci jsou testy propustnosti jednotek MikroTik SXT nad hranicí 100 Mbit/s, což je vzhledem k neexistenci těchto jednotek s gigabitovým portem do března roku 2012 (MikroTik, 2014d) zcela zavádějící údaj. Pokud byly testy prováděny pomocí integrovaného testu propustnosti společnosti MikroTik (Btest), byly jednotky neúměrně zatíženy tímto generováním, což mohlo zkreslit výsledky (laboratorně ověřeno u výkonnějších jednotek MikroTik RB912).

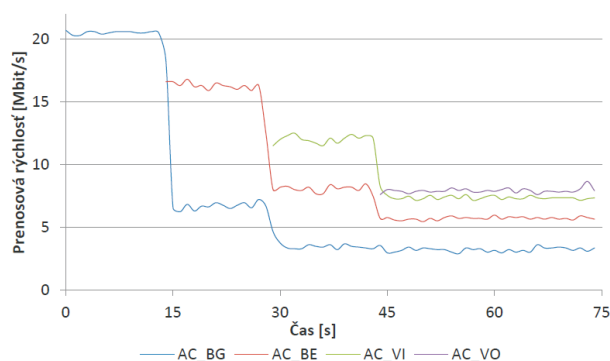
Nejnovější bakalářská práce, která má také nejblíže k tomuto tématu se jmenuje Optimalizace PtMP spojení ve WLAN 802.11a,n na platformě MikroTik (Michalina, 2014). V této práci autor provádí optimalizaci parametrů, které jsou důležité pro nejefektivnější využití přenosové rychlosti u spojů bod-multibod, kde se zpravidla na jeden přístupový bod připojuje více klientských stanic (koncových zákazníků přístupu k síti internet).

Pro optimalizaci byly v této práci zvoleny dva hlavní parametry. Jednalo se o změnu nastavení RTS/CTS a služby WMM (viz kapitola 2.9 a 2.10). Testování přenosové rychlosti při změně parametrů RTS/CTS jsou zaznačeny na obrázku číslo 5. Autor k tomuto výsledku dodává, že už jen zapnutím tohoto mechanismu rychlost výrazně klesá. Nastavením nejnižší hodnoty klesla rychlost oproti vypnutému mechanismu až o 60 %. Dále dodává, že nastavení takto nízké hodnoty RTS Threshold je vhodné pouze při velmi zarušených podmínkách.



Obr. 5 Přenosová rychlost při různých nastavení mechanismu RTS/CTS  
Zdroj: Michalina, 2014.

Autor také testoval použití WMM mechanismu, kde postupně po patnácti vteřinách zahajoval přenosy různých priorit. Nejprve přenos s nejnižší prioritou a naposledy s nejvyšší prioritou. Chování tohoto mechanismu zobrazuje obrázek č. 6. Je z něj zřejmé, že přenos s vyšší prioritou má přednost před přenosem s nižší prioritou. Spojené bod-bod mohou tohoto mechanismu využít pouze tak, že pakety označené vyšší prioritou vyřídí přednostně, aby nedocházelo ke zvyšování latencí, například u VoIP volání, na úkor stahování dat nebo prohlížení webových stránek.



Obr. 6 Průběh spojení s různou prioritou WMM.  
Zdroj: Michalina, 2014.

Při analýze bylo zjištěno, že neexistuje práce, která by se zabývala srovnáním rychlostí jednotlivých standardů na stejném hardware, aby byl test co nejobektivnější. Velkou roli hraje i vývoj daných norem a technologií, kde výrobci vydávají každý rok několik nových zařízení a firmware pro tato zařízení aby zvýšili jejich propustnost. Další možností je použití nové technologie na starý standard (NV2 na 802.11g), což bude také obsahem testování. Aktuální testy propustnosti na svém webu neuvádí ani firma MikroTik. Lze však nalézt uživatelské testy na jejich oficiálním fóru. Většinou však u těchto testů nejsou zveřejněné nastavené parametry.

V žádné práci nejsou uvedeny konkrétní parametry programů, které byly použity pro testování.

## 5 Vlastní práce

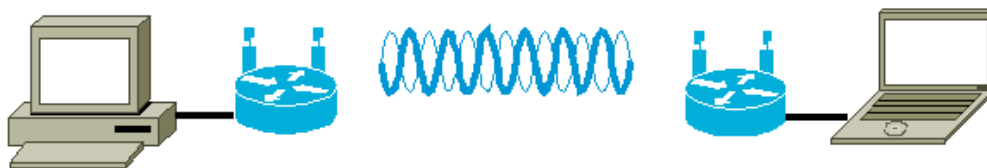
### 5.1 Metodika

Měření je rozděleno na dvě hlavní části. První část vlastní práce je zaměřena na výběr vhodné technologie v domácích (indoor) podmínkách (zařízení ve vzdálenosti dva metry od sebe s přímou viditelností, bez interference) a druhá část na testování technologie ve venkovních podmínkách (test ostrého nasazení). Více informací o umístění zařízení při testování je v kapitole 5.3.

Obě části budou testovány se stejným hardware a software, aby testy byly co nejobektivnější. Výjimku tvoří antény u technologie MikroTik, kde v domácích podmínkách budou použity 2dBi dipólové<sup>1</sup> antény. U přístupových bodů NanoBeam nejsou antény demontovatelné.

Přenos dat (generování a přijímání) bude probíhat přímo mezi dvěma počítači, aby nebyly nijak ovlivněny, zejména výkonově, přístupové body zajišťující přenos. Schéma zapojení je zobrazeno na obrázku číslo 7. Adresace sítě bude nastavena v rozsahu 192.168.0.0/24 bez směrování na přístupových bodech.

Vysílací výkon bude v domácích podmínkách nastaven na 10 dBm a ve venkovních podmínkách na 27 dBm (viz kapitola 2.2).



Obr. 7 Hardwarové zapojení pro všechny testy.

Samotné testování každé konfigurace spoje bude vždy rozděleno na 3 části:

1. Generování UDP dat (UDP přenos mezi PC1 a PC2) bude zajištěno pomocí programu iperf, který bude spuštěn souběžně s příkazem ping. Testování bude trvat 60 vteřin, kdy 30 vteřin se budou data odesílat (Upload) a 30 vteřin se budou data přijímat (Download). Výstupem z programu iperf je průměrná rychlost a množství přenesených dat každou vteřinu přenosu, průměrná rychlost a množství přenesených dat za prvních 30 vteřin a následně za druhých 30 vteřin. Z průměrných rychlostí za každou vteřinu lze vypočítat směrodatnou odchylku, která bude hlavním ukazatelem stability přenosu.

Souběžně s generováním dat bude spuštěn příkaz ping, který bude každou vteřinu odesílat požadavek ICMP Echo Request a bude změřena doba mezi přijmutím ICMP Echo Reply pro analýzu chybovosti spoje. Výstupem z příkazu ping je odezva za jednotlivé vteřiny přenosu, průměrná odezva za celý přenos,

---

<sup>1</sup> Dipólová anténa je nejjednodušším typem rádiové antény, skládající se z vodivého drátu, který je poloviční délky k maximální vlnové délce, kterou má anténa generovat. Tento drát je rozdělen v polovinu a obě části jsou od sebe odděleny izolátorem. (Janssen, 2014)

minimální odezva, maximální odezva, počet ztracených paketů a průměrná ztrátovost. Pro účely této práce bude stačit průměrná odezva.

2. Stejný test jako v bodu jedna, pouze pro přenos dat na TCP protokolu.
3. Třetím testem bude samostatný ping, kdy ICMP Echo Request bude odeslán každých pět milisekund, pomocí programu hrPing. Tento požadavek bude mít danou velikost šedesát bytů. Výstupem bude minimální odezva, maximální odezva, průměrná odezva, počet ztracených paketů a průměrná ztrátovost.

Při těchto testech nebudou data analyzována na úrovni odchyty paketů, protože použitím programu pro odchyt dochází ke snižování propustnosti mezi jednotlivými počítači a ke zhoršování odezvy při přenosu (předem laboratorně ověřeno). Při testech také nebude použito žádné šifrování přenosu dat.

Ovládání počítače na vzdálené straně bude probíhat pomocí VNC (Virtual Network Computing). Konkrétně pomocí programu VNC REAL. Na vzdáleném počítači bude spuštěn VNC server a pomocí VNC klienta se na něj bude připojovat, pokud na něm budou potřeba provést změny v nastavení nebo zjištění výsledků. V průběhu testů bude VNC klient odpojený, aby přenos přes síť nezkresloval výsledky.

Při testování v domácích podmínkách se budou testovat tyto standardy a technologie:

- Jednotlivé standardy 802.11b/g/a/n.
- Zařízení firmy Ubiquiti a MikroTik.
- Použití technologie nstream, NV2 (MikroTik) a AirMAX (Ubiquiti).

Pro testování ve venkovních podmínkách budou zvoleny pouze dva nejrychlejší standardy (největší propustnost). Před samotným testováním bude proveden scan všech sítí, vysílajících na celém bezlicenčním pásmu pro pozdější porovnání výsledků a výběru vhodných kanálů. Některé testy budou provedeny pouze u vybraných konfigurací a na nejvhodnějších kanálech. Při testování ve venkovních podmínkách se budou měnit tyto parametry:

- Vysílací frekvence (kanál). Pouze při venkovním testování.
- Prohození přístupového bodu a klienta. Pouze u vybraných konfigurací.
- Zapnutí/vypnutí NV2 protokolu u zařízení MikroTik.
- Změna parametru TDMA period size u MikroTiku při zapnutém NV2.
- Zapnutí/vypnutí Aggregation u UBNT NanoBeam.
- Zapnutí/vypnutí AirMAX technologie u UBNT NanoBeam.

Funkce WMM bude vždy zapnutá, ale nemá žádný vliv na výsledky, protože počítače, které budou generovat provoz, nebudou tyto data označovat podle priorit.

Protože se bude jednat o spoj o dvou zařízeních (přístupový bod a klient), nemá smysl zapínat ochranu před skrytými uzly.

## 5.2 Použitý hardware

K měření byl použit notebook Acer Aspire 5536 (AMD Turion X2 Dual-Core RM75 s frekvencí 2,2 GHz, 3 GB RAM, 64bitový operační systém Windows 7, 1Gbit LAN) a stolní počítač (Intel Core 2 Duo 3,2 GHz, 4GB RAM, 64bitový operační systém Windows 7, 1Gbit LAN).

Pro měření standardu 802.11b, 802.11g a 802.11a byla použita konfigurace MikroTik RB433 jako přístupový bod a MikroTik RB411 jako klientská stanice.

Pro měření standardu 802.11a (z důvodu porovnání stejného standardu na různém hardware od stejného výrobce) a 802.11n byla použita konfigurace 2krát MikroTik RB912UAG.

Pro měření standardu 802.11n (z důvodu porovnání stejného standardu na hardware různých výrobců) byla použita konfigurace 2krát UBNT NanoBeam M5.

Popis jednotlivých zařízení:

- MikroTik RB433, 64 MB RAM, 300 MHz, 3krát miniPCI, 3krát LAN, vč. L4. K němu bezdrátová karta MikroTik R52Hn miniPCI 802.11n, Atheros AR9220 (2,4/5 GHz, 25 dBm). Jako vysílací anténa byla použita 2dBi dipólová anténa spojená s bezdrátovou kartou pigtailem MMCX male/RSMA female o délce 30 cm.
- MikroTik RB411, 32MB RAM, 300 MHz, miniPCI, 1krát LAN, vč. L3 s připojenou bezdrátovou miniPCI kartou TL-WN562AG, Atheros 5006X (2,4/5 GHz) s pigtailem U.FL/RSMA o délce 10 cm a 2dBi dipólovou anténou.
- MikroTik RB912UAG-5HPnD, 2×2 MIMO RouterBoard, Atheros AR9432 taktovaný na 600 MHz s integrovanou kartou 5 GHz 802.11a/n, USB port a možnost napájení PoE i přes konektor. 1Gbit LAN port s ESD ochranou +16 kV i na obou RF portech, miniPCIe slot a SIM card slot.
- UBNT NanoBeam M5, anténa 300 mm, označení NBE-M5-300, LAN port RJ45 10/100 Mbps, napájení 12–24V (pouze PoE). Max. výstupní výkon 23dBm, duální anténa, vyzařovací úhel H/V 8°/8°, zisk antény 22dBi. Procesor MIPS 74KC, 550 MHz, 64 MB RAM, 8 MB NAND.

Z důvodu, že součástí RB 912UAG není na rozdíl od jednotky NanoBeam parabolická anténa, musela být při venkovním měření použita 2krát parabolická anténa JRC-24 EXTREM MIMO s RSMA-F, duální MIMO, 23,6 ±0,6dBi, PSV ≤ 1,5, vyzařovací úhel (-3 dB) 9°, předozadní poměr ≥ 38 dB, konektory R-SMA.

Pro umístění RouterBoardů k anténě 2krát venkovní box GentleBOX JR-200. Pro propojení RouterBoardů a antén 4krát pigtail MMCX male/RSMA male přímý 25cm RG178U.

Pro propojení přístupových bodů a počítačů byl použitý FTP kabel o maximální délce pět metrů. K napájení byly použity originální PoE adaptéry od výrobců.

## 5.3 Lokalita

Testované spoje budou umístěny na dvou obytných domech v obci Blatnice pod Svatým Antonínkem. První se nachází v nadmořské výšce 231 metrů nad mořem, druhý ve výšce 201 metrů nad mořem. Vzdálenost mezi domy je 743 metrů. Antény budou umístěny současně na stejném stožáru nad sebou. Mezi anténami je přímá viditelnost a volná Fresnelova zóna, která má v polovině délky spoje poloměr 3,2 metru (Jirous, 2014). Jako přístupový bod bude považováno místo označené na obrázku č. 8 jako bod s červenou značkou. Klientská stanice a tedy místo, kam je třeba internetovou konektivitu zavést, je bod se zelenou barvou.

Seznam dostupných sítí naskenovaných v lokalitě označené červenou značkou tvoří přílohu A této práce.

Skenování bylo provedeno zařízením MikroTik RB912UAG s anténami Jirous.



Obr. 8 Umístění bezdrátového spoje.  
Zdroj: Mapy.cz, 2014.

## 5.4 Nastavení programů

### 5.4.1 Iperf

Iperf je nástroj pro měření maximální šířky pásma TCP a UDP, umožňující ladění různých parametrů a vlastností. (Iperf, 2014)

Konkrétní přepínače s parametry serveru při měření TCP přenosu:

- -s – jedná se o server
- -t 30 – test bude probíhat 30 vteřin

- -w 1500k – TCP window size
- -i 1 – interval ve vteřinách, za který se bude počítat dílčí rychlost
- >název.txt – název a cesta k souboru, do kterého jsou data ukládána

U klienta se při nastavení navíc udává přepínač -c a IP adresa, ke kterému serveru se má připojit a přepínač -r, který zajistí, že se po testu odesílání dat provede ihned test přijímání dat.

Konkrétní přepínače s parametry serveru při měření UDP přenosu:

- -s – jedná se o server
- -u – jedná se o test UDP přenosu
- -t 30 – test bude probíhat 30 vteřin
- -w 1500k – socket buffer size
- -i 1 – interval ve vteřinách, kdy budou dílčí data ukládána do souboru
- >název.txt – název a cesta k souboru, do kterého jsou data ukládána

U klienta se při nastavení navíc udává přepínač -c a IP adresa, ke kterému serveru se má připojit, přepínač -r, který zajistí, že se po testu odesílání dat provede ihned test přijímání dat a přepínač -b s parametrem 200, který udává generovanou velikost datového toku u UDP testu v megabitech za vteřinu.

#### 5.4.2 hrPing

Stejně jako program ping v operačním systému Windows také hrPing posílá ICMP Echo Request pakety na vzdálený počítač a čeká na ICMP Echo Reply. Navíc hrPing může posílat UDP pakety i ICMP pakety s časovým razítkem. Ne všechny typy paketů totiž mohou projít bránou firewall dané sítě. Program hrPing má možnost měnit tyto parametry. Odezvu každé smyčky lze měřit v mikrosekundách (1/1000 msec). (Cfos software, 2014)

Konkrétní přepínače s parametry programu:

- 192.168.0.51 – IP adresa, kam se ICMP paket odesílá
- -n 1000 – počet odeslaných ICMP požadavků, konkrétně 1000
- -s 5 – interval v milisekundách, jak často se ICMP požadavek odešle
- >název.txt – název a cesta k souboru, do kterého jsou data ukládána

## 5.5 Výsledky měření všech standardů v domácích podmínkách

V první části praktického měření jsou porovnány tři spoje (RB433 s RB411, 2krát RB912 a UBNT NanoBeam M5), čtyři standardy (802.11b/g/a/n), tři proprietární protokoly (nstream, NV2, AirMAX) a dvě doplňkové funkce (Aggregation a RTS Threshold). Provedených testů je celkem dvacet a jsou zobrazeny v přehledném grafu na obrázku číslo 9.

Graf se skládá ze dvou základních částí, kde horní část tvoří propustnost jednotlivých konfigurací v megabitech za sekundu a spodní část tvoří odezvu v milisekundách, která byla naměřena při dané maximální propustnosti. Propustnost a k ní patřičná odezva byla měřena vždy ve dvou směrech (Download a Upload) a při testu TCP a UDP spojení. Výsledkem měření každé normy jsou tak vždy čtyři rychlosti a čtyři odezvy. Součástí tohoto grafu je i tabulka číslo 3, kde jsou uvedeny jednotlivé konfigurace ke každému měření.

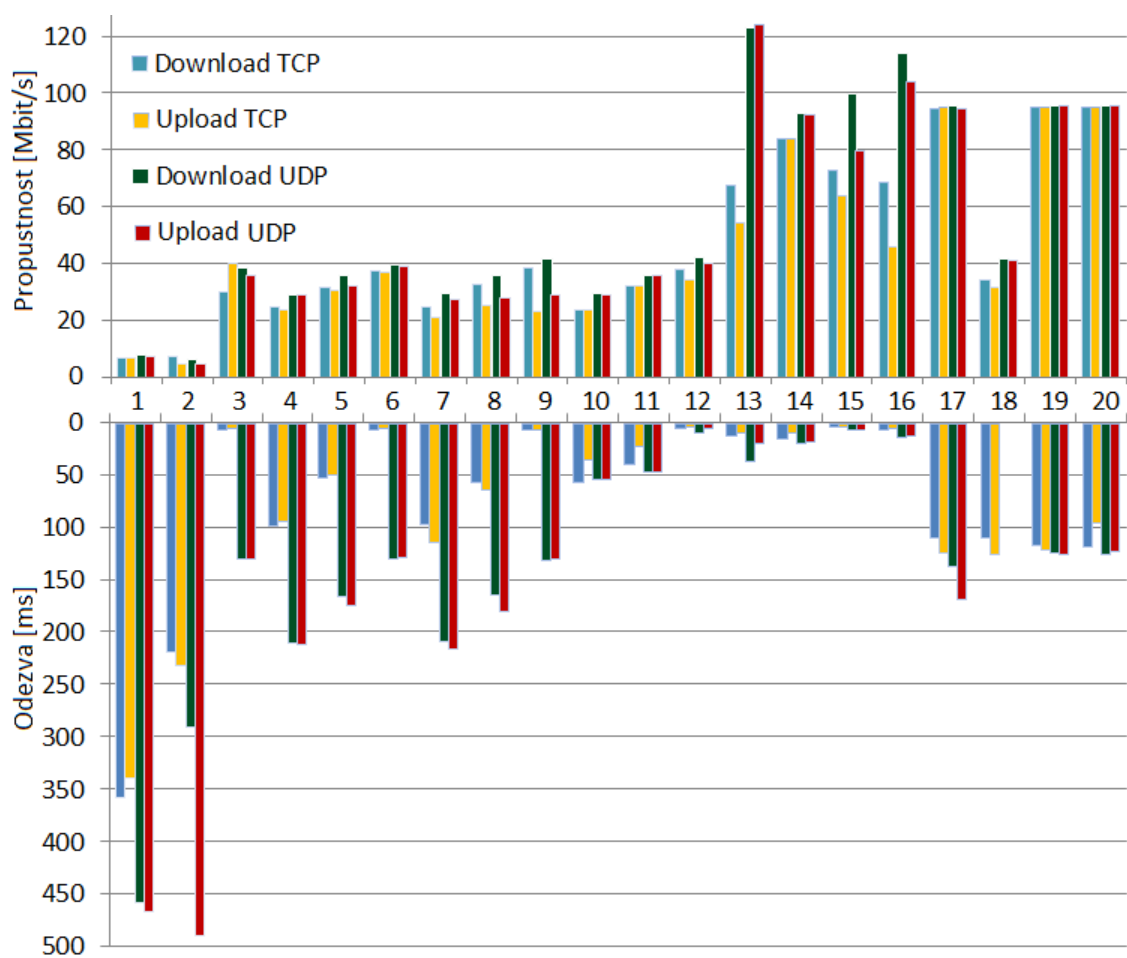
Rychlostně nejbližší má ke standardu 802.11a standard 802.11g. Obě jsou standardizovány s maximální data-rate 54 Mbit/s. Při srovnání lze konstatovat, že obě technologie mají stejnou maximální propustnost až na malé výjimky, které tvoří TCP Upload. Srovnání odezvy je zcela stejné. Zde lze konstatovat, že podobné výsledky se daly čekat, protože použité technologie jsou zcela stejné a rozdíl je pouze ve frekvenci přenosového kanálu. Pokud by však došlo na rušení vedlejších kanálů, výsledky by se ihned změnily (více v kapitole 2.1.1).

Další čtyři výsledky, které jsou velmi rozmanité, tvoří RB912 se standardem 802.11n. Testy UDP protokolu dosahují rychlosti přes 100 Mbit/s se zachováním velmi nízké odezvy. TCP přenos ale velmi zaostává za maximem UDP, hlavně pak u standardu 802.11n bez použití přídatných protokolů.

Stejnou rychlost lze vidět u měření č. 17, 19 a 20, kde je testován standard 802.11n na zařízení NanoBeam (UBNT). Nevýhodou těchto zařízení je absence gigabitového ethernetového portu, z čehož vyplývá, že testy nemohou nikdy přesáhnout hranici 100 Mbit/s. U testu s vypnutou agregací (měření č. 18) je rychlost jednoznačně nejnižší a při testech UDP spojení nebyly přijaty žádné ICMP pakety Echo Request, i když timeout byl nastaven na 1000 ms.

Omezení 100Mbit/s portem by nemělo být tak zásadní ve venkovních podmínkách, kde přenosová rychlost může být omezena rušením okolních stanic.





Obr. 9 Srovnání jednotlivých standardů a technologií při měření v domácích podmínkách.

Tab. 3 Jednotlivé standardy a technologie použité při měření.

1. RB433, b	8. RB433, a nstream	15. RB912, n NV2 TDMA, 1ms
2. RB433, b nstream	9. RB433, a NV2	16. RB912, n NV2, TDMA 2ms
3. RB433, b NV2	10. RB912, a	17. UBNT, n AirMAX ON, Aggr. ON
4. RB433, g	11. RB912, a nstream	18. UBNT, n AirMAX OFF, Aggr. OFF
5. RB433, g nstream	12. RB912, a NV2	19. UBNT, n AirMAX OFF, Tres. 200
6. RB433, g NV2	13. RB912, n	20. UBNT, n AirMAX OFF, Aggr. ON
7. RB433, a	14. RB912, n nstream	

Hlavním ukazatelem stability přenosu byla zvolena směrodatná odchylka, vypočtená z naměřených dat. Pro výpočet každé směrodatné odchylky je použito všech 30 hodnot z jednotlivého testu TCP propustnosti. Současně s průměrnou odezvou při testu bez zatížení jsou hodnoty zaznamenány v tabulce č. 4.

Vyšší směrodatná odchylka je u testu TCP uploadu u standardu 802.11a NV2. Po analýze podkladů k tomuto měření bylo zjištěno, že rychlost přenosu byla nestabilní prvních pět vteřin, kdy se postupně snížila až na nulu. Od páté vteřiny je přenos zcela stabilní. Tento pokles mohl být způsoben například změnou modulace. U testu číslo 16 je po analýze podkladů zřejmé, že maximální rychlost nebyla ihned ze začátku přenosu, ale postupně se zvyšovala.

Zde je důležité si všimnout, že takovéto postupné zvyšování rychlosti (modulace) velmi ovlivní jak průměrnou rychlost, tak směrodatnou odchylku. Na první pohled by se tak mohlo zdát, že spoj je nestabilní. Má však pouze pomalý nárůst rychlosti. Proto je vždy důležité individuálně zkoumat každé měření. Průběh tohoto konkrétního měření číslo 16 tvoří přílohu B a C této práce.

Zkoumáním průměrné odezvy bez zatížení spoje lze zjistit, že spoje vykazují nízkou odezvu ve všech měřeních. Pokud je tedy spoj zatížen jen minimálně (při testu odezvy byl v řádu stovek kilobytů za vteřinu), odezva se drží také na minimu. Ztrátovost zde byla skoro vždy nulová.

Tab. 4 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při domácím (indoor) měření.

Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	0,89	1,69	11. test, Down.	0,41	1,14
1. test, Up.	2,76		11. test, Up.	1,65	
2. test, Down.	0,39	2,88	12. test, Down.	4,25	3,30
2. test, Up.	2,62		12. test, Up.	10,65	
3. test, Down.	2,74	3,65	13. test, Down.	8,26	1,01
3. test, Up.	0,52		13. test, Up.	6,74	
4. test, Down.	2,58	1,38	14. test, Down.	2,99	1,16
4. test, Up.	0,56		14. test, Up.	2,40	
5. test, Down.	0,95	1,34	15. test, Down.	5,51	3,70
5. test, Up.	1,01		15. test, Up.	4,49	
6. test, Down.	3,88	2,15	16. test, Down.	8,83	3,80
6. test, Up.	0,68		16. test, Up.	17,60	
7. test, Down.	2,44	1,34	17. test, Down.	1,38	2,34
7. test, Up.	0,89		17. test, Up.	1,50	
8. test, Down.	0,38	1,63	18. test, Down.	3,43	2,12
8. test, Up.	2,09		18. test, Up.	0,46	
9. test, Down.	2,83	3,69	19. test, Down.	0,20	2,12
9. test, Up.	2,47		19. test, Up.	1,36	
10. test, Down.	2,22	0,82	20. test, Down.	0,45	2,27
10. test, Up.	0,46		20. test, Up.	2,06	

## 5.6 Výsledky měření vybraných norem ve venkovních podmínkách

Druhá polovina praktické části je zaměřena na ověření naměřených hodnot z první poloviny ve venkovních podmínkách. Všechna měření byla provedena na třech kanálech, kde první dva (104/5520 MHz a 112/5560 MHz) byly vybrány jako nejméně zarušené a třetí (140/5700 MHz) jako nejvíce zarušený. Při výběru kanálů byly zohledněny nejen naměřené hodnoty úrovně signálu, které tvoří přílohu A, ale i praktické poznatky o umístění daných přístupových bodů, směrovosti a jejich vytížení.

V této části se budou testovat pouze standardy 802.11a a 802.11n, které v testech v domácích podmínkách dopadly nejlépe. Konkrétní konfigurace, které budou mezi sebou porovnávány (vždy na třech kanálech), jsou uvedeny v následující tabulce číslo 5.

Úroveň přijímaného signálu se u všech testů pohybovala v rozmezí -70 dBm až -65dBm. Jednotky tak měly vždy dostatečný signál pro použití nejvyšší modulační rychlosti.

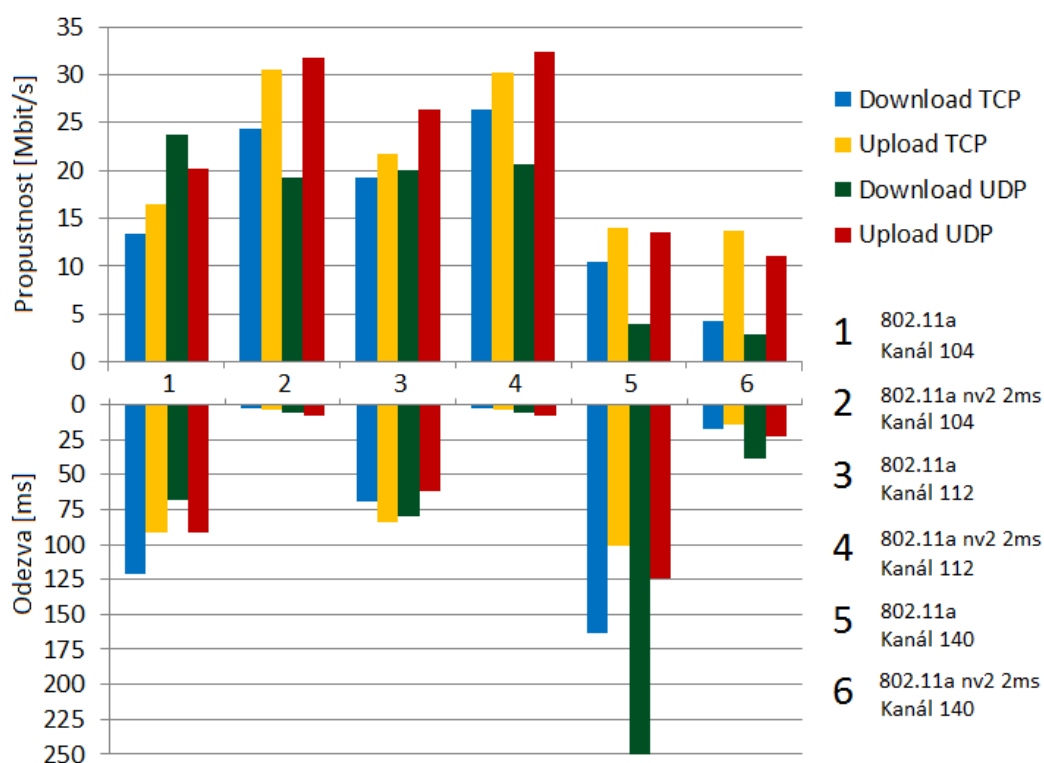
Tab. 5 Konfigurace jednotlivých testů.

Kapitola	Konfigurace 1		Konfigurace 2	
	Zařízení	Norma + poznámka	Zařízení	Norma + poznámka
5.6.1	RB 912	802.11a	RB 912	802.11a NV2, 2 ms
5.6.2	RB 912	802.11n NV2, 2ms	NanoBeam	802.11n AirMAX
5.6.3	NanoBeam	802.11n	NanoBeam	802.11n AirMAX
5.6.4	RB 912	802.11n	RB 912	802.11n NV2, 2 ms
5.6.5.	RB 912	802.11n NV2, 1 ms	RB 912	802.11n NV2, 2 ms
5.6.6	RB 912	802.11n NV2, 2 ms AP v centru	RB 912	802.11n NV2, 2 ms AP na okraji
5.6.6	NanoBeam	802.11n AirMAX AP v centru	NanoBeam	802.11n AirMAX AP na okraji
5.6.7	NanoBeam	802.11n AirMAX Aggregation OFF	NanoBeam	802.11n AirMAX Aggregation ON

### 5.6.1 Porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik)

K měření (porovnání) propustnosti standardu 802.11a a stejné normy s protokolem NV2 byl použit MikroTik RB912 a antény Jirous. Měření probíhalo v horizontální polarizaci. Výsledky jsou zaznačeny v grafu na obrázku číslo 10.

Z porovnání lze zjistit, že použití protokolu NV2 výrazně zvyšuje propustnost TCP přenosu. Toto však neplatí u zarušeného kanálu, kde se rychlost TCP downloadu snížila za cenu udržení nízké latence. Nízká latence je zřejmě hlavní předpoklad pro použití protokolu NV2. Ukazují to výsledky na všech testovaných kanálech, kde byl protokol NV2 zapnutý.



Obr. 10 Porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik)

V tabulce číslo 6 je opět zaznačená směrodatná odchylka u všech TCP testů a odezva bez zatížení spoje. Zde je nutno upozornit, že průměrná rychlost se pohybovala kolem dvaceti megabitů. Směrodatná odchylka je tedy na první pohled nízká, ale je také závislá na průměrné rychlosti, která je zde nižší, než například u testů standardu 802.11n. Zároveň lze ale konstatovat, že je stabilní.

U velmi zarušeného kanálu je při nepoužití NV2 protokolu velmi vysoká odezva i bez zátěže. Taková konfigurace je pro použití připojení k internetu zcela nevhovující.

Tab. 6 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik)

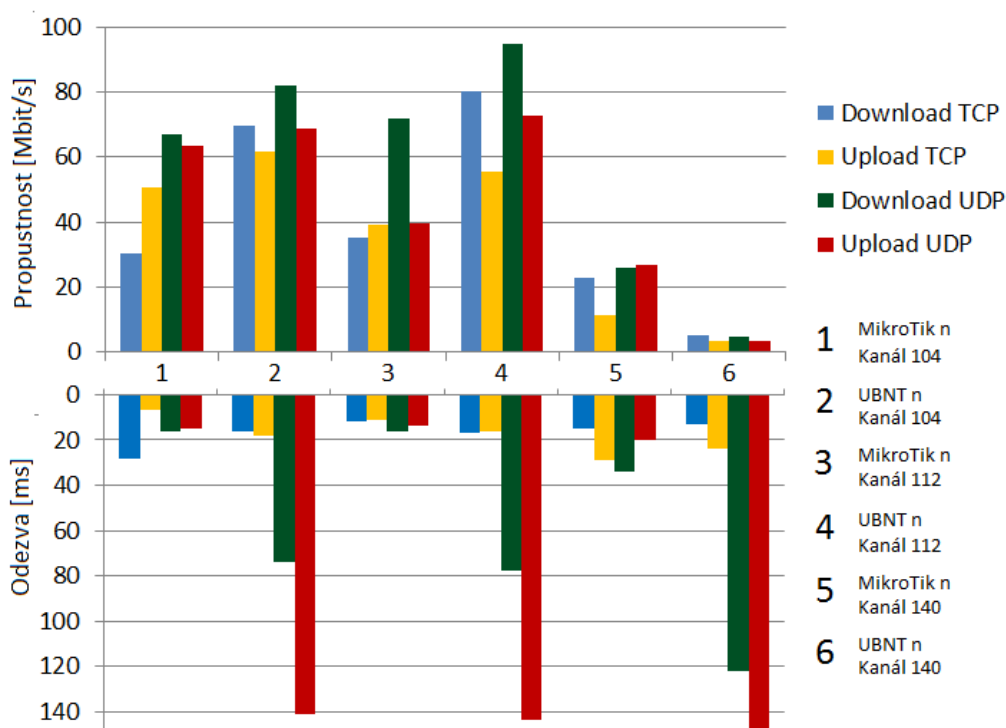
Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	4,12	3,46	4. test, Down.	2,43	3,7
1. test, Up.	1,63		4. test, Up.	1,01	
2. test, Down.	2,29	3,46	5. test, Down.	3,66	80,8
2. test, Up.	1,27		5. test, Up.	1,97	
3. test, Down.	2,01	1,39	6. test, Down.	5,33	12,9
3. test, Up.	1,04		6. test, Up.	1,91	

### 5.6.2 Porovnání standardu 802.11n NV2 (MikroTik) a 802.11n AirMAX (UBNT)

Jedno z nejdůležitějších měření, kde se srovnávají dvě nejpoužívanější konfigurace, je zobrazeno v grafu na obrázku číslo 11. Ve všech případech se jedná o standard 802.11n, ale s různým hardware od dvou firem a s různými proprietárními protokoly. U zařízení firmy MikroTik se jedná o protokol NV2 a u zařízení firmy UBNT se jedná o protokol AirMAX, což jsou protokoly využívající TDMA mechanismus (více v kapitole 3.1 a 3.2).

Z měření jasně vyplývá, že na méně zarušených kanálech dosahuje zařízení firmy UBNT vyšší přenosové rychlosti jak při přenosu TCP, tak i UDP. Odezva při měřeních propustnosti zařízení MikroTik (při plném zatížení) byla vždy na přijatelné úrovni do 50 ms. Při UDP testu u zařízení firmy UBNT se odezva pohybovala nad hranicí 50 ms, u upload testu až nad hranicí 140 ms. Při měření v domácích podmínkách byla odezva stejně vysoká, ale zde se mohlo jednat o zkreslení kvůli absenci 1Gbit/s portu. Při testu na 104 kanále se však rychlost pohybovala kolem 70 Mbit/s. Vysoká odezva tak zřejmě přímo nesouvisí s rychlostí ethernetového portu.

Na zarušeném 140. kanále dosahovalo zařízení firmy MikroTik výrazně lepších výsledků, než zařízení firmy UBNT. Důvodem zde může být kvalitnější anténa, jejíž součástí je i límec pro zabránění rušení ze stran.



Obr. 11 Porovnání zařízení firmy MikroTik a UBNT na standardu 802.11n s TDMA.

Pro porovnání těchto dvou technologií je směrodatná odchylka velmi důležitá. Je však zřejmé, že ve všech testech zobrazených v tabulce číslo 7, kromě posledních dvou, jsou odchylky velmi podobné. Pokud se ale podíváme na poslední dva testy podrobně, zjistíme, že zhruba čtyřnásobný rozdíl mezi směrodatnou odchylkou u downloadu je zde proto, že RB912 byl při testu rychlosti schopný přenášet čtyřnásobně vyšší rychlostí, než zařízení NanoBeam.

Odezva bez zatížení spoje je u zařízení RB912 velmi vysoká, ale opět stabilní i při zatížení spoje.

Tab. 7 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání zařízení firmy MikroTik a UBNT na standardu 802.11n s TDMA

Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	10,17	32,3	4. test, Down.	4,96	2,4
1. test, Up.	9,62		4. test, Up.	10,11	
2. test, Down.	17,11	3,9	5. test, Down.	8,80	28,0
2. test, Up.	11,60		5. test, Up.	6,46	
3. test, Down.	6,36	10,0	6. test, Down.	2,11	4,9
3. test, Up.	13,48		6. test, Up.	3,57	

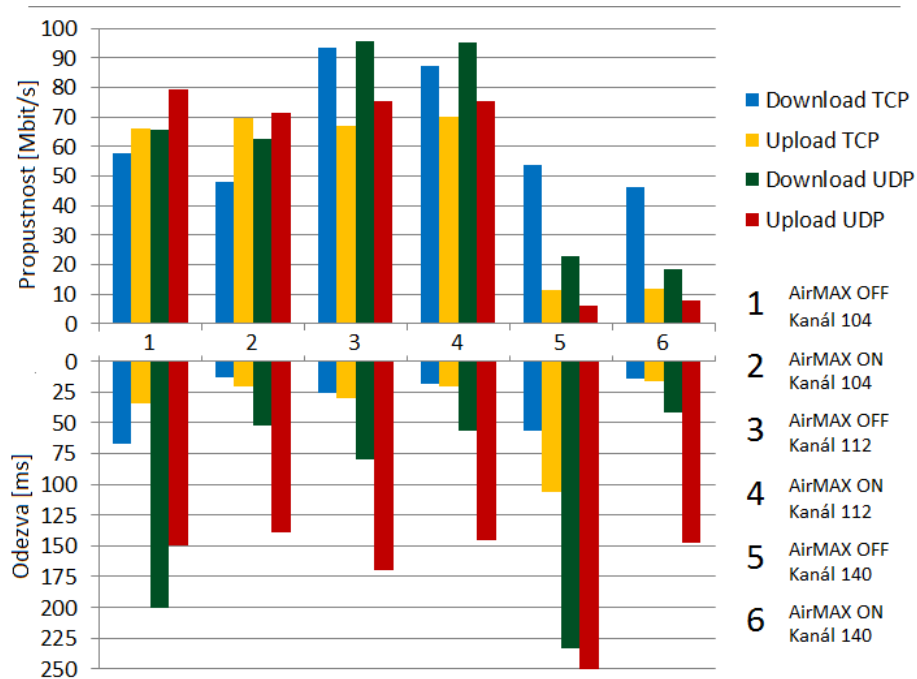
### 5.6.3 Porovnání TDMA protokolu AirMAX (ON/OFF) u zařízení UBNT

Na obrázku číslo 12 je znázorněno porovnání zařízení firmy UBNT se zapnutou a vypnutou funkcí AirMAX. Můžeme zde konstatovat, že zapnutí této funkce nemá významný dopad na propustnost. Lze si ale všimnout mírného snížení latence. U UDP testů propustnosti se však stále pohybuje nad 50 ms, což již není ideální. Testy byly prováděny ihned po sobě tak, aby zde nebylo žádné zkreslení z rušení.

V tabulce číslo 8 jsou opět uvedeny hodnoty směrodatné odchylky u všech TCP testů a odezva bez zátěže. Všimnout si zde lze stejné směrodatné odchylky u TCP downloadu a uploadu u testu pět a šest. Směrodatná odchylka je velmi podobná, ale rychlost se liší až čtyřnásobně.

Tab. 8 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání TDMA protokolu AirMAX (ON/OFF) u zařízení UBNT.

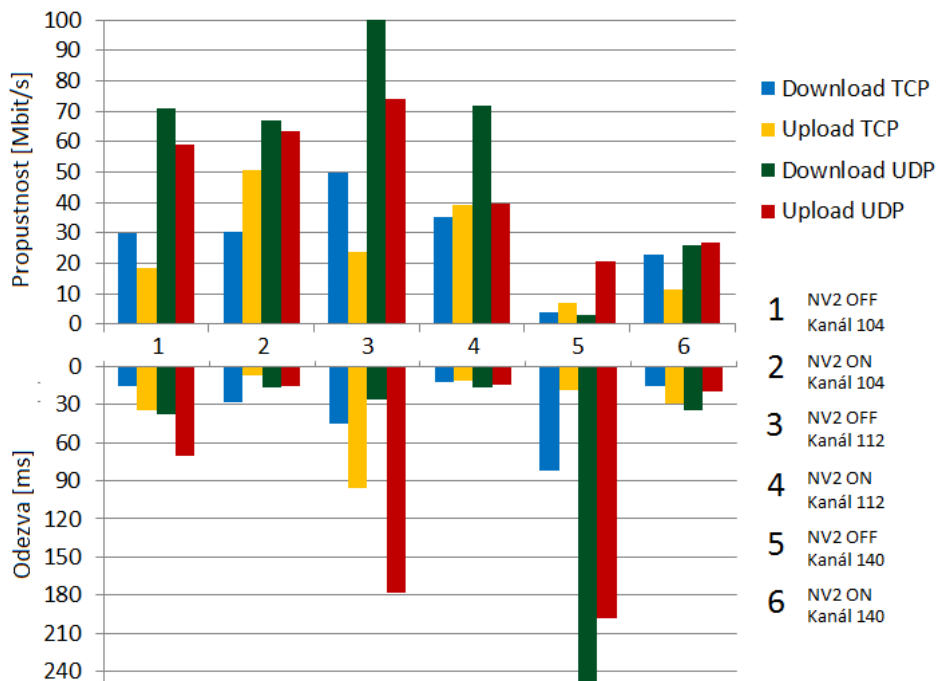
Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	12,88	1,85	4. test, Down.	7,28	1,90
1. test, Up.	16,58		4. test, Up.	11,72	
2. test, Down.	6,38	2,28	5. test, Down.	11,37	3,30
2. test, Up.	14,85		5. test, Up.	14,72	
3. test, Down.	2,55	1,71	6. test, Down.	10,25	2,61
3. test, Up.	16,52		6. test, Up.	13,26	



Obr. 12 Porovnání UBNT 802.11n se zapnutou a vypnutou funkcí AirMAX.

### 5.6.4 Porovnání TDMA protokolu NV2 (ON/OFF) u zařízení MikroTik

Stejné testy byly provedeny se zařízením od firmy MikroTik (obrázek číslo 13). Zde se až na jednu výjimku odezva také snižovala, rychlost však velmi kolísala a nelze tak jednoznačně konstatovat, která konfigurace je v těchto podmínkách lepší.



Obr. 13 Porovnání MikroTik 802.11n se zapnutou a vypnutou funkcí NV2.

V tabulce číslo 9 si lze všimnout vyšší odezvy při testech bez zátěže bez použití funkce AirMAX, zejména pak u zarušeného kanálu. Směrodatné odchylky korepondují s naměřenou maximální rychlostí.

Tab. 9 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání TDMA protokolu NV2 (ON/OFF) u zařízení MikroTik

Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	6,1	2,73	4. test, Down.	6,36	10,0
1. test, Up.	13,69		4. test, Up.	13,48	
2. test, Down.	10,17	32,30	5. test, Down.	1,59	105,0
2. test, Up.	9,62		5. test, Up.	3,39	
3. test, Down.	17,62	3,49	6. test, Down.	8,80	28,0
3. test, Up.	12,71		6. test, Up.	6,46	

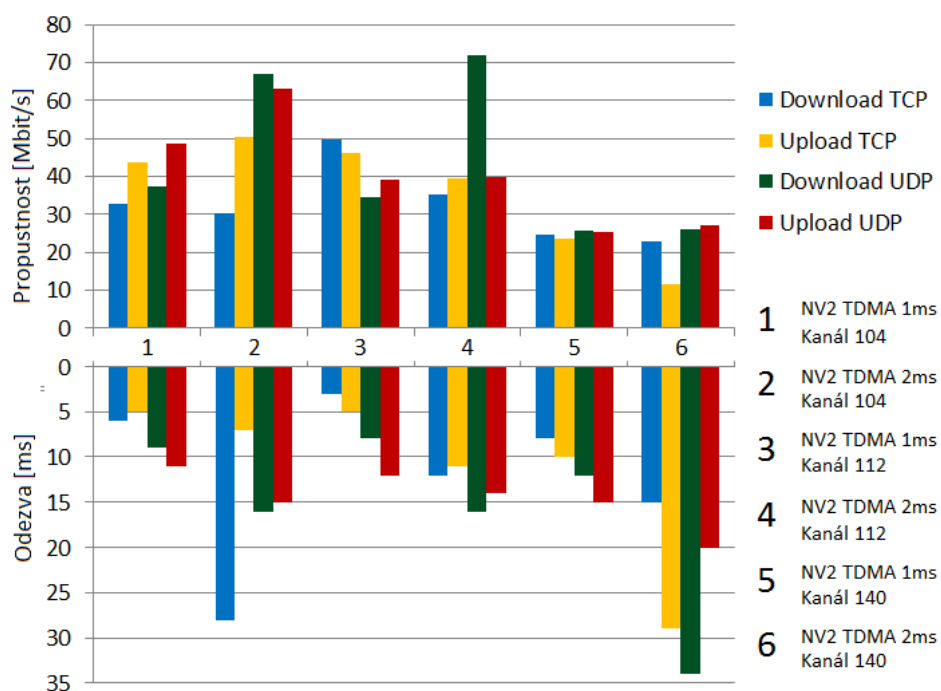
### 5.6.5 Porovnání nastavení TDMA protokolu (1 ms/2 ms) u zařízení MikroTik

U zařízení RB912 lze nastavit tzv. „TDMA period size“. Hodnotu od jedné do deseti milisekund, která udává délku časového slotu. Defaultní hodnota je 2 ms. V tomto testu, jehož výsledky jsou zaznačeny na obrázku číslo 14, jde o porovnání nastavení s hodnotou jedné a dvou milisekund. Výsledkem by mělo být, zda délka této periody ovlivňuje propustnost a odezvu spoje. Tento test byl také proveden v nezarušených podmínkách při domácím měření.

Stejně jako v domácích podmínkách, rychlost UDP přenosu je vždy o něco vyšší s delší periodou. U TCP přenosu je propustnost o něco nižší nebo stejná. Co však platí vždy u kratší periody, je kratší doba odezvy.

V tabulce číslo 10 jsou zachyceny jednotlivé směrodatné odchylky a odezvy bez zatížení spoje. Zde také platí nižší odezva při kratší periodě.





Obr. 14 Porovnání MikroTik 802.11n s TDMA 1 ms a 2 ms.

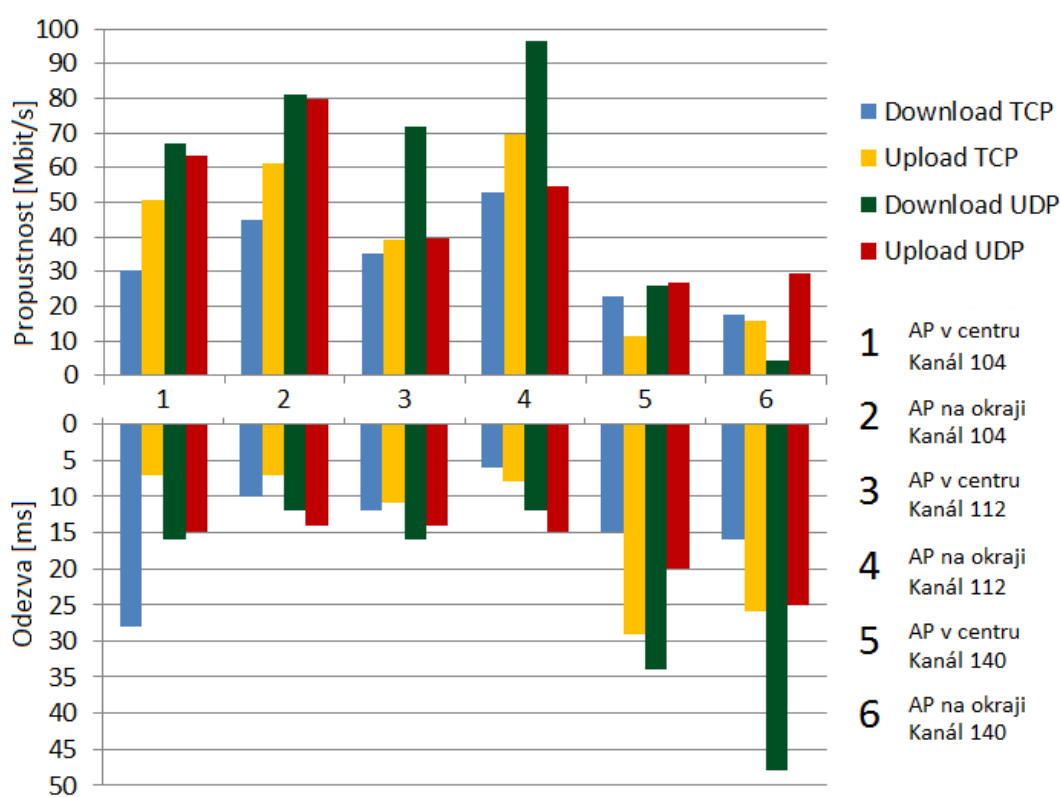
Tab. 10 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání MikroTik 802.11n s TDMA 1 ms a 2 ms.

Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	7,08	4,1	4. test, Down.	6,36	10,0
1. test, Up.	7,12		4. test, Up.	13,48	
2. test, Down.	10,17	32,0	5. test, Down.	4,66	9,1
2. test, Up.	9,62		5. test, Up.	3,51	
3. test, Down.	8,5	3,7	6. test, Down.	8,8	28,0
3. test, Up.	4,32		6. test, Up.	6,46	

### 5.6.6 Porovnání prohození přístupového bodu a klienta (Mikrotik i UBNT)

Jedním z nejzajímavějších testů bylo prohození přístupového bodu a klientské stanice. Neměnilo se zde žádné jiné nastavení. Jednou byl přístupový bod (AP) umístěn ve více zarušené části obce, kde má většina poskytovatelů své přístupové body. Podruhé byl přístupový bod umístěn v okrajové části obce, kde byl „zákazník“, ke kterému měli data primárně směřovat. Toto prohození lze provést pouze softwarovou konfigurací. Nemusí se měnit umístění žádných zařízení.

Vždy byl použit standard 802.11n s TDMA protokolem. Z testů na obrázku číslo 15 lze vyvodit, že přístupový bod umístěný na okraji obce byl lepší ve všech parametrech, kromě testů na zarušeném kanálu.



Obr. 15 Porovnání MikroTik 802.11n NV2 při prohození přístupového bodu a klienta.

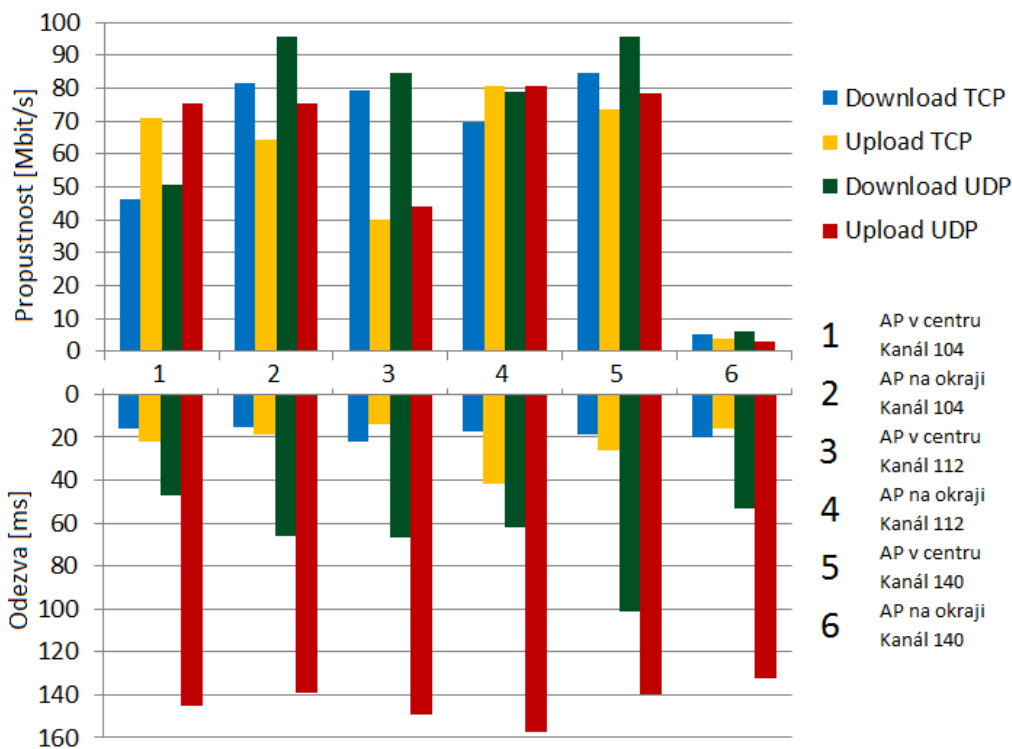
V tabulce číslo 11 nejsou žádné viditelné souvislosti mezi hodnotami směrodatné odchylky. U odezvy si však lze všimnout, že při umístění přístupového bodu na okraji, vykazují spoje nižší odezvu.

Tab. 11 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání MikroTik 802.11n NV2 při prohození přístupového bodu a klienta.

Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	10,17	32,3	4. test, Down.	11,25	6,0
1. test, Up.	9,62		4. test, Up.	2,78	
2. test, Down.	9,81	13,4	5. test, Down.	8,8	28,0
2. test, Up.	9,92		5. test, Up.	6,46	
3. test, Down.	6,36	10,0	6. test, Down.	9,29	6,4
3. test, Up.	13,48		6. test, Up.	6,55	

Stejně provedené testy pouze s jiným hardware jsou zaznačeny v grafu na obrázku číslo 16. Zde se také potvrdilo, že umístění přístupového bodu mimo centrum dovede zvýšit propustnost daného spoje. Na zarušeném kanále to však neplatilo, protože v blízkosti klientské stanice bylo umístěno stejné zařízení nastavené také jako přístupový bod, které zarušilo příjem od testovaného přístupového bodu.

V tabulce číslo 12 je zaznačena odezva, která je nízká a ve zhruba stejném rozsahu kolem dvou milisekund. Stabilita spojů velmi kolísala, i když celková rychlost byla velmi vysoká.



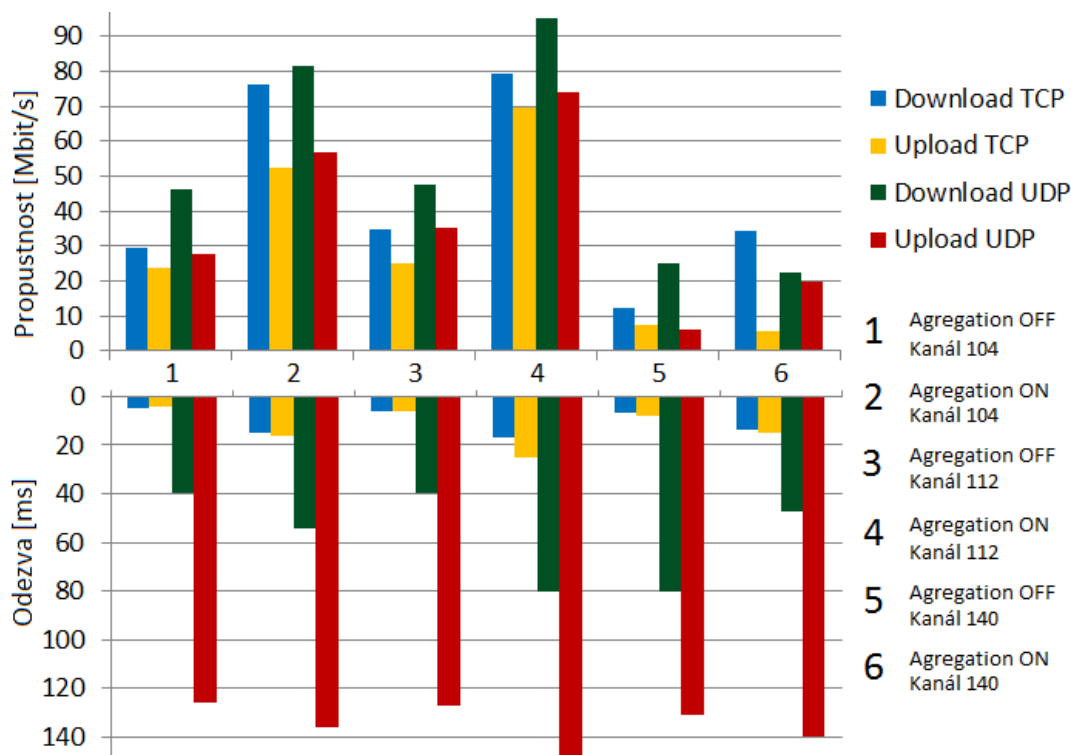
Obr. 16 Porovnání UBNT 802.11n AirMAX při prohození přístupového bodu a klienta.

Tab. 12 Směrodatná odchylka u všech TCP testů propustnosti a odezva bez zatížení při porovnání UBNT 802.11n AirMAX při prohození přístupového bodu a klienta.

Označení	Směr. odchylka [Mbit/s]	Ping [ms]	Označení	Směr. odchylka [Mbit/s]	Ping [ms]
1. test, Down.	8,81	3,94	4. test, Down.	4,27	2,22
1. test, Up.	13,66		4. test, Up.	16,19	
2. test, Down.	11,91	1,98	5. test, Down.	14,24	1,97
2. test, Up.	14,72		5. test, Up.	28,55	
3. test, Down.	5,83	1,92	6. test, Down.	0,86	3,25
3. test, Up.	11,83		6. test, Up.	4,42	

### 5.6.7 Porovnání funkce Aggregation (ON/OFF) u zařízení UBNT

Stejně jako v domácích podmínkách, tak i ve venkovních podmínkách byly provedeny testy na vliv funkce agregace u zařízení UBNT (výsledek testů na obrázku číslo 17). Jelikož generovaná data byla stejného typu, stejného cíle a stejné priority, spojování jednotlivých rámců do větších bylo velkou výhodou. Ušetřila se tak velká část režie a testy se zapnutou agregací dopadly výrazně lépe než bez této funkce. Rychlý ping dopadl u všech konfigurací podobně, a to od dvou do tří milisekund. Směrodatné odchylky zde nejsou vypočteny z důvodu jednoznačnosti porovnání pomocí grafu propustností.



Obr. 17 Porovnání UBNT 802.11n se zapnutou a vypnutou funkcí Aggregation.

## 6 Závěr

Ze všech testů vyplývá, že výhodnější je použití standardu 802.11n, než staršího standardu 802.11a. I s proprietárním protokolem NV2 dosahuje standard 802.11a pouze poloviční propustnosti, než standard 802.11n.

Dále z testů vyplynulo, že použití TDMA protokolu nemá na maximální propustnost spoje (bod-bod) zásadní vliv. Pokud je však nízká odezva prioritou, je vhodné TDMA protokol použít, a to s nižší vysílací periodou.

Pokud je naší prioritou rychlost, je vhodnější zvolit zařízení firmy UBNT. Neplatí to však v případech, kdy je v blízkosti přístupový bod, vysílající na stejném kanále. Pokud výrobce instaluje do svých jednotek pouze 100Mbit/s port, i když je teoretická přenosová rychlost standardu 802.11n 130Mbit/s, zřejmě pro to má své důvody. Jednotky jsou schopné vytvořit stabilní spoj na desítky kilometrů, kde tak vysoké přenosové rychlosti nejsou schopny dosáhnout. Zde, pro použití na pár stovek metrů, by byl gigabitový ethernetový port vhodnější.

Vyšší odezva u jednotek NanoBeam by se dala vysvětlit právě prioritizací datového toku. Při generování datového toku nejsou data nijak označována (QoS) a tak není zřejmé, podle jakého pravidla jsou data přenášena. Odezva byla vždy měřena při plném zatížení spoje a tak nebylo zjištěno, jaká odezva by byla při devadesáti, sedmdesáti či padesáti procentním zatížení. Je možné, že právě zahlcením hardwarových front v bezdrátových jednotkách může docházet k jiným vlastnostem přenosu. Také je možné, že neoznačením dat nemohl fungovat systém prioritizace. O toto označení by se měly starat přímo přístupové body (bod-multibod), ke kterým se zákaznické stanice připojují, nebo přímo klientské stanice. Jelikož bylo u některých testů použito proprietárních protokolů, u kterých výrobce podrobně nepopisuje jejich princip, lze nad jejich funkčností jen polemizovat.

Výraznou roli na kvalitu přenosu má použitý hardware. Kromě firmy Mikrotik a UBNT existují na trhu i firmy, které se specializují na určité hardwarové části, používané právě pro tyto spoje. Při testování RB912 byly použity antény, které dodává česká firma Jirous, specializující se přímo na antény pro bezdrátový přenos dat. Oproti sériově vyráběným jednotkám NanoBeam zde existují výrazné rozdíly v parametrech a každá anténa Jirous se testuje jednotlivě. Z testů jasně vyplynulo, že antény Jirous si lépe poradí se zarušeným prostředím než jednotky NanoBeam od firmy UBNT. Abychom však eliminovali ještě vliv bezdrátové jednotky, bylo by vhodné otestovat pro porovnání jednotku od firmy UBNT s anténami od firmy Jirous. Jednou z možností je také dokoupit k anténám UBNT hliníkový ochranný límec s radomem (předním krytem).

Hlavním faktorem, který ovlivňuje testy ve venkovním prostředí je zarušení přenosového média. V blízkosti spoje se nacházelo několik dalších poskytovatelů internetového připojení, jejichž počet několikrát přesahuje počet volných kanálů. Pokud bychom spoj umístili jiným směrem, výsledky by byly zcela jistě mírně odlišné. Důležité pro aktuální přenosovou rychlost spoje je také to, zda stanice na stejném vysílacím kanále aktuálně přenáší či nikoliv. Pro eliminaci této skutečnosti byly testy vždy provedeny dvakrát, a pokud se výsledky zcela lišily, byl proveden ještě třetí ověřovací test. Měření ve venkovních podmínkách je velmi obtížné pro stále měnící se okolní podmínky. A právě z těchto důvodů se musí každý nový spoj

přímo nastavit a také jednou za čas zkontrolovat a popřípadě upravit jeho nastavení.

Při prohození vysílacího přístupového bodu a klienta bylo dosaženo výrazně lepších parametrů. V praxi ale není zcela běžné, aby u „zákazníků“ byly přístupové body, kde se nastavuje většina parametrů spoje. Pokud se však jedná o bod-bod, většinou má poskytovatel přístup na obě jednotky, aby mohl upravovat jejich konfiguraci.

V lokalitě testovaného spoje zůstane umístěn spoj složený z jednotek RB 912 a antén Jirous, protože se ukázal jako odolnější vůči rušení. Požadavky na rychlost tohoto spoje jsou poloviční, než činila jeho maximální rychlost. Odezva je při použití NV2 protokolu velmi nízká (v řádech milisekund), což je vyhovující i pro videohovory. Přístupový bod (AP), bude umístěn na okraji obce, což se ukázalo jako vhodnější řešení.

## 6.1 Cenové a praktické srovnání

Výhodou jednotek NanoBeam je jejich kompaktní rozměr, rychlost sestavení, dobrá manipulace a především nízká cena. V současnosti se tato jednotka prodává za 1900 Kč. Součástí balení je parabolická anténa, ozařovač, 100Mbit/s PoE adaptér pro napájení po síťovém kabelu, jednoduché uchycení na stožár. Celá jednotka se prodává dohromady a její složení trvá přibližně tři minuty.

Konkrétní hardware, který byl použit pro měření jednotek RB912 se nedodává dohromady<sup>2</sup> a bylo jej nutno poskládat z více částí. Anténa JRC-24 EXTREM MIMO (2 500 Kč), RB912UAG-5HPnD (1300 Kč), krabice pro umístění RB912 k anténě (250 Kč), Gbit PoE injektor (100 Kč), pigtail MMCX male/RSMA male (2krát 65 Kč). Jedna strana spoje stála tedy dohromady 4 280 Kč. V porovnání s cenou jedné jednotky NanoBeam je zřejmé, proč se v praxi převážně používají jednotky NanoBeam a další kompaktní jednotky od firmy UBNT. Firma MikroTik ale vyrábí více produktových řad, kde lze také nalézt podobná all-in-one řešení za příznivou cenu.

Nelze tak dát jednoznačné doporučení podle ceny, protože spoj na stejném standardu lze zakoupit za 3 000 Kč i za 10 000 Kč.

Ještě lze dodat, že sestavení celého kompletu určeného pro toto testování i s tvrzením těsnících hmot trvalo nejméně 8hodin. Mechanismus uchycení je však propracovanější a lze si směřovat zvlášť horizontální a vertikální rovinu. Pokud se také pokazí jen bezdrátová karta, stačí ji reklamovat vyjmutím z boxu a nemusí se demontovat a odesílat na reklamaci celé zařízení i s anténou.

Největší nevýhodou pro uživatele těchto bezdrátových spojů je skutečnost, že protokoly NV2 a AirMAX, i když jsou založeny na TDMA protokolu, nejsou navzájem kompatibilní. Každý poskytovatel se tedy musí předem rozhodnout, zda bude celý spoj od jedné, nebo druhé firmy. Při použití standardu 802.11n bez proprietárních protokolů, lze propojit jednotky i konkurenčních firem.

---

<sup>2</sup> Lze ale koupit anténu přímo dodávanou výrobcem a dokoupit zvlášť RB912. Dodává se i ve venkovním provedení. Označení: MikroTik parabolická anténa mANT30 PA 5GHz 70cm. Aktuální cena 2 700 Kč/kus.

Pokud se poskytovatel rozhodne, že do přilehlé vesnice přivede bezdrátový internet, nebo potřebuje pokrýt signálem ulici, která není dostupná přímo z hlavního vysílacího bodu, musí použít právě spoj bod-bod, ke kterému napřímo připojí přístupový bod pro připojení zákazníků. V současné době platí, že pro připojení zákazníků se používá standardu 802.11a nebo 802.11n. Pokud je tedy propustnost přístupového bodu závislá na maximu standardu 802.11n, stačí použít spoj bod-bod na stejné technologii se stejnou přenosovou rychlostí.

Jsou-li na spoj kladeny větší nároky, je nutné využít zařízení využívající frekvenci 10 GHz. Nejlevnější spoj od firmy UBNT stojí v současné době 23 000 Kč za obě strany (i4wifi, 2014). Jeho propustnost se pohybuje dle specifikace výrobce do 100 Mbit/s half duplex<sup>3</sup>. Pokud je však prioritou ještě větší rychlost, například 175 Mbit/s full duplex<sup>4</sup>, ceny se pohybují kolem 150 000 Kč za spoj (Ipmedia, 2014).

Je tedy na zvážení každého poskytovatele, jak velkou kapacitu spoje potřebuje, zda bude kapacitu využívat pouze pro jeden přístupový bod, nebo bude dále připojovat po metalových či optických přípojkách firmy a domácnosti.

V tomto konkrétním případě, bude v místě určení pouze jeden přístupový bod s použitím standardu 802.11a a jedna metalická přípojka. Je tedy zcela dostačující použít spoj, založený na standardu 802.11n.

Další možností je použití optických kabelů. I když samotný hardware je již velmi levný, výkopové práce, legislativa a soukromé vlastnictví pozemků vždy nedovoluje použití této varianty.

## 6.2 Praktický přínos

Tato práce shrnuje aktuálně používané technologie, které využívají jak malí a střední poskytovatelé internetu, tak uživatelé pro šíření internetu v domácnostech. Práce je významným vodítkem při nákupu bezdrátového spoje, kdy může budoucímu uživateli ušetřit peníze i čas s výběrem.

Také je zde přehlednými grafy porovnáno, které konfigurace jsou vhodnější do jakých podmínek a jaké mají vlastnosti.

---

<sup>3</sup> Způsob obousměrného přenosu dat. V half duplex komunikaci, obě zařízení mohou přijímat i odesílat, ale v jednom čase mohou buď pouze odesílat, nebo pouze přijímat. (Bagad, 2007)

<sup>4</sup> Způsob obousměrného přenosu dat. Ve full duplex komunikaci mohou obě zařízení přijímat i odesílat a to i ve stejný okamžik. (Bagad, 2007)

## 7 Literatura

- BAGAD, V.S. A I.A. DHOTRE. *Computer networks*. 1. vyd. 2007. ISBN 81-8431-194-X.
- BLEGEN, C. *What is 11AC Wi-Fi?. D-Link* [online]. 2013 [cit. 2014-11-30]. Dostupné z: <http://blog.dlink.com/what-is-11ac-wi-fi/>
- BUMBÁLEK, Z. *Modulační techniky v moderních bezdrátových sítích*. České vysoké učení technické v Praze, FEL [online]. 2010 [cit. 2014-11-30]. Dostupné z: <http://access.fel.cvut.cz/view.php?cisloclanku=2010020004>
- BUZEK, J. *Spoje „poslední míle“ na bázi technologie IEEE 802.11*. 2010. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Ivo Šmejkal.
- CARROLL, B. *CCNA wireless official exam certification guide*. Indianapolis: Cisco Press, 2008, xxviii, 473 s. Exam certification guide series. ISBN 978-1-58720-211-7.
- CFOS SOFTWARE. *hrPing*. [online]. 2014 [cit. 2014-05-11]. Dostupné z: <http://www.cfos.de/en/ping/ping.htm>
- CHEBROLU, K, RAMAN B A S SEN. *LongDistance 802.11b Links: Performance Measurements and Experience*. Kanpur, INDIA, 2006.
- ČTÚ, *Využívání vymezených rádiových kmitočtů*. [online]. 2014 [cit. 2014-11-30]. Dostupné z: <https://www.ctu.cz/ctu-informuje/jak-postupovat/radiove-kmitocty/vyuzivani-vymezeny-radiovy-ch-kmitoctu.html>
- ČTÚ, *Všeobecné oprávnění č. VO-R/12/09.2010-12*. [online]. 2010 [cit. 2014-11-30]. Dostupné z: [https://www.ctu.cz/cs/download/oop/rok\\_2010/vo-r\\_12-09\\_2010-12.pdf](https://www.ctu.cz/cs/download/oop/rok_2010/vo-r_12-09_2010-12.pdf)
- DAFNE DI ROCCO, E. *Physics of 802.11 wireless networks*. 2009. UNIVERZA V LJUBLJANI. Vedoucí práce Prof. dr. Rudolf Podgornik.
- ERGEN, M. *IEEE 802.11: Tutorial*. University of California Berkeley, 2002.
- GAST, M. *802.11 Wireless networks: the definitive guide*. 2nd ed. Sebastopol: O'Reilly, 2005, xxi, 630 s. ISBN 978-0-596-10052-0.
- GAST, M. *802.11n: a survival guide*. Sebastopol, CA: O'Reilly, 2012, 123 s. ISBN 14-493-1204-7.
- IEEE. *802.11™: Wireless LANs*. [online]. 2013 [cit. 2013-05-08]. Dostupné z: <http://standards.ieee.org/about/get/802/802.11.html>
- INTEL, *Ultimate N Wi-Fi Link 5300: Product Brief*. [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ultimate-n-wifi-link-5300-brief.pdf>
- IPERF, *The TCP/UDP Bandwidth Measurement Tool*. [online]. 2014 [cit. 2014-11-30]. Dostupné z: <https://iperf.fr>
- IPMEDIA, *Rádiový spoj ORCAVE 1S10 10 GHz*. [online]. 2014 [cit. 2014-12-20]. <http://www.ipmedia.cz/default.asp?cls=stoitem&stiid=1807>
- I4WIFI, *UBIQUITI PowerBridge M10, 10 GHz - kompletní spoj*. [online]. 2014 [cit. 2014-12-20]. <http://www.i4wifi.cz/Paterni-spoje/PowerBridge-M10-10-GHz-kompletni-spoj-precizni-anteny-28-dBi.html>



- JANSSEN, C. *Dipole Antenna*. [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://www.techopedia.com/definition/5053/dipole-antenna>
- JIROUS, *Výpočet Wi-fi*. [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://cz.jirous.com/vypocet-wifi/>
- LAMMLE, T. *CCNA wireless study guide*. Indianapolis, Ind.: Wiley Technology Pub., 2010, xxxvi, 512 s. ISBN 978-047-0901-700.
- MICHALINA, D. *Optimalizace PtMP spoje ve WLAN 802.11a,n na platformě MikroTik*. 2014. Bakalářská práce. Vysoká škola báňská – Technická univerzita Ostrava. Vedoucí práce Libor Michalek.
- MIKROTIK. *manual: Interface/Wireless*. [online]. 2014a [cit. 2014-11-30]. Dostupné z: <http://wiki.MikroTik.com/wiki/Manual:Interface/Wireless>
- MIKROTIK. *manual: WMM: How WMM works*. [online]. 2014b [cit. 2014-11-30]. Dostupné z: <http://wiki.MikroTik.com/wiki/Manual:WMM>
- MIKROTIK. *About us*. [online]. 2014c [cit. 2014-12-01]. Dostupné z: <http://www.mikrotik.com/aboutus>
- MIKROTIK. *MikroTik News*. [online]. 2014d [cit. 2014-12-01]. Dostupné z: [http://wiki.mikrotik.com/wiki/MikroTik\\_News](http://wiki.mikrotik.com/wiki/MikroTik_News)
- MIKROTIK. *manual:NV2*. [online]. 2012 [cit. 2014-11-30]. Dostupné z: <http://wiki.MikroTik.com/wiki/Manual:Nv2>
- PERAHIA, ELDAD. *IEEE 802.11n Development: History, Process, and Technology*. IEEE Communications Magazine. 2008, s. 7.
- SKIPALA, O. *Bezdrátové sítě v zarušených prostředích*. Brno, 2011. Diplomová práce. Masarykova univerzita. Vedoucí práce Eva Hladká.
- ŠLINZ, P. *Problematika vysokého zatížení bezdrátových sítí standardu 802.11b/g*. Brno, 2012. Diplomová práce. Masarykova univerzita. Vedoucí práce David Rohleder.
- UBIQUITI. *AirMAX TDMA system*. [online]. 2014a [cit. 2014-11-30]. Dostupné z: [http://dl.ubnt.com/datasheets/airmax/UBNT\\_DS\\_airMAX\\_TDMA.pdf](http://dl.ubnt.com/datasheets/airmax/UBNT_DS_airMAX_TDMA.pdf)
- UBIQUITI. *AirOS. XM.v5.5.8: Rocket M5* [Firmware]. 2014b. Dostupné z: <http://www.ubnt.com/download/>
- VÁGNER, A. *REÁLNÁ PROPUSTNOST ZARÍZENÍ PRACUJÍCÍCH NA STANDARDU 802.11N*. 2011. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Petr Münster.
- WISPA. *„Awards A Plenty” At WISPAPALOOZA*. [online]. 2014 [cit. 2014-11-30]. Dostupné z: <http://web.archive.org/web/20111108031214/http://www.wispa.org/?p=5138>



# Přílohy

## A Výstup ze skenování dostupných bezdrátových stanic v okolí spoje

Frekvence	Signal strength	Noise floor	Signal to noise	Frekvence	Signal strength	Noise floor	Signal to noise
5500	-45	109	64	5600	-73	109	36
5500	-71	109	38	5600	-76	109	33
5500	-73	109	36	5600	-76	109	33
5500	-78	109	31	5600	-81	109	28
5500	-81	109	28	5620	-64	112	48
5500	-83	109	26	5620	-65	112	47
5500	-59	109	50	5620	-79	112	33
5520	-75	111	36	5620	-85	112	27
5520	-81	111	30	5620	-87	112	25
5520	-82	111	29	5640	-43	112	69
5520	-84	111	27	5640	-70	112	42
5520	-87	111	24	5640	-81	112	31
5520	-88	111	23	5640	-87	112	25
5540	-46	111	65	5660	-36	114	78
5540	-68	111	43	5660	-80	114	34
5540	-78	111	33	5660	-80	114	34
5540	-80	111	31	5660	-82	114	32
5540	-82	111	29	5660	-85	114	29
5540	-86	111	25	5660	-90	114	24
5540	-86	111	25	5660	-46	114	68
5540	-87	111	24	5680	-48	112	64
5540	-89	111	22	5680	-65	112	47
5560	-68	112	44	5680	-79	112	33
5560	-72	112	40	5680	-79	112	33
5560	-79	112	33	5680	-81	112	31
5560	-82	112	30	5680	-85	112	27
5560	-85	112	27	5680	-85	112	27
5560	-89	112	23	5700	-71	112	41
5580	-59	112	53	5700	-74	112	38
5580	-78	112	34	5700	-75	112	37
5580	-80	112	32	5700	-80	112	32
5580	-83	112	29	5700	-81	112	31
5580	-86	112	26	5700	-82	112	30
5580	-87	112	25	5700	-83	112	29
5580	-88	112	24	5700	-85	112	27

## **B Výstup z měření v domácích podmínkách, standard 802.11n (MikroTik), NV2, TDMA 2 ms, TCP upload**

Client connecting to 192.168.0.50, TCP port 5001  
TCP window size: 1.46 MByte

```
-----  
[ 4] local 192.168.0.51 port 50835 connected with 192.168.0.50 port 5001  
[ ID] Interval   Transfer   Bandwidth  
[ 4] 0.0- 1.0 sec 2.12 MBytes 17.8 Mbits/sec  
[ 4] 1.0- 2.0 sec 128 KBytes 1.05 Mbits/sec  
[ 4] 2.0- 3.0 sec 640 KBytes 5.24 Mbits/sec  
[ 4] 3.0- 4.0 sec 2.12 MBytes 17.8 Mbits/sec  
[ 4] 4.0- 5.0 sec 3.00 MBytes 25.2 Mbits/sec  
[ 4] 5.0- 6.0 sec 3.25 MBytes 27.3 Mbits/sec  
[ 4] 6.0- 7.0 sec 4.00 MBytes 33.6 Mbits/sec  
[ 4] 7.0- 8.0 sec 4.25 MBytes 35.7 Mbits/sec  
[ 4] 8.0- 9.0 sec 5.75 MBytes 48.2 Mbits/sec  
[ 4] 9.0-10.0 sec 5.88 MBytes 49.3 Mbits/sec  
[ 4] 10.0-11.0 sec 7.00 MBytes 58.7 Mbits/sec  
[ 4] 11.0-12.0 sec 7.25 MBytes 60.8 Mbits/sec  
[ 4] 12.0-13.0 sec 5.00 MBytes 41.9 Mbits/sec  
[ 4] 13.0-14.0 sec 8.00 MBytes 67.1 Mbits/sec  
[ 4] 14.0-15.0 sec 8.25 MBytes 69.2 Mbits/sec  
[ 4] 15.0-16.0 sec 5.75 MBytes 48.2 Mbits/sec  
[ 4] 16.0-17.0 sec 6.12 MBytes 51.4 Mbits/sec  
[ 4] 17.0-18.0 sec 6.38 MBytes 53.5 Mbits/sec  
[ 4] 18.0-19.0 sec 5.00 MBytes 41.9 Mbits/sec  
[ 4] 19.0-20.0 sec 6.75 MBytes 56.6 Mbits/sec  
[ 4] 20.0-21.0 sec 6.50 MBytes 54.5 Mbits/sec  
[ 4] 21.0-22.0 sec 6.62 MBytes 55.6 Mbits/sec  
[ 4] 22.0-23.0 sec 7.00 MBytes 58.7 Mbits/sec  
[ 4] 23.0-24.0 sec 5.38 MBytes 45.1 Mbits/sec  
[ 4] 24.0-25.0 sec 7.25 MBytes 60.8 Mbits/sec  
[ 4] 25.0-26.0 sec 6.62 MBytes 55.6 Mbits/sec  
[ 4] 26.0-27.0 sec 7.62 MBytes 64.0 Mbits/sec  
[ 4] 27.0-28.0 sec 5.75 MBytes 48.2 Mbits/sec  
[ 4] 28.0-29.0 sec 7.25 MBytes 60.8 Mbits/sec  
[ 4] 29.0-30.0 sec 7.25 MBytes 60.8 Mbits/sec  
[ 4] 0.0-30.0 sec 164 MBytes 45.8 Mbits/sec
```

## **C Výstup z měření v domácích podmínkách, standard 802.11n (MikroTik), NV2, TDMA 2 ms, TCP download**

```
[ 4] local 192.168.0.51 port 5001 connected with 192.168.0.50 port 49183
[ 4] 0.0- 1.0 sec 6.23 MBytes 52.3 Mbits/sec
[ 4] 1.0- 2.0 sec 9.39 MBytes 78.8 Mbits/sec
[ 4] 2.0- 3.0 sec 8.15 MBytes 68.4 Mbits/sec
[ 4] 3.0- 4.0 sec 9.49 MBytes 79.6 Mbits/sec
[ 4] 4.0- 5.0 sec 8.22 MBytes 69.0 Mbits/sec
[ 4] 5.0- 6.0 sec 6.56 MBytes 55.0 Mbits/sec
[ 4] 6.0- 7.0 sec 6.03 MBytes 50.6 Mbits/sec
[ 4] 7.0- 8.0 sec 6.26 MBytes 52.5 Mbits/sec
[ 4] 8.0- 9.0 sec 7.37 MBytes 61.8 Mbits/sec
[ 4] 9.0-10.0 sec 8.54 MBytes 71.6 Mbits/sec
[ 4] 10.0-11.0 sec 9.59 MBytes 80.5 Mbits/sec
[ 4] 11.0-12.0 sec 8.27 MBytes 69.4 Mbits/sec
[ 4] 12.0-13.0 sec 9.39 MBytes 78.8 Mbits/sec
[ 4] 13.0-14.0 sec 7.81 MBytes 65.5 Mbits/sec
[ 4] 14.0-15.0 sec 9.38 MBytes 78.7 Mbits/sec
[ 4] 15.0-16.0 sec 7.85 MBytes 65.9 Mbits/sec
[ 4] 16.0-17.0 sec 9.47 MBytes 79.5 Mbits/sec
[ 4] 17.0-18.0 sec 7.56 MBytes 63.4 Mbits/sec
[ 4] 18.0-19.0 sec 8.52 MBytes 71.5 Mbits/sec
[ 4] 19.0-20.0 sec 7.43 MBytes 62.3 Mbits/sec
[ 4] 20.0-21.0 sec 9.26 MBytes 77.6 Mbits/sec
[ 4] 21.0-22.0 sec 8.77 MBytes 73.6 Mbits/sec
[ 4] 22.0-23.0 sec 9.39 MBytes 78.8 Mbits/sec
[ 4] 23.0-24.0 sec 8.38 MBytes 70.3 Mbits/sec
[ 4] 24.0-25.0 sec 7.72 MBytes 64.8 Mbits/sec
[ 4] 25.0-26.0 sec 7.88 MBytes 66.1 Mbits/sec
[ 4] 26.0-27.0 sec 8.86 MBytes 74.3 Mbits/sec
[ 4] 27.0-28.0 sec 8.80 MBytes 73.8 Mbits/sec
[ 4] 28.0-29.0 sec 6.62 MBytes 55.6 Mbits/sec
[ 4] 29.0-30.0 sec 7.97 MBytes 66.9 Mbits/sec
[ 4] 0.0-30.2 sec 247 MBytes 68.6 Mbits/sec
```

## D Zdrojová data pro jednotlivé grafy

Tab. 13 Srovnání jednotlivých standardů a technologií při měření v domácích podmínkách.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	8,0	7,5	457	466	6,7	6,8	357	338
2	6,2	4,8	290	489	7,3	5,0	218	231
3	38,8	35,9	129	129	29,9	39,9	7	5
4	29,1	28,8	210	211	24,6	23,7	98	94
5	35,7	32,1	166	174	31,8	30,6	52	49
6	39,6	39,3	130	128	37,7	37,2	6	5
7	29,4	27,5	209	215	24,6	21,1	96	114
8	35,9	28,2	164	180	32,7	25,2	57	64
9	41,8	29,1	131	129	38,4	23,3	7	7
10	29,4	29,3	53	54	23,8	23,9	56	35
11	36,2	36,0	47	47	32,3	32,4	40	22
12	42,3	40,1	9	5	37,9	34,4	5	4
13	123	124	36	20	67,3	54,1	12	9
14	93,1	92,3	19	18	83,7	83,9	15	10
15	99,6	79,9	7	7	72,7	63,9	4	3
16	114	104	14	12	68,6	45,8	6	5
17	95,6	94,2	137	168	94,6	95,2	110	124
18	41,5	41,3			34,1	31,7	109	126
19	95,7	95,5	124	126	94,9	95,1	117	121
20	95,6	95,6	126	122	94,8	95,0	118	95

Tab. 14 Porovnání standardu 802.11a (MikroTik) a standardu 802.11a s NV2 (MikroTik).

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	13,4	16,5	121	91	23,7	20,2	68	91
2	24,4	30,5	3	4	19,2	31,8	6	8
3	19,3	21,8	69	84	20,1	26,3	80	62
4	26,3	30,2	3	4	20,7	32,4	6	8
5	10,5	14,0	163	101	3,9	13,5	250	124
6	4,2	13,7	18	14	2,83	11,1	39	23

Tab. 15 Porovnání zařízení firmy MikroTik a UBNT na standardu 802.11n s TDMA.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	30,2	50,5	28	7	66,9	63,2	16	15
2	69,7	61,5	16	18	82,1	68,5	74	141
3	35,3	39,3	12	11	71,8	39,7	16	14
4	80,2	55,4	17	16	94,8	72,6	78	144
5	22,7	11,5	15	29	25,9	27,0	34	20
6	5,3	3,3	13	24	4,6	3,3	122	150

Tab. 16 Porovnání UBNT 802.11n se zapnutou a vypnutou funkcí AirMAX.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	57,8	66,2	67	34	65,5	79,1	200	150
2	48,1	69,8	13	21	62,5	71,4	52	139
3	93,4	66,8	26	30	95,6	75,1	80	170
4	87,4	70,1	19	21	95,3	75,4	57	145
5	53,7	11,4	57	106	22,6	5,9	233	250
6	46,2	11,9	14	17	18,5	7,9	42	148

Tab. 17 Porovnání MikroTik 802.11n se zapnutou a vypnutou funkcí NV2.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	29,7	18,5	15	34	71,0	59,2	38	70
2	30,2	50,5	28	7	66,9	63,2	16	15
3	49,8	23,9	45	96	102,0	73,9	26	178
4	35,3	39,3	12	11	71,8	39,7	16	14
5	3,8	7,0	82	19	2,9	20,5	250	198
6	22,7	11,5	15	29	25,9	27,0	34	20



Tab. 18 Porovnání MikroTik 802.11n s TDMA 1 ms a 2 ms.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	32,7	43,7	6	5	37,4	48,6	9	11
2	30,2	50,5	28	7	66,9	63,2	16	15
3	49,6	46,0	3	5	34,6	38,9	8	12
4	35,3	39,3	12	11	71,8	39,7	16	14
5	24,5	23,5	8	10	25,8	25,2	12	15
6	22,7	11,5	15	29	25,9	27,0	34	20

Tab. 19 Porovnání MikroTik 802.11n NV2 při prohození přístupového bodu a klienta.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	30,2	50,5	28	7	66,9	63,2	16	15
2	45,0	61,3	10	7	81,2	79,8	12	14
3	35,3	39,3	12	11	71,8	39,7	16	14
4	52,9	69,7	6	8	96,5	54,5	12	15
5	22,7	11,5	15	29	25,9	27,0	34	20
6	17,5	15,9	16	26	4,4	29,6	48	25

Tab. 20 Porovnání UBNT 802.11n AirMAX při prohození přístupového bodu a klienta.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	46,1	70,8	16	22	50,7	75,5	47	145
2	81,4	64,1	15	19	95,5	75,5	66	139
3	79,1	40,2	22	14	84,6	44,0	67	149
4	69,7	80,5	17	42	78,9	80,8	62	157
5	84,6	73,7	19	26	95,4	78,3	101	140
6	5,0	3,8	20	16	5,94	2,8	53	132

Tab. 21 Porovnání UBNT 802.11n se zapnutou a vypnutou funkcí Aggregation.

Číslo testu	TCP Down.	TCP Up.	Ping 1	Ping 2	UDP Down.	UDP Up.	Ping 3	Ping 4
1	29,5	23,5	5	4	46,0	27,5	40	126
2	76,0	52,2	15	16	81,5	56,7	54	136
3	34,6	24,9	6	6	47,3	35,2	40	127
4	79,4	69,7	17	25	95,2	73,8	80	150
5	12,1	7,3	7	8	25,1	6,2	80	131
6	34,2	5,4	14	15	22,5	19,8	47	140