VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Analýza PtMP spoje za použití protokolu NV2

PtMP Connection Analysis using NV2 protocol

2016 **Tomáš Jelínek**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Tomáš Jelínek**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Analýza PtMP spoje za použití protokolu NV2
PtMP Connection Analysis using NV2 protocol

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Proveďte rozbor protokolu NV2.
2. Implementujte protokol NV2 do PtMP spoje za použití platformy Mikrotik.
3. Analyzujte a zhodnoťte vhodnost protokolu oproti klasickému řešení přístupové metody (CSMA).

Seznam doporučené odborné literatury:

Documentation: MikroTik RouterOS Software. MikroTik Routers and Wireless [online]. 2012 [cit. 2013-02-06]. Dostupné z: http://www.mikrotik.com/documentation.html

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Libor Michalek, Ph.D.**

Datum zadání: 01.09.2014

Datum odevzdání: 29.04.2016

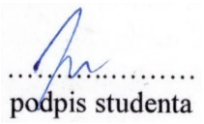
doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *9. července 2016*



Poděkování

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Liborovi Michálkovi, Ph.D., za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Abstrakt

Tato práce se zabývá doposud málo zdokumentovaným využitím protokolu NV2 v PtMP sítích 802.11 a/n na platformě Mikrotik a zkoumá, jakým způsobem lze docílit nejefektivnějšího využití rádiového spektra. V teoretické části práce je popsán protokol NV2 a rozebrán princip jeho komunikace. Je provedeno srovnání s klasickou sítí 802.11 a/n a také s často využívaným protokolem Nstreme. Dále se věnuje platformě Mikrotik a jejímu operačnímu systému RouterOS. Práce ukazuje konkrétní způsoby konfigurace těchto zařízení a popisuje stěžejní parametry nastavitelné u jednotlivých protokolů. V praktické části je sestavena testovací PtMP síť a provedena série testů ve venkovním nezarušeném prostředí. Je provedeno srovnání, jakým způsobem reagují jednotlivé protokoly na situace, ke kterým dochází v reálném provozu. Autor na základě provedených testů ukazuje, že protokol NV2 ve většině případů přináší zlepšení výkonnosti a za popsaných okolností může být dobrou investicí při potenciální inovaci sítě.

Klíčová slova

802.11a, 802.11n, Mikrotik, NV2, Nstreme, PtMP, RouterOS, RTS/CTS, bezdrátové sítě, 5GHz

Abstract

The purpose of this study is to investigate the so far scarcely documented effects of the protocol NV2 in the PtMP networks 802.11 a/n and in the Mikrotik platform in order to identify the most efficient exploitation of the radio spectrum. In a detailed theoretical section, the theses describes the protocol NV2 including its communication principle and makes a comparison with both the classical network 802.11 a/n and a frequently used protocol Nstreme. Then the detailed explanation on the platform Mikrotik as well as related operational system RouterOS is provided. Furthermore, the present study draws on the number of different configurations and key parameters which can be set for each of the protocols. In the practical section, a testing network PtMP was built up in the un-interfered outdoor environment with the aim to compare how the different protocols respond to the real life conditions. Based on the results of the tests the author concludes that protocol NV2 is in most of the cases well suited to improve performance and therefore can represent a good investment to a potential innovation of the network under the described circumstances.

Key words

802.11a, 802.11n, Mikrotik, NV2, Nstreme, PtMP, RouterOS, RTS/CTS, Wireless Networks, 5GHz

Obsah

Seznam použitých zkratek

Zkratka	Význam
AP	Universal serial bus
API	Application programming interface
BGP	Border gateway protocol
BPSK	Binary phase-shift keying
DSCP	Differentiated services code point
CLI	Command Line Interface
CPU	Central processing unit
CSMA/CA	Carrier sense multiple access with collision avoidance
ČTÚ	Český telekomunikační úřad
CW	Content window
DCF	Distributed Coordination Function
DIFS	DCF interframe space
EoIP	Ethernet over IP
GI	Guard interval
HW	Harware
IP	Internet protocol
IPSec	IP security
ISP	Internet service provider
L2	Layer 2 (Data link layer)
L2TP	Layer 2 tunneling protocol
MAC	Media access control
MCS	Modulation and coding scheme
MIMO	Multiple input and multiple output
MME	Mesh made easy protocol
MPLS	Multiprotocol label switching
MSS	Maximum segment size
NV2	Nstreme version 2
OFDM	Orthogonal frequency-division multiplexing

OSPF	Open shortest path first protocol
OVPN	Open VPN
PCF	Point Coordination Function
PIFS	PCF interframe space
PPTP	Point to point tunneling protocol
PTMP	Point to Multipoint
PXE	Preboot execution environment
PtP	Point to point
QAM	Quadrature amplitude modulation
QoS	Quality of service
RAM	Random-access memory
RIP	Routing information protocol
ROS	Router operating system (RouterOS)
RTS/CTS	Request to Send / Clear to Send
RTT	Round-trip time
SIFS	Short interframe space
SIM	Subscriber identity module
TDMA	Time division multiple access
USB	Universal serial bus
UTP	Unshielded twisted pair
VLAN	Virtual local area network
VPN	Virtual private network
Wi-Fi	Wirelles Fidelity
WPA2	Wi-Fi protected access II
x86	IBM PC kompatibilní architektura
3G	Mobilní sítě třetí generace

Seznam ilustrací a seznam tabulek

Úvod

Přístup k síti Internet pomocí bezdrátové sítě v bezlicenčním pásmu hraje v České republice významnou roli. Dle údajů ČTU je u nás v současné době přes 2200 operátorů, kteří poskytují veřejně dostupnou službu přístupu k Internetu.[1] Většina těchto operátorů působí na lokální úrovni a počet jejich zákazníků se pohybuje řádově v tisících. Velké rozšíření Wi-Fi ISP způsobila z velké části nedostatečná infrastruktura vysokorychlostních sítí, a především nízké náklady na připojení koncových uživatelů v porovnání s ostatními technologiemi.

Vysoký počet uživatelů a omezené množství přenosových kanálů však způsobuje problémy se vzájemným rušením, hlavně v hustě osídlených oblastech. Navíc Wi-Fi bylo původně vyvinuto k použití uvnitř budov, kde se zařízení vzájemně slyší. U nasazení ve venkovním prostředí však dochází k problému se skrytými uzly, tedy stanicemi, které se navzájem rádiově neslyší. Tento problém sice řeší dotazování RTS/CTS, nicméně to zvyšuje režii při přenosu. Na potřebu co nejefektivnějšího využití rádiového spektra reagují výrobci zařízení vyvíjením nových technologií. Jednou z nich je protokol NV2 od firmy Mikrotik, kterým se budu zabývat v této práci.

Práce je rozdělena do tří částí. První část je věnována stručnému úvodu do standardu 802.11a/n a popisu přístupových metod k médiu v sítích 802.11. Druhá část pojednává o platformě Mikrotik a operačnímu systému RouterOS. Dále jsou v ní popsány principy komunikace a konfigurace protokolů Nstreme a NV2. Třetí a zároveň nejobsáhlejší část práce řeší nasazení technologie NV2 do prostředí reálné sítě typu PtMP. Také jsou zde testovány výkonnostní parametry spoje a odolnost vůči rušení při nasazení technologie Nstreme a NV2 do sítí 802.11a/n. Závěrem, na základě výsledků provedeného testování, budou vyhodnoceny nejefektivnější možnosti využití platformy Mikrotik pro sítě typu PtMP.

1 Bezdrátové sítě Wi-Fi v pásmu 5 GHz

Bezdrátová síť typu Wi-Fi (Wirelles Fidelity) je typ počítačové sítě, ve které je spojení mezi jednotlivými uzly sítě uskutečňováno pomocí elektromagnetických vln. Jde o souhrnné označení bezdrátových sítí, které respektují specifikaci podle normy IEEE 802.11. Tato norma má řadu variant, lišících se parametry a schopnostmi sítí. Varianty, kterými se budeme zabývat v této práci, jsou popsány dále v textu. Správu norem pro Wi-Fi má na starosti Wi-Fi Aliance, neziskové sdružení několika set zainteresovaných společností. Wi-Fi bylo původně určeno jako náhrada metalických rozvodů místních sítí, poslední dobou se však stalo vyhledávaným způsobem pro připojení koncových uživatelů k internetu. Výhodou technologie je snadná instalace a nízké pořizovací ceny. Díky tomu jsou v ČR tyto sítě velice rozšířené. Protože je pásmo bezlicenční, není nijak regulováno množství zařízení, využívajících toto přenosové pásmo. Z toho plyne i jejich hlavní nevýhoda v podobě vysokého využití přenosového pásma, způsobující vzájemné rušení. Zařízení musí splňovat podmínky sepsané ČTÚ, například dodržet maximální vyzářený výkon a komunikační frekvence. Kompletní podmínky pro provoz Wi-Fi v pásmu 5 GHz jsou vypsány ve všeobecném oprávnění VOR/12/09.2010-12.[2]

1.1 Standard IEEE 802.11a

Tato norma vznikla v roce 1999 jako reakce na velké zarušení pásma 2,4 GHz a popisuje požadavky na zařízení pracující v pásmu 5 GHz. V ČR je provozováno na frekvencích 5150-5250 MHz pro použití uvnitř budov a 5470-5725 MHz pro použití i venku. Toto pásmo je rozděleno do tří podpásem s rozdílnými podmínkami provozu. K dispozici je celkem 19 nepřekrývajících se kanálů (8 vnitřních, 11 venkovních) s šířkou 20 MHz.

Při přenosu je použita technika OFDM (Orthogonal Frequency Division Multiplexing), které se využívá u mnoha bezdrátových technologií. Princip spočívá v rozdělení frekvenčního pásma do 56 úzkých podkanálů (pro přenos dat je použito 48) s menší bitovou rychlostí, do nichž je dělena informace. Mezi vysílání jednotlivých symbolů je vložen ochranný interval (GI), který zabraňuje rámcům, vysílaným delší cestou (např. kvůli odrazům), aby kolidovaly s rámci, které přišly kratší cestou. Každý podkanál je dále kódován jednou z modulací BPSK, QPSK, 16-QAM nebo 64-QAM, dle úrovně přijatého signálu a odstupu signálu od šumu. Rychlost komunikace v závislosti na použité modulaci je zobrazena v tabulce 1.1, přičemž maximum je 54 Mbps. Používá se přístupová metoda CSMA, která bude vysvětlena níže.[3]

Tabulka 1.1: *Přehled rychlostí v 802.11a*

Modulace	Kódový poměr	Počet všech bitů na podkanál	Počet bitů na OFDM symbol	Počet dat. bitů na OFDM symbol	Přenosová rychlost [Mbps]
BPSK	1/2	1	48	24	6
BPSK	3/4	1	48	36	9
QPSK	1/2	2	96	48	12
QPSK	3/4	2	96	72	18
16-QAM	1/2	4	192	96	24
16-QAM	3/4	4	192	144	36
64-QAM	1/2	6	288	192	48
64-QAM	3/4	6	288	216	54

1.2 Standard IEEE 802.11n

Norma vznikla v roce 2009, kvůli potřebě uspokojit stále stoupající datové nároky dnešních aplikací a je zamýšlena jako bezdrátová alternativa Fast Ethernetu.[4] Zařízení je možno provozovat v pásmu 2,4 i 5 GHz a je zachována kompatibilita se staršími standardy 802.11 a/b/g. Nejpomalejší připojená stanice však způsobí zpomalení celého vysílače. Klíčovými vlastnostmi standardu 802.11n jsou MIMO (Multiple Input Multiple Output), využití 40 MHz kanálu a technika shlukování rámců na MAC podvrstvě.

MIMO technologie používá více vysílacích a přijímacích antén. Více antén umožňuje více samostatných přenosů, tzv. prostorový multiplex. Signál je rozdělen do několika proudů a ty se vysílají do více antén na stejném kanálu. MIMO technologie počítá s vícecestným šířením signálu. Vícecestné signály jsou odražené signály, které přicházejí do přijímače s určitým zpožděním oproti signálům v přímém směru. V případě, že signály dorazí do přijímače z různých prostorových směrů, je možno je navzájem oddělit a propustnost se tím násobí. U sítí založených na standardu 802.11a/b/g bylo vícecestné šíření chápáno jako interference degradující schopnost přijímače obnovit z přijatého signálu obsaženou informaci. MIMO používá diverzitu vícecestných signálů ke zvýšení schopnosti přijímače obnovit ze signálu požadovanou informaci.

Při přenosu je opět použita technika OFDM, byl však zvýšen počet podkanálů na 52 pro 20MHz kanál, a na 108 podkanálů pro kanál šířky 40 MHz. Byla přidána také možnost snížení ochranného intervalu na polovinu, čímž se dosáhne toho, že rámec bude odeslán dřív. Rychlosti jsou určovány dle tzv. MCS (Modulation Coding Scheme), a pro pásmo 5 GHz jsou uvedeny v tabulce 1.2. Tabulka znázorňuje prvních 16 indexů, se kterými budeme pracovat v další části práce.[5][6]

Tabulka 1.2: *Přehled MCS schémat pro frekvence 5 GHz*

Index MCS	Počet antén	Typ modulace	Kódovací poměr	Přenosová rychlost [Mbps]			
				20 MHz kanál		40 MHz kanál	
				GI 800 ns	GI 400 ns	GI 800 ns	GI 400 ns
0	1	BPSK	1/2	6,5	7,2	13,5	15
1	1	QPSK	1/2	13	14,4	27	30
2	1	QPSK	3/4	19,2	21,7	40,5	45
3	1	16-QAM	1/2	26	28,9	54	60
4	1	16-QAM	3/4	39	43,3	81	90
5	1	64-QAM	2/3	52	57,8	108	120
6	1	64-QAM	3/4	58,5	65	121,5	135
7	1	64-QAM	5/6	65	72,2	135	150
8	2	BPSK	1/2	13	14,4	27	30
9	2	QPSK	1/2	26	28,9	54	60
10	2	QPSK	3/4	39	43,3	81	90
11	2	16-QAM	1/2	52	57,8	108	120
12	2	16-QAM	3/4	78	86,7	162	180
13	2	64-QAM	2/3	104	115,6	216	240
14	2	64-QAM	3/4	117	130	243	270
15	2	64-QAM	5/6	130	144,4	270	300
…							
31	4	64-QAM	5/6	260	288,9	540	600

1.3 Přístupové metody v bezdrátových sítích Wi-Fi

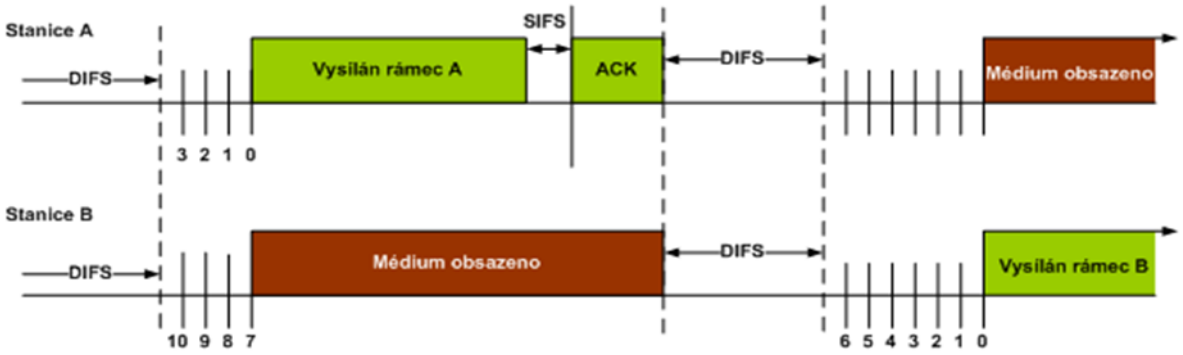
Jelikož bezdrátové sítě využívají k přenosu dat sdílené médium (vzduch), je třeba zabezpečit, aby nedocházelo k nežádoucím situacím, jako ztráta či poškození dat, kolize, atp. a zároveň přístup k médiu řídit. V době, kdy sdílené médium používá jedno zařízení, nesmí je používat žádné jiné. Cílem je přidělit sdílené médium zařízení do výlučného použití na omezenou dobu, potřebnou pro přenos jednoho rámce. Po jejím uplynutí je médium uvolněno a může být přiděleno jinému zařízení. U sítí 802.11 se o řízení přístupu k médiu stará MAC podvrstva linkové vrstvy. Podle intervalu přístupu k médiu rozdělujeme přístupové metody na deterministické (lze určit maximální časový interval, ve kterém se stanice dostane k médiu) a stochastické (nelze zaručit časový interval, stanice musí čekat). Testováním sítí s různými přístupovými metodami se budeme zabývat v praktické části práce.

1.3.1 CSMA/CA

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) je stochastická přístupová metoda, která nepoužívá centrální autoritu, ale všechny uzly sítě jsou si při soutěži o médium rovny. Je založená na principu, kdy každá stanice před vysíláním paketu určitý čas poslouchá, zda je přenosové médium volné. Pokud ano, stanice počká náhodně zvolenou dobu, a pokud do té doby médium neobsadí jiná stanice, odvysílá rámec a poté čeká na potvrzení. V opačném případě čeká na konec probíhajícího vysílání. Standardy definují u sítí 802.11 dvě základní varianty řízení přístupu. DCF (Distributed Coordination Function), která je povinná a PCF (Point Coordination Function), volitelná a implementovaná jen u některých výrobků.

DCF je založena na přístupové metodě CSMA/CA a lze ji využít u sítí typu ad-hoc a infrastructure. Jsou zde zavedeny 2 konstanty, SIFS (určuje dobu, do které musí příjemce nepoškozeného rámce odeslat potvrzení) a DIFS (doba, která musí uplynout po uvolnění média, než bude možné zahájit další přenos). Metoda pracuje s tzv. oknem soutěžení (CW). Pokud má stanice data k odeslání, detekuje, zda je médium volné. Pokud ano, počká, než uplyne DIFS, vygeneruje náhodné číslo z intervalu <0, CW> a začne odpočítávat. Během odpočítávání neustále kontroluje, zda je médium volné. Pokud ne, je odpočítávání zastaveno a pokračuje opět až po uvolnění média. Po ukončení odpočítávání stanice odešle rámec a čeká na potvrzení. Pokud potvrzení nedorazí, znamená to, že došlo ke kolizi. Interval, ze kterého se volí náhodné číslo, se zdvojnásobí a začíná nové odpočítávání. Princip komunikace je znázorněn na obrázku 1.1. DCF neobsahuje žádný mechanismus pro prioritizaci přístupu k médiu. [7][8]

PCF je kombinací dvou přístupových metod (CSMA/CA a pooling) a lze ji využít jen u sítí typu infrastructure s přístupovým bodem, který plní roli centrální autority. Tyto metody se pravidelně střídají. U metody pooling se AP postupně dotazuje koncových stanic, zda mají něco k přenosu. Pokud stanice do doby SIFS nezareaguje, AP po uplynutí doby PIFS osloví další stanici. [9]



Obrázek 1.1: *Princip DCF [7]*

1.3.2 **RTS/CTS**

RTS/CTS je rozšíření přístupové metody CSMA/CA, které řeší problém skrytých a předsunutých uzlů. Sítě 802.11 byly původně určeny do interiéru a při návrhu standardu se počítalo s tím, že se všechny komunikující stanice navzájem uslyší a budou tudíž schopny detekovat případné obsazení média jednou z nich. Ve venkovním prostředí, při použití směrových antén a spojů na dlouhé vzdálenosti v členitém terénu, nelze zaručit, že stanice bude schopna detekovat obsazení média jinou stanicí. Tento problém řeší následujícím způsobem právě mechanismus RTS/CTS.

Uzel, který chce vysílat, vyšle do svého okolí zprávu RTS (Request to Send). V ní sdělí, s kým chce komunikovat a jak dlouho. Příjemce povolí komunikaci zprávou CTS (Clear to Send). Všechny ostatní uzly se na dobu vysílání odmlčí. Zprávy RTS/CTS musí být vysílány nejnižší přenosovou rychlostí, aby je mohly zachytit všechny stanice. To snižuje propustnost, a proto je mechanismus většinou používán pro rámce až od určité velikosti (parametr RTS threshold). Pravděpodobnost vzniku kolize u přenosu malých rámců je totiž nízká, protože jsou odeslány rychle. [9]

1.3.3 **TDMA**

TDMA (Time Division Multiple Access) je deterministická metoda přístupu ke sdílenému médiu, kde se o řízení komunikace stará centrální autorita (AP). Všechna zařízení používají pro komunikaci společný frekvenční kanál, dělený do mnoha časových slotů. Klientské stanice komunikují jedna po druhé a každá používá pro komunikaci vlastní slot. To zabraňuje kolizím a umožňuje stanicím sdílet stejný přenosový kanál. Přiřazování časových slotů je možné řídit také dynamicky, dle různých algoritmů. [10] Tento typ řízení používá i protokol NV2, kterým se budeme zabývat v této práci.

2 Platforma Mikrotik

Mikrotik je lotyšská firma, založená v roce 1996, se sídlem v hlavním městě Riga. Zabývá se vývojem a prodejem bezdrátových systémů pro ISP v mnoha zemích po celém světě. Od roku 1997 vyvíjí operační systém pro routery označený jako RouterOS a v roce 2002 začala s výrobou vlastního HW pro tento operační systém. Od té doby se portfolio jejích produktů značně rozšířilo a společnost se stala významných hráčem na poli výrobků pro ISP i koncové zákazníky. Společnost pořádá po celém světě konference MikroTik User Meeting (MUM), kde prezentuje své stávající i budoucí produkty a nové technologie. Úplně první konference se konala 19. 1. 2006 v Praze, kam zavítala od té doby ještě dvakrát, v roce 2009 a 2015. To ilustruje velké rozšíření bezdrátových sítí v ČR a důležitost místního trhu pro tuto firmu. Dnes má společnost 160 zaměstnanců a neustále rozšiřuje produktovou nabídku a vývoj ROS. [11]

2.1 RouterBOARD

RouterBoard je obchodní značka firmy Mikrotik, pod kterou prodává vlastní HW určený pro počítačové sítě (např. Wi-Fi routery, switche, antény, bezdrátové karty a různá příslušenství). Jako Routerboardy se však spíše označují základní desky od firmy Mikrotik, které se dají rozšířit pomocí různých doplňků (Wi-Fi karty, paměti, antény, SIM karty atp.).

RouterBOARDy obsahují CPU, RAM a dle typu integrovanou síťovou kartu a různé porty pro připojení doplňkových zařízení. Dodávají se s předinstalovaným ROS, který dokáže plně využít jejich schopností, ale v případě potřeby na nich lze provozovat i jiné systémy linuxové distribuce. Lze je využít samostatně např. jako routery nebo jako součást modulárního systému, kde ve spojení s různými anténami fungují jako bezdrátové přístupové body nebo klientské stanice. Na obrázku 2.1 je pro ilustraci znázorněn RouterBOARD RB411GL s jedním ethernetovým portem a miniPCI slotem, který je osazen bezdrátovou kartou RouterBOARD R52Hn. Dále je k dispozici 1 neosazený USB port, který může sloužit např. k připojení 3G modemu pro zálohování konektivity. Routerboard je umístěn v instalační krabici za sektorovou anténou a celý komplet je možno nasadit jako AP pro síť typu PtMP.

Obrázek 2.1: *Osazený RouterBOARD RB411GL*

2.2 RouterOS

RouterOS (ROS) je routerový operační systém založený na linuxovém jádru v3.3.5, vyvíjený firmou Mikrotik od roku 1997. Primárně se využívá na Routerboardech, ale díky jeho linuxovému jádru je zaručena jeho podpora i na jiném HW (x86, Alix, atp.). Dodává se jako součást Routerboardů nebo jej lze zakoupit jako samostatnou licenci.

2.2.1 Instalace

ROS je distribuován ve formě balíčků NPK, které jsou buď předinstalované na HW typu RouterBOARD, nebo je nutné je do zařízení nainstalovat. Existuje několik verzí balíčků pro různé HW platformy (mipsbe, mipsle, smips, tile, ppc, arm, x86). U x86 systémů je také možno využít instalace pomocí ISO souboru. Instalace na vestavěný systém se provádí pomocí programu Netinstall, určeného pod Windows. Zařízení se propojí s PC UTP kabelem a aktivuje se na něm bootování z ethernetu. V programu Netinstall zvolíme balíčky pro příslušnou HW platformu, nastavíme IP adresu ze stejného rozsahu, jako má PC, zapneme PXE server a po nabootování dojde automaticky k instalaci systému. [12]

Licence pro ROS existuje v několika verzích, je časově neomezená (kromě L0, která slouží na odzkoušení a je aktivní po dobu 24 hodin) a nabízí neomezený upgrade na nové verze. Licence L3 se nabízí pouze jako předinstalovaná součást zařízení RouterBOARD a její hlavní omezení je, že nenabízí možnost režimu bezdrátový přístupový bod. Licence L4-L6 jsou na tom z hlediska počtu funkcí stejně, ale u nižších verzí L4 a L5 jsou některé funkce limitovány (omezení počtu tunelů, VLAN, front, atp.). Licence je nepřenosná a platí jen pro zařízení, na kterém byla poprvé aktivována. [13]

2.2.2 Konfigurace

ROS je možné konfigurovat a spravovat několika způsoby. První a nejvíce používanou metodou je připojení pomocí programu Winbox, určeného pod Windows. Pomocí tohoto graficky orientovaného programu je možno nastavovat většinu funkcí pohodlně myší a klávesnicí. Program se neustále vyvíjí a je možné jej stáhnout na webu Mikrotiku. Ukázka prostředí programu je na obr. 2.2.

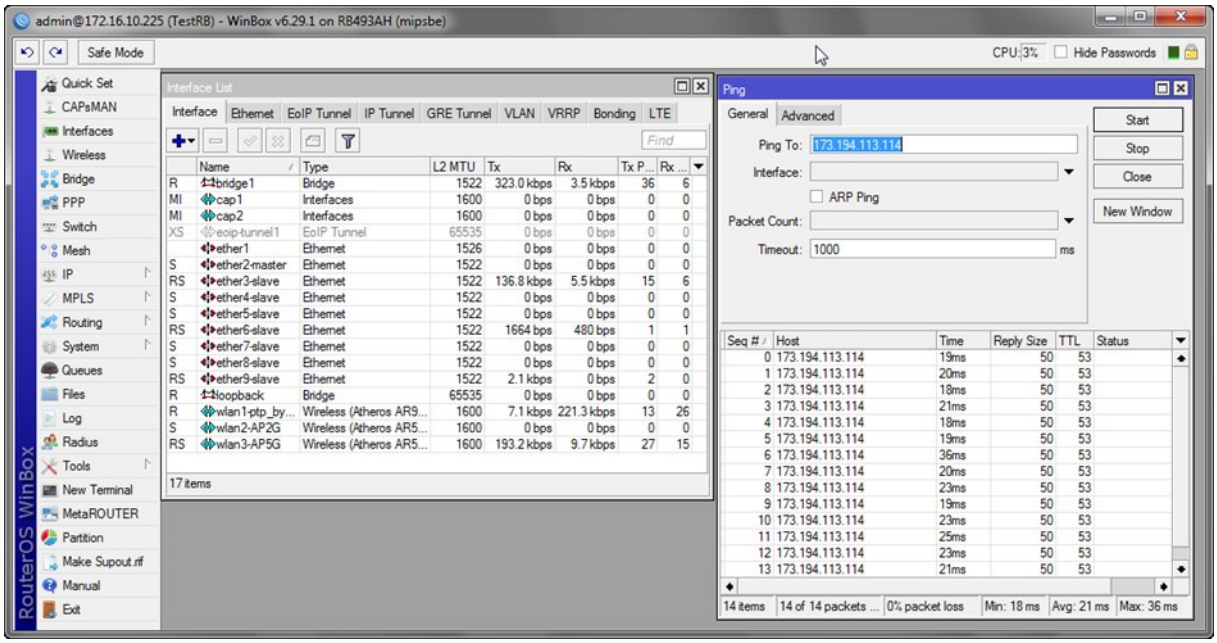
Další možností je využít webového rozhraní Webfig, které v posledních verzích dosáhlo značného pokroku a nyní je funkčně v podstatě totožné s Winboxem, navíc není omezené nutností používat OS Windows.

Dále je možné využít API, pomocí kterého můžeme ROS ovládat z aplikací třetích stran.

Poslední možností je využití pokročilého CLI, pomocí něhož lze nastavit veškeré funkce ROS. Konfigurace probíhá pomocí textových příkazů a je možno využít nápovědu a doplňování příkazů přes klávesu Tab. Tímto způsobem se dá připojit k ROS protokolem Telnet, SSH, z lokální konzole nebo prostřednictvím sériového portu, pokud ho zařízení obsahuje. Následující příklad demonstruje způsob zadávání příkazu pomocí CLI a slouží k přiřazení IP adresy bezdrátovému rozhraní routeru.

```
[admin@TestRB] > ip address add address=192.168.1.1 netmask=24
interface=wlan1
```

Pokud nemá zařízení přidělenou IP adresu, je možno ke spojení využít speciální protokol komunikující na L2 a připojit se k zařízení pomocí nástrojů Mac-Telnet a Mac-Winbox, což jsou ekvivalenty výše uvedených nástrojů.



Obrázek 2.2: *Ukázka prostředí Winbox*

2.2.3 Oblasti využití

Jak už bylo řečeno, systém ROS se skládá z balíčků, které do něj přidávají rozličné funkce, potřebné pro konkrétní využití zařízení. ROS podporuje mnoho funkcí, mezi nejzákladnější lze zmínit následující: [14]

- Bezpečnostní Firewall (pravidla podobná iptables), Omezující Firewall (QoS)
- VPN (Tunel) Server/Klient s podporou protokolů PPTP, L2TP, OVPN, EoIP, IPsec
- Wi-Fi zařízení v režimech AP, Klient, WDS (Podpora protokolů 802.11abgn)
- Kompletní Hotspotové řešení včetně realizace plateb, Proxy server
- Bridge, Router s podporou dynamických protokolů (RIP, OSPF, BGP, MME)

2.3 Protokol Nstreme

Nstreme je proprietární protokol firmy Mikrotik, který byl vyvinut pro zlepšení bezdrátových spojů typu PtP a PtMP. Provozovat je ho možné výhradně na zařízeních se systémem ROS (AP i klientské stanice) a je funkční jen na kartách s čipem Atheros AR5210 a novějších (CM9, R52,…).

2.3.1 Princip

Protokol nepoužívá přístupovou metodu CSMA/CA, které je běžná u komunikace dle standardu 802.11, ale řešení nazývané pooling. AP se postupně dotazuje připojených klientů, jestli mají nějaká data na odvysílání. Tím se snižuje přístupová doba, protože klientská stanice nemusí, před započetím vysílání, detekovat volné médium. Zároveň tím odpadá problém se skrytými uzly.

Další technikou, kterou využívá Nstreme, je sdružování rámců. Přenášené rámce jsou sdružovány do jednoho velkého a přeneseny najednou. To má za následek snížení režie a díky tomu zvýšení rychlosti přenosu, za cenu mírného zvýšení latence. Možnosti nastavení sdružování rámců jsou popsány v následující části.

Díky implementovaným technikám dochází u bezdrátových spojů, využívajících protokolu Nstreme, ke zvýšení propustnosti, spoje je možno provozovat i na velké vzdálenosti a se zvyšováním vzdálenosti nedochází k výraznému snižování rychlosti. Spoj se rovněž dokáže dynamicky přizpůsobovat aktuálním parametrům přenosu. Testování protokolu Nstreme v síti PtMP se budeme věnovat v praktické části práce. [16]

2.3.2 Nastavení v RouterOS

Množina parametrů, které lze u protokolu Nstreme v ROS nastavit, je podobná jako u 802.11, některé nastavení se však při provozu ignorují, podrobnější informace naleznete ve [15]. V rámci tematického vymezeni této práce se budeme věnovat jen parametrům, které ovlivňují chování protokolu Nstreme. [16]

- Enable pooling – Zapíná přístupovou metodu pooling.
- Disable CSMA – Pokud je zapnutý pooling, vypíná přístupovou metodu CSMA. Klientské stanice zbavuje povinnosti poslouchat, zda je médium před vysíláním volné. Zvyšuje propustnost spoje, ale v zarušeném prostředí může způsobit výrazné zhoršení kvality.
- Framer policy – Určuje, jakým způsobem dochází ke sdružování rámců. Při odesílání se rámce řadí do fronty a dle tohoto parametru jsou odesílány. Pokud je fronta prázdná, karta nečeká a rámce odesílá okamžitě. Tím se eliminuje nárůst zpoždění při nízkém provozu.
- None - Sdružování rámců není aktivní
- Best fit – Dochází ke sdružování do velkého rámce do maximální velikosti určené parametrem Framer Limit. Nedochází ke fragmentaci.
- Exact size – Dochází ke sdružování do velkého rámce do maximální velikosti určené parametrem Framer Limit. Pokud se rámec do tohoto velkého rámce nevejde, je fragmentován a odeslána je jen jeho část. Zbylá část se pošle v dalším velkém rámci. Tato volba (s parametrem Framer Limit nastaveném na nejvyšší hodnotu) poskytuje nejvyšší propustnost, mírně však zvyšuje zpoždění.
- Framer limit – Určuje maximální velikost sdruženého rámce.

2.4 Protokol Nstreme Dual

Protokol Nstreme Dual (Nstreme2) je další z proprietárních řešení firmy Mikrotik a je nadstavbou protokolu Nstreme. Toto řešení je určeno pro spoje typu PtP a pracuje s dvojicí bezdrátových karet na každé straně, jedna vysílá a druhá přijímá. Jeho výhoda spočívá v tom, že každý směr komunikace probíhá na jiné frekvenci a lépe se plánuje nastavení kanálů na jednotlivých vysílačích s ohledem na rušení v daném místě. Pro připojení se používají buď dvě samostatné antény, nebo jedna dvou polarizační, s velkou izolací mezi konektory. I přes nesporné výhody se od využívání tohoto protokolu poslední dobou upouští a realizace PtP spojů se přesouvá na plně duplexní spoje pracující na frekvenci 10 GHz a vyšší. V této práci se proto tímto protokolem zabývat nebudeme. [16]

2.5 Protokol NV2

Protokol NV2 (Nstreme v2) je nejmladším proprietárním řešením přístupu k médiu od firmy Mikrotik. Stejně jako protokol Nstreme jej není možno provozovat na zařízení od jiného výrobce. Je založen na technologii TDMA a podporuje všechny bezdrátové karty s chipem Atheros pro sítě 802.11n. Pro sítě 802.11 a/b/g je zabudována podpora od verze AR5212. Protokol se neustále vyvíjí a dá se předpokládat, že v budoucnu přibydou další funkce, jako např. časová synchronizace mezi přístupovými body. [17]

2.5.1 Princip

Přístup k médiu je v sítích s protokolem NV2 řízen AP. Ten rozděluje čas na pevně dané úseky, které se dále dynamicky dělí na části pro downlink (data se odesílají směrem ke klientským stanicím) a uplink (data se odesílají směrem k AP), toto rozdělení je závislé na stavu front na AP a klientských stanicích. Úsek pro uplink je dále dělen mezi připojené klientské stanice v závislosti na jejich požadavcích na přenosové pásmo. Na začátku každého úseku pošle AP všem připojeným klientským stanicím harmonogram, kde jim přidělí přesné časové okno, kdy mohou vysílat.

Pro připojení nový klientský stanic k AP je v časovém úseku pro uplink pravidelně vysíláno speciální časové okno, ve kterém mohou nepřipojené klientské stanice požádat o registraci k AP. Následně je klientské stanici přiděleno vlastní okno pro dokončení registrace a započetí vysílání.

Jelikož NV2 nepoužívá technologii CSMA, může docházet k vzájemnému rušení se sítěmi vysílajícími na stejném kanále. Zařízením, které nepodporují NV2, se totiž jejich komunikace jeví jako šum. [17]

2.5.2 Srovnání NV2 s 802.11

U protokolu NV2, na rozdíl od klasické 802.11, řídí přístup k médiu AP. To eliminuje problémy se skrytými uzly a umožňuje centralizované řízení, kdy AP přiděluje každé klientské stanici prostor k vysílání individuálně, dle určitých zásad. Tím se zefektivňuje komunikace, protože klientské stanice nemusí soupeřit o přístup k médiu a snižuje se tak režie komunikace. NV2 používá selektivní potvrzování rámců. To zlepšuje propustnost hlavně u spojů na delší vzdálenost, protože se nemusí s vysíláním následujícího rámce čekat, než dorazí potvrzení od právě odeslaného. Díky technice sdružování rámců se snižuje režie spojená s odesláním každého rámce. [17]

2.5.3 Srovnání NV2 s Nstreme

U sítí s protokolem NV2 distribuuje AP klientským stanicím harmonogram vysílání pomocí vysílání typu broadcast. Tím, že nemusí s každou stanicí komunikovat individuálně, dochází k úspoře času, který je možno použít k přenosu dat. Zároveň to umožňuje, aby AP nastavil každé stanici okno pro uplink individuálně, v závislosti na odhadu vzdálenosti stanice. To zvyšuje propustnost, zvláště u sítí typu PtMP. Díky vestavěné podpoře QoS a možnosti měnit délku úseků pro komunikaci mezi AP a klientskou stanicí, je u sítí s nasazeným protokolem NV2 větší možnost kontroly nad zpožděním v síti. [17]

2.5.4 QoS u NV2

Protokol NV2 obsahuje vlastní implementaci mechanismu QoS. Je založena na proměnlivém počtu front, kterým je přiřazena různá priorita. Zpracování front vychází z definice v 802.1D-2004. Nejdříve jsou odeslány všechny rámce z fronty s nejvyšší prioritou a následně dochází, sestupně dle priority, k odbavení rámců z dalších front. To může mít za následek zablokování rámců u front s nejnižší prioritou. Při plánování politiky QoS je tedy třeba postupovat obezřetně.

Nastavení QoS je řízeno AP, klientské stanice od něj nastavení přebírají. Defaultně používá NV2 dvě fronty. V tomto režimu jsou všechny odchozí rámce zpracovány vlastním algoritmem protokolu, založeném na typu a velikosti paketů. Volitelně je možno zvýšit počet front na 4 nebo 8 a rozdělení rámců do front řídit dle nastavené priority. Ta se nastavuje přímo v ROS, nevkládá se do hlavičky paketů a je tak dostupná jen uvnitř systému. Mechanismus řazení do front, dle nastavené priority, je zobrazen v tabulce 2.1. S pakety, které nemají nastavenu žádnou prioritu, se pracuje jako by měli nastavenu prioritu 0. Všimněme si, že pakety s touto prioritou jsou řazeny do fronty 2 a jsou tím pádem upřednostněny před pakety s prioritou 1 a 2. Na to je třeba si při nastavování priority dát pozor.

Prioritu je možno nastavit buď firewallovými pravidly (eventuálně v bridge filter u sítí na L2) přímo na konkrétní hodnotu nebo nepřímo z příchozích rámců (VLAN priorita, MPLS EXP). Další možností je nastavit prioritu z DSCP v hlavičce paketu. Tímto způsobem je možno šířit nastavení QoS v celé síti. Na hraničním routeru se nastaví DSCP značkování a všechny AP s protokolem NV2 si nastaví prioritu z DSCP a dle ní řadí rámce do příslušných front. [17]

Tabulka 1.3: *Mechanismus řazení do front u QoS na protokolu NV2*

Počet front = 2	Počet front = 4	Počet front = 8
Priority 0,1,2,3 > fronta 0	Priority 0,1 > fronta 0	Priorita 0 > fronta 2
Priority 4,5,6,7 > fronta 1	Priority 2,3 > fronta 1	Priorita 1 > fronta 0
	Priority 4,5 > fronta 3	Priorita 2 > fronta 1
	Priority 6,7 > fronta 4	Priorita 3 > fronta 3
		Priorita 4 > fronta 4
		Priorita 5 > fronta 5
		Priorita 6 > fronta 6
		Priorita 7 > fronta 7

2.5.5 Nastavení v RouterOS

Stejně jako u protokolu Nstreme je hodně parametrů společných se sítěmi 802.11. Je zde ovšem více parametrů, které neovlivňují chování systému a ignorují se, podrobnější informace naleznete ve [15]. Zde se budeme opět věnovat jen parametrům, které souvisejí s protokolem NV2. Kromě nastavení zabezpečení se vše nastavuje jen na AP a klientská stanice se konfiguraci sama přizpůsobí.

- Queue Count – Specifikuje, kolik prioritních front bude použito, je možno zadat 2, 4, 8.
- QoS – Určuje, zda bude pro řazení rámců do front použit vnitřní algoritmus (jsou využívány jen 2 fronty, nastavení default), nebo zda bude použito řazení dle priorit (nastavení frame priority).

- Cell Radius – Udává vzdálenost nejvzdálenější stanice v kilometrech, nejmenší hodnota je 10 km. Toto nastavení má vliv na velikost časového okna, rezervovaného pro připojení nových stanic a pro odhad vzdálenosti stanice. Vzdálenější stanice potřebují více času, než se k nim signál dostane a v případě krátkého intervalu na AP, by nebyly schopny se připojit. V podmínkách ČR většinou nedochází ke komunikaci na tak dlouhé vzdálenosti, takže se ponechává na minimální hodnotě, aby AP zbytečně neplýtvalo rezervovaným časem.
- Tdma Period Size – Udává velikost časového úseku v milisekundách, v rámci něhož dochází k dělení pro uplink a downlink pro jednotlivé stanice, výchozí hodnota je 2 ms. Pokud ji snížíme, klesne zpoždění, ale i propustnost, protože vzroste režie protokolu. Zvýšení způsobí nárůst zpoždění i propustnosti a používá se u spojů na dlouhé vzdálenosti. Zde velkou část doby, určené k přenosu, zabere zpoždění při přenosu signálu ke stanici a zpět a na přenos dat zbývá poměrově malý úsek. Pokud máme v ROS nainstalovaný balíček WirelessFP, je možno nastavit i hodnotu auto a velikost určuje systém automaticky. To umožňuje na nevytížených spojích dosáhnout nízké hodnoty zpoždění, aniž bychom přišli o propustnost, při zvýšení zatížení.
- Nv Security – V sítích s protokolem NV2 není použit mechanismus zabezpečení z klasické 802.11. Tento parametr udává, zda se bude používat vlastní mechanismus zabezpečení, podobný WPA2.
- Nv2 Preshared Key – Bezpečnostní klíč, který je nutné zadat stejný na AP i klientské stanici. Z toho klíče jsou odvozeny klíče k šifrování dat.

3 Praktická část práce

V předchozí části byly shrnuty teoretické poznatky o bezdrátových sítích WiFi v pásmech a/n a principy fungování jednotlivých protokolů. Nyní přijde na řadu praktické ověření získaných znalostí pomocí série testů. Celá kapitola je strukturována do několika částí. Nejdříve bude představeno a stručně popsáno HW zařízení použité pro realizaci testovací PtMP sítě. Dále budou zmíněny nástroje, sloužící k měření sledovaných parametrů sítě, včetně jejich možných nastavení. Následně práce popisuje sestrojenou PtMP síť. Poté následují kapitoly vztahující se k jednotlivým měřením, které jsou dále členěny dle jednotlivých protokolů.

3.1 Použitý hardware

3.1.1 Routerboard SXT Lite5ac

Routerboard SXT Lite5ac je venkovní jednotka pro pásmo 5 GHz fungující ve standardu a/n/ac. Jednotka obsahuje jeden 100MBit ethernetový port a duální anténu o zisku 16 dBi s pokrytím 28°. Zajímavostí je přítomnost druhého bezdrátového rozhraní na frekvenci 2,4 GHz, které slouží na správu zařízení např. pomocí notebooku nebo mobilního telefonu (podporuje jen 1 spojení). Jednotku je možno využít pro páteřní spoj na krátké vzdálenosti, častější je však využití pro připojení k AP v klientském režimu, což bude i náš případ.

3.1.2 Routerboard LHG 5

Routerboard LHG 5 je novinka od firmy Mikrotik, jedná se o venkovní jednotku pro pásmo 5 GHz fungující ve standardu a/n. Jednotka obsahuje jeden 100MBit ethernetový port a duální parabolickou anténu o zisku 24 dBi s pokrytím 7°. Výhodou je zabudování rádiové části přímo do ohniska antény, čímž odpadají ztráty na RF kabelech. Jednotku je možné, vzhledem k parametrům, využít jako páteřní spoj do méně zarušených oblastí nebo pro připojení k AP v klientském režimu.

3.1.3 Routerboard RB912UAG-5HPnD

RouterBOARD RB912UAG-5HPnD je základní deska od firmy Mikrotik. Deska obsahuje mimo jiné integrovaný gigabitový ethernetový port a 5 GHz modul fungující ve standardu a/n. Pro připojení k MIMO anténě slouží 2 MMCX konektory. Součástí desky je licence L4 ROS a je tudíž vhodná pro použití jako přístupový bod k připojování klientských stanic. V tomto režimu bude využívána i při testovacích měřeních.

Obrázek 3.1: *Použitý hardware. Zleva SXT Lite5ac, LHG 5 a RB912UAG*

3.1.4 Antény RFE SH-TP

SH-TP 5 je řada sektorových anténa pro pásmo 5GHz od slovenské firmy RF Elements. Jedná se o skalární antény, jejichž vyzařovací diagram je symetrický ve vertikální a horizontální rovině. Antény mají vzhledem ke své konstrukci velmi dobré potlačení bočních a zadních laloků a vyrovnaný zisk pro celé spektrum využitelných frekvencí. Díky tomu se hodí jako antény na přístupový bod do zarušených oblastí nebo do míst, kde je třeba použít velký vertikální úhel pokrytí. Vyrábí se s úhly pokrytí od 30 do 90 stupňů. V testovací síti budou využity modely s pokrytím 30 a 60 stupňů. Pro připojení k aktivním jednotkám slouží twistport adaptér.

3.1.5 Twistport adaptér stíněný pro Routerboard

Twistport adaptér je zařízení od firmy RF Elements sloužící k připojení aktivních zařízení od firem Mikrotik, UBNT a Cambium Networks k anténám vybavených konektorem twistport. Konektor umožňuje rychlé a bezztrátové spojení a rozpojení antén a jednotek. V testovací síti bude použit adaptér pro Routerboard ve stíněné verzi, která zlepšuje odolnost mezi rušením zařízení, umístěných blízko u sebe na jednom stožáru.

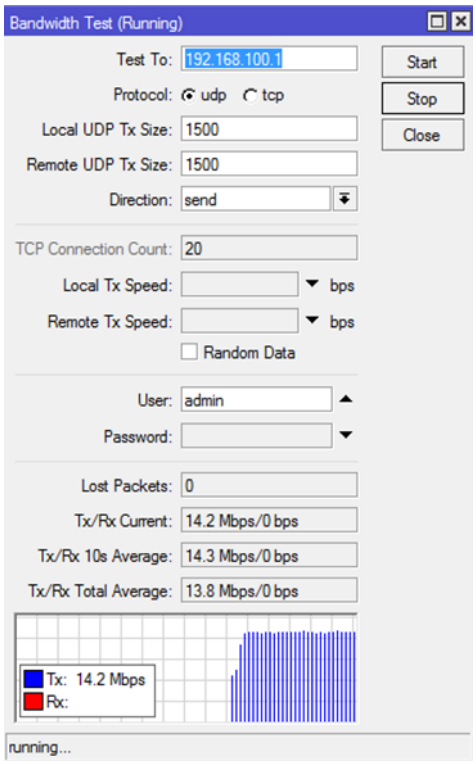
Obrázek 3.2: *Anténa RFE SH-TP 30 s osazeným Twistport adaptérem*

3.2 Použitý software

3.2.1 Mikrotik Bandwith test

Mikrotik Bandwith test je proprietární nástroj na testování propustnosti sítě a je součástí každého operačního systému ROS v menu Tools. Pokud máme postavenou celou síť na produktech od Mikrotiku, můžeme si jednoduše otestovat aktuální propustnost kteréhokoliv segmentu sítě. Pro testování z PC je k dispozici i verze pro Windows. Nástroj funguje na principu klient-server a lze jej použít na testování UDP i TCP protokolu. Server je v ROS implicitně zapnutý, takže k zahájení testu je třeba spustit klientskou část a vyplnit IP adresu s přihlašovacími údaji serveru. Dále je třeba navolit parametry testu. Na obrázku 3.3 je ukázáno nastavení pro testování UDP provozu. Nadefinovat lze velikost UDP paketů, směr datového toku, rychlost datového toku (pokud tato položka nebude zvolena, bude generován maximální datový tok, který je schopná síť přenést) a volba pro náhodný obsah paketů (pro zamezení vlivu komprese paketů). Po spuštění pak ihned vidíme aktuální datovou propustnost testovacího spoje, která se zanáší do grafu. Do statistiky se také zapisuje průměrná

rychlost za posledních 10 vteřin a celkově. U testování TCP provozu není možné nastavovat velikost paketů, ale místo toho můžeme nastavit počet paralelně probíhajících TCP spojení. Při testování UDP protokolu jsou do přenosu započítány i IP a UDP hlavičky, u TCP jen samotná data. V naší síti budeme používat tento nástroj pro testování UDP propustnosti mezi AP a klientskými stanicemi.



Obrázek 3.3: *Testování UDP přenosu programem Mikrotik Bandwith Test*

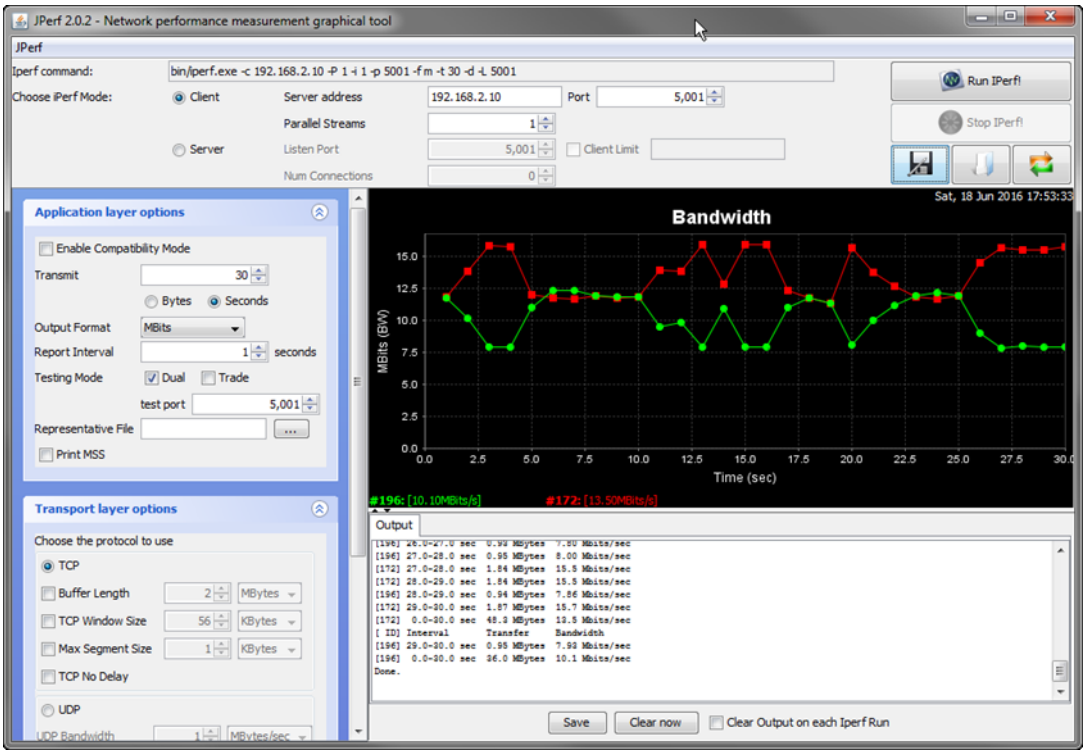
3.2.2 The DUDE

The DUDE je program od firmy Mikrotik pro monitorování a správu síťových zařízení. Je určen především pro produkty s operačním systémem ROS, u kterých nabízí největší škálu funkcí, ale dají se s ním monitorovat i zařízení jiných výrobců, jako například switche, routery, servery, tiskárny atp. Program je rozdělen na serverovou a klientskou část. Serverová část se instaluje jako balíček do ROS a je určena jen pro zařízení s procesorem architektury x86, TILE a ARM. Klientská část se instaluje jako program pod Windows. Ve starší verzi byla i možnost instalace serverové části pod Windows, ta však není s novou verzí kompatibilní. Mezi jeho klíčové funkce patří automatické mapování sítě a vytváření schémat, analýza a monitoring zařízení, generování upozornění skrze protokoly SNMP, ICMP, DNS a TCP a přímý přístup k nástrojům pro správu zařízení. V testovací síti bude tento program spuštěn pod virtuálním prostředím na PC a bude využíván především pro rychlý přístup ke konfiguraci jednotlivých zařízení a jako GUI pro testování spektra.

3.2.3 JPerf

Nástroj JPerf je grafická nástavba oblíbeného nástroje IPerf. Ten slouží pro testování propustnosti sítě pro UDP a TCP protokol. GUI zajišťuje spuštění nástroje Iperf se zadanými parametry a následně zobrazuje grafy z výsledků měření. Jedná se o multiplatformní nástroj napsaný v jazyce JAVA. Nástroj funguje opět v režimu klient-server. Na obrázku 3.4 je ukázáno nastavení pro

testování obousměrného TCP provozu. Nadefinovat lze velikost MSS, okna TCP a bufferu. Je možno zvolit, zda chceme testovat spoj jednosměrně, obousměrně nebo postupně v každém směru, a dále pak množství přenesených dat nebo délku přenosu. Po spuštění se nám začne vykreslovat graf přenosu a ukládat aktuální přenosová rychlost v zadaných intervalech. Po skončení přenosu je vypočítána průměrná rychlost. Tento nástroj bude v testovací síti použit pro testování propustnosti TCP protokolu mezi AP a 1 stanicí.



Obrázek 3.4: *Testování TCP přenosu programem JPerf*

3.2.4 Fping

Nástroj Fping je pokročilou verzí známého programu ping, který posílá ICMP Echo Request pakety na vzdálené zařízení a čeká na ICMP Echo Reply. Fping nabízí stejné funkce jako klasický ping, ale má také několik funkcí navíc. Umožňuje například měnit čas mezi jednotlivými „pingy“, zvukově signalizovat neúspěšné přijetí odpovědi a ukládat výsledky do souboru. V této práci bude využita především jeho funkce testování více zařízení současně. Je možné nastavit buď seznam, anebo rozsah IP adres, na které jsou posílány pakety, a program po dokončení vypočítá průměrnou odezvu na všechna testovaná zařízení. Pakety na jednotlivá zařízení jsou buď odesílány postupně, anebo je každému přiřazeno vlastní vlákno a jsou testovány paralelně.

3.3 Sestavení PtMP sítě

Nyní přistoupím k samotné realizaci testovací sítě. Bylo potřeba splnit tři podmínky. Za prvé docílit toho, aby testovací síť co nejvíce odpovídala podmínkám reálného nasazení. Proto jsem zvolil měření v exteriéru a použití jednotek k tomu určených. Za druhé bylo nutné najít místo, kde nebude žádné rušení v pásmu 5 GHz, aby bylo dosaženo maximální výkonnosti zařízení, a měření nebylo ovlivněno jinými sítěmi. A nakonec bylo třeba docílit toho, aby se daly realizovat všechny

naplánované testy. Například při měření se skrytými uzly to znamenalo umožnit takové rozmístění zařízení, aby klientské stanice měly přímou viditelnost na AP a zároveň neslyšely samy sebe navzájem. Nakonec se podařilo najít vhodnou lokalitu v podobě rozlehlé louky na odlehlém místě, bez přítomnosti jakéhokoliv rušení z cizích sítí. Tato louka se nachází v osadě Kývalka poblíž Brna a je využívána jako sezónní kemp pro návštěvníky nedalekého Masarykova okruhu. Na pozemku je umístěna dlouhá budova, která byla využita jako zázemí při měření, jež bylo časově poměrně náročné. Zároveň skýtala možnost variabilního uspořádání testovaných zařízení, tak aby vyhovovalo podmínkám jednotlivých měření.

Základ sítě tvořily dva přístupové body. Použity byly základní desky RouterBOARD RB912UAG-5HPnD namontované do stíněného Twistport adaptéru, které byly dle potřeby osazeny sektorovými anténami SH-TP 30 nebo SH-TP 60. K přístupovým bodům bylo připojeno 10 stanic, 7ks Routerboard LHG 5 a 3 ks Routerboard SXT Lite5ac. Všechna zařízení byla zároveň propojena UTP kabelem do Gigabitového switche, do kterého byly též zapojeny 2 testovací notebooky. Na jednom PC běžel ve virtuálním prostředí ROS pro x86 procesory, na němž byl spuštěn monitorovací program DUDE. Rozmístění jednotlivých zařízení se měnilo dle potřeb testů a bude popsáno u každého měření zvlášť. Do všech zařízení od Mikrotiku byl nahrán nejnovější ROS verze stable 6.34.6 a byl proveden upgrade firmware. Měřící pracoviště je znázorněno na obr. 3.5.

Obrázek 3.5: *Měřící pracoviště při měření odezvy a propustnosti*

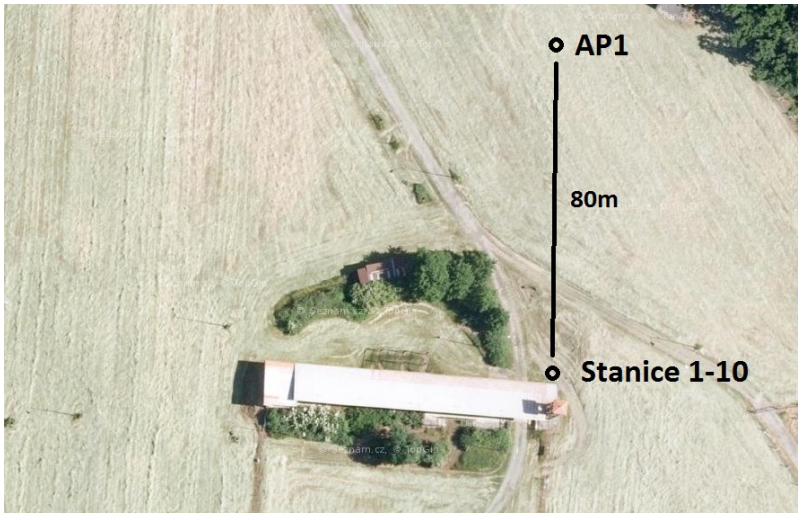
3.4 Nastavení měřících nástrojů a sítě

Pokud není v textu uvedeno jinak, je nastavení měřících nástrojů a důležitých parametrů testovací sítě následující.

- Bandwith Test: Protocol UDP, Směr TX/RX/TX+RX, velikost paketů 1500, trvání 60s
- FPing: posílá se 50 paketů o velikosti 50 bajtů generovaných po 300ms
- JPerf: počet spojení 1 a 20, trvání 30s, ostatní hodnoty default
- 802.11a/n: rychlost 54/54 a 144/144 Mbps, HW retries 7, disable RTS/CTS, ostatní default
- Nstreme: enable pooling, disable CSMA, best fit 3200
- NV2: auto TDMA period size, Cell Radius 10km, Queue 2, QoS default

3.5 Měření odezvy

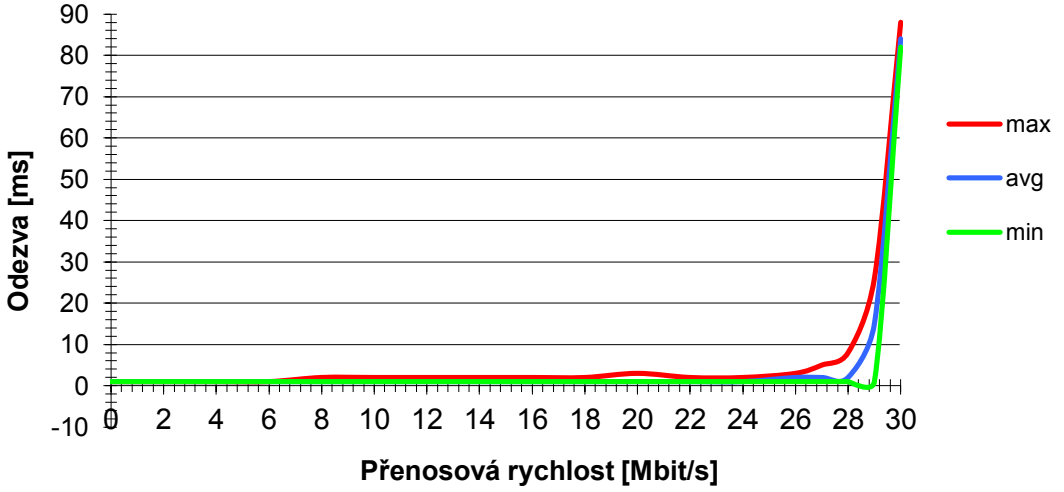
Prvním provedeným měřením byla závislost odezvy na přenosové rychlosti. Odezva (anglicky round-trip time RTT) je v počítačových sítích doba, která uplyne od vyslání paketu do přijetí odpovědi na něj. Je to jeden ze základních ukazatelů pro popis chování sítě. Rozmístění zařízení testované sítě je znázorněno na obr. 3.6. Před samotným měřením byla provedena kontrola spektra na AP i stanicích pomocí spektrálního analyzátoru zabudovaného v jednotkách pro ověření, že v okolí nevysílá žádné jiné zařízení, viz Příloha B: Všechny stanice byly připojeny na AP se signálem v rozmezí -45 až -55 dB a během testu si udržovaly maximální TX/RX rate, dle zvoleného standardu. Měření bylo provedeno z důvodu dosažení maximální rychlosti jen na jednu stanici. Ostatní byly připojeny do sítě, ale neprobíhala na nich žádná komunikace. Na generování přenášených dat byl použit nástroj Bandwith Test pro UDP protokol, přenos probíhal směrem ke stanici. Rychlost se postupně zvyšovala od nuly až po maximální přenosovou rychlost, které byla schopna síť v dané konfiguraci dosáhnout. Pro každou rychlost byl po ustálení spuštěn program Fping a byla zaznamenána minimální, maximální a průměrná odezva. Odezva byla u všech měření zaokrouhlena na milisekundy, což je pro měření na WiFi sítích dostačující přesnost.



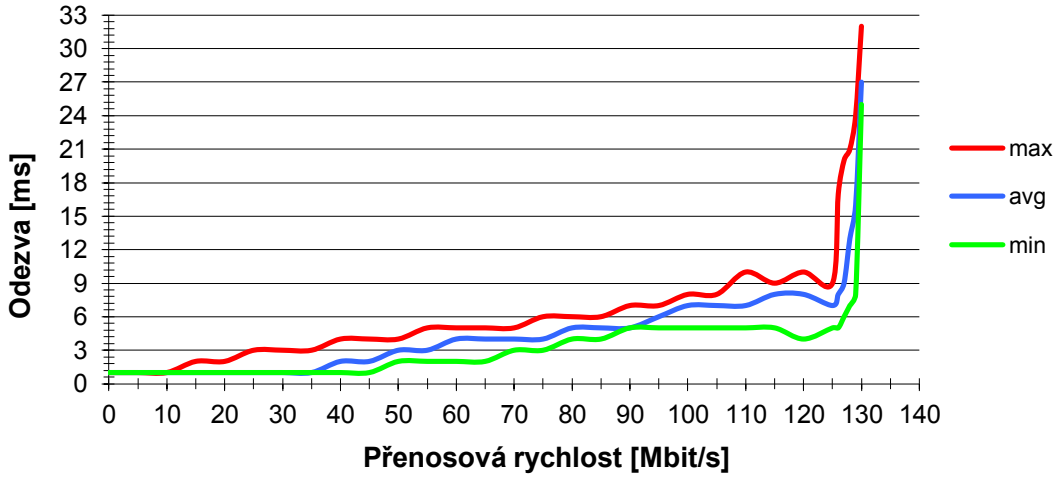
Obrázek 3.6: *Testovací síť při měření odezvy a propustnosti*

3.5.1 **802.11**

Na obr. 3.7 je znázorněna změna odezvy při zvyšování přenosové rychlosti u sítě 802.11a. Odezva se drží na minimálních hodnotách až do okamžiku dosažení rychlosti 29 Mbit/s. Po té prudce stoupne na hodnotu 85 ms. Toto zvýšení je způsobeno frontou na výstupním bezdrátovém rozhraní. Zde se začnou hromadit pakety, které není zařízení schopno odesílat v momentě dosažení maximální přenosové kapacity bezdrátového spoje. Ta je v uvedeném případě 30 Mbit/s. Průběh odezvy u sítě 802.11n je znázorněn na obrázku 3.8. Zde se odezva s rostoucí přenosovou rychlostí postupně zvyšovala až do dosažení rychlosti 127 Mbit/s, kdy se opět prudce zvýšila z důvodu zaplnění fronty. Maximální dosažená rychlost byla 130 Mbit/s a průměrná odezva u této rychlosti se pohybovala kolem hodnoty 30 ms, což je výrazný pokles proti průměrné hodnotě u sítě 802.11a.



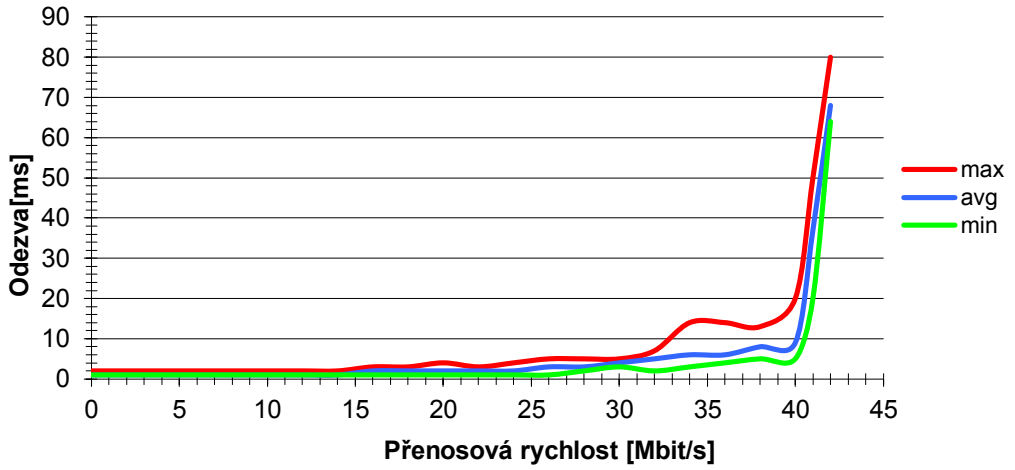
Obrázek 3.7: *Závislost odezvy na přenosové rychlosti u 802.11a*



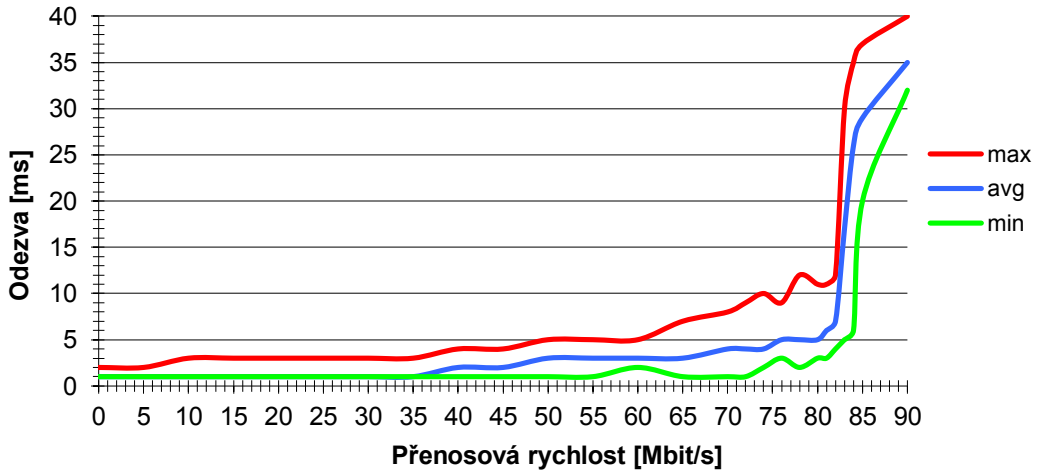
Obrázek 3.8: *Závislost odezvy na přenosové rychlosti u 802.11n*

3.5.2 Nstreme

Průběh odezvy u protokolu Nstreme pro sítě 802.11a je znázorněn na obr. 3.9. Je dosaženo zvýšení maximální propustnosti na 42 Mbit/s a mírného nárůstu zpoždění. To je způsobeno technikou sdružování rámců, která je vysvětlena v kapitole 2.3.1. U sítí 802.11n došlo naopak ke snížení maximální propustnosti, která se pohybuje na hodnotě 92 Mbit/s. Je to pravděpodobně způsobeno neodladěním protokolu Nstreme, který vznikl dříve než standard 802.11n. Graf průběhu odezvy ukazuje obr. 3.10.



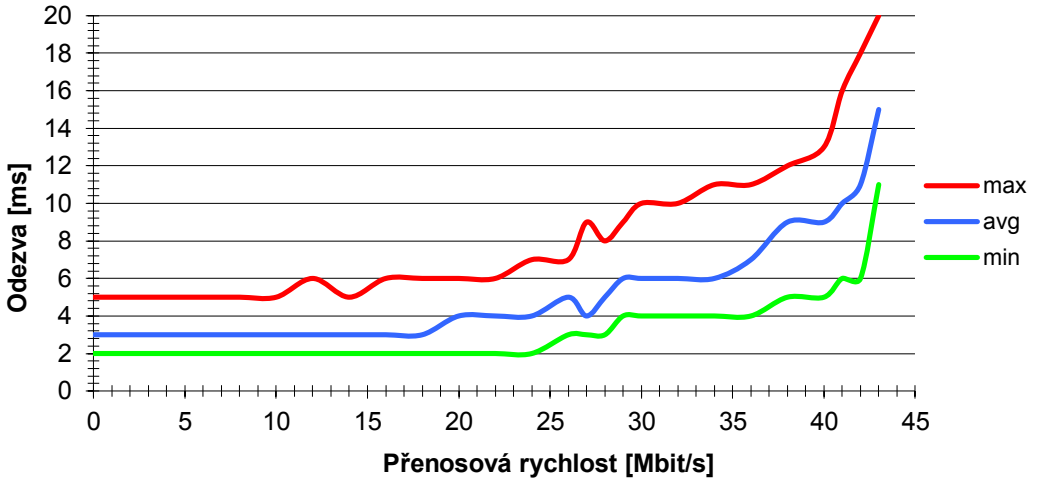
Obrázek 3.9: *Závislost odezvy na přenosové rychlosti u 802.11a Nstreme*



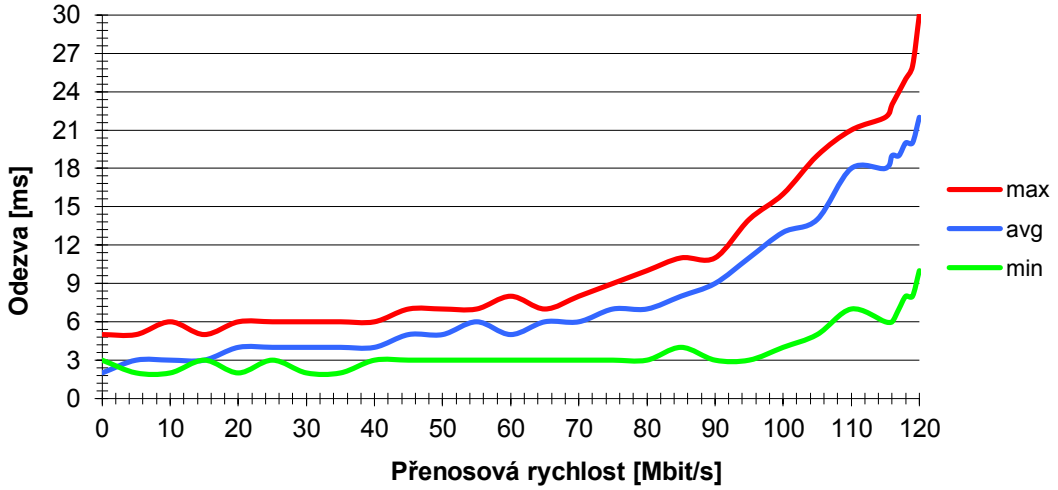
Obrázek 3.10: *Závislost odezvy na přenosové rychlosti u 802.11a Nstreme*

3.5.3 NV2

Na obr. 3.11 je znázorněn průběh odezvy pro protokol NV2 u sítí 802.11a. Nejvyšší naměřená rychlost je 42 Mbit/s. Nedochází zde ke skokovému zvýšení odezvy při dosažení maximální kapacity spoje, ale průměrná odezva se postupně zvyšuje od 2 do 15 ms. To je dosaženo díky vestavěnému mechanismu QOS a přístupové metodě TDMA. Graf průběhu odezvy pro síť 802.11n je znázorněn na obr. 3.12. Průběh závislosti na rychlosti je podobný jako u sítě 802.11a. Maximální dosažitelná rychlost je 120 Mbit/s.



Obrázek 3.11: *Závislost odezvy na přenosové rychlosti u 802.11a NV2*



Obrázek 3.12: *Závislost odezvy na přenosové rychlosti u 802.11n NV2*

3.5.4 Srovnání protokolů

Z předchozích vyobrazení průběhů odezvy vyplývá, že nejvyšší přenosové rychlosti dosahuje klasická síť 802.11n, její nevýhodou je skokové zvýšení odezvy při dosažení maximální kapacity spoje. Tento problém řeší nasazení protokolu NV2, který za cenu nepatrného snížení propustnosti podstatně zlepšuje průběh odezvy. Zatím je však předčasné činit závěry o vhodnosti nasazení určitého protokolu na základě jediného testu.

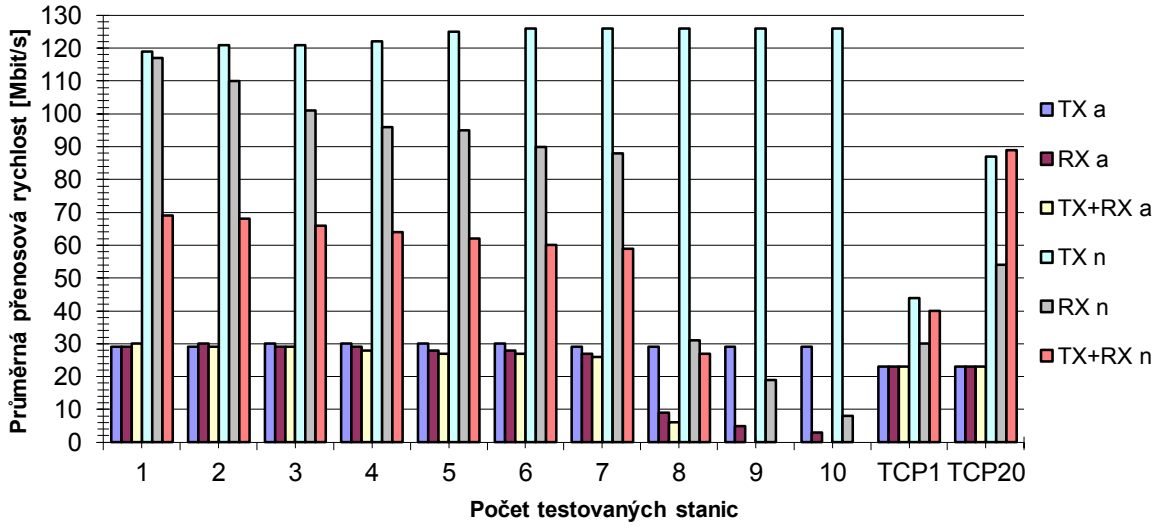
3.6 Měření propustnosti PtMP sítě

Po zjištění maximální propustnosti dosahované jednotlivými protokoly a průběhu odezvy se budu zabývat závislostí přenosové rychlosti na počtu komunikujících stanic. Topologie sítě zůstala stejná jako v předchozím případě. Test byl opět zrealizovaný pomocí nástroje Bandwith Test, generováním UDP přenosu. Rychlost však nebyla omezená a vždy se testovalo nejvyšší možnou rychlostí. V ROS na AP jsme si vytvořili skripty pro test na každou stanici ve směru TX, RX a TX/RX. Každý test trval 1 minutu. Začalo se s testováním jedné stanice a postupně se zvyšoval

počet stanic, až nakonec komunikovaly všechny. Testy byly spouštěny paralelně a zaznamenávala se celková průměrná dosažená rychlost všech testovaných stanic. Po ustálení přenosu, cca 5 vteřin po začátku měření, byl spuštěn Fping a byla zaznamenána průměrná odezva na všechny právě testované stanice. Dále byl proveden test TCP přenosu pro jedno a dvacet generovaných spojení. Jelikož TCP test pomocí nástroje Bandwith test vytěžuje CPU zařízení na 100 %, a měření by tak mohlo být zkreslené, byl k tomuto testu použit nástroj JPerf. Za testovanou stanici byl připojen notebook se spuštěným programem v roli serveru. Na druhém notebooku, který byl připojen přes switch k AP, byla spuštěna klientská část programu a prováděno testování. Tento test byl proveden jen pro jednu stanici a slouží pro srovnání, jak si jednotlivé protokoly poradí s TCP přenosem.

3.6.1 **802.11**

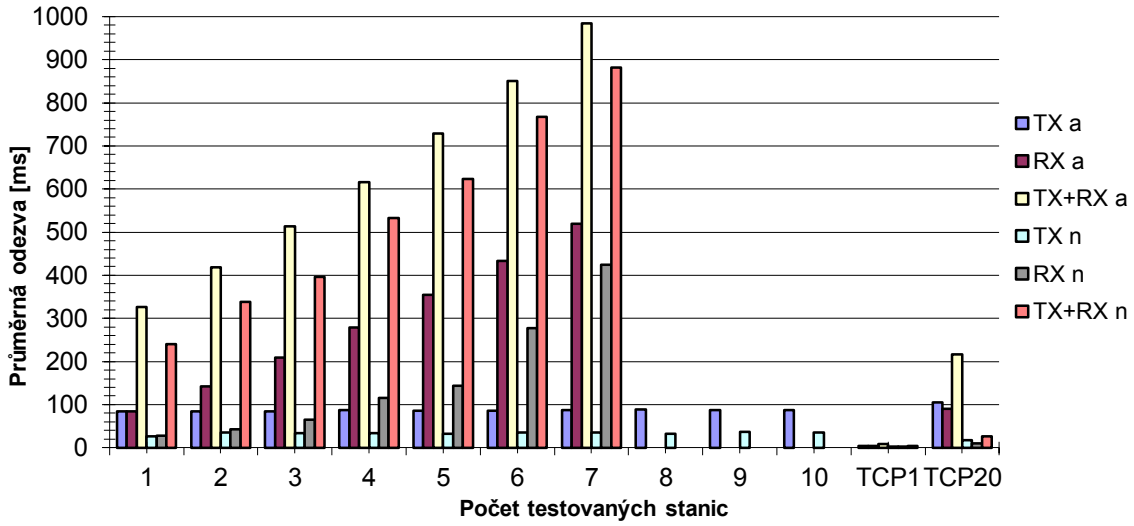
Na obr. 3.13 je vidět závislost průměrné přenosové rychlosti sítě na počtu komunikujících stanic. Tentokrát je graf společný pro sítě 802.11a/n. Na první pohled nás zaujmou dvě skutečnosti. Za prvé, že maximální kapacita spoje nedosahuje hodnot zjištěných v předchozím měření. To je způsobeno tím, že náběh na plnou rychlost při měření nástrojem Bandwith Test chvíli trvá. Průměrná rychlost se však vypočítává z celé doby měření, takže dochází k mírnému zkreslení. Proto také při měření na více stanicích paralelně dle grafu rychlost jakoby roste, i když se v reálu nemění. Tato mírná odchylka však nevadí, protože se vyskytuje u všech měření a nám jde především o vzájemné porovnání hodnot. Druhou skutečností, která je na první pohled patrná, je skokové snížení uploadu při zahájení komunikace osmé stanice. Zde kvůli vysvětlení trochu odbočíme od tématu. Poslední tři jednotky s označením 8, 9, 10 jsou vybaveny novějším chipsetem QCA9882 pro komunikaci dle standardů 802.11a/n/ac. Jednotky 1-7 obsahují chipset AR9344 pro komunikaci dle 802.11a/n, tedy stejné řady jako AP s chipsetem AR9342. Za uvedené problémy může pravděpodobně určitá nekompatibilita, která se projevuje právě u sítí s klasickou 802.11. Změna verze ROS neměla na funkci žádný vliv. U ostatních protokolů k problémům nedocházelo, takže jednotky byly v testovací síti ponechány a výsledky u 802.11 pro stanice 8-10 nebudou zahrnuty do srovnání.



Obrázek 3.13: *Závislost rychlosti na počtu stanic u 802.11a/n*

Nyní se vraťme zpět k měření. Rychlost downloadu se nemění, rychlost uploadu s přibývajícím počtem komunikujících stanic klesá. U testu TCP je vidět, že i jedno spojení je schopno

vytížit kapacitu sítě 802.11a pro TCP přenos na maximum, která je 23Mbit/s. U sítě dle 802.11n, je třeba pro dosažení vyšší rychlosti větší počet spojení.



Obrázek 3.14: *Závislost odezvy na počtu stanic u 802.11 a/n*

Na obr. 3.14 je zobrazena závislost průměrné odezvy na počtu komunikujících stanic. U downloadu se odezva nemění a odpovídá hodnotě změřené v předchozím testu. U uploadu hodnota se zvyšujícím počtem stanic lineárně roste. Je to způsobené soupeřením o přístup k médiu. Z grafu je také patrná velmi nízká hodnota zpoždění u TCP přenosu po jednom spojení. Odezvy u stanic 8-10 pro RX a TX/RX přenos nebyly do grafu z výše popsaného důvodu zahrnuty.

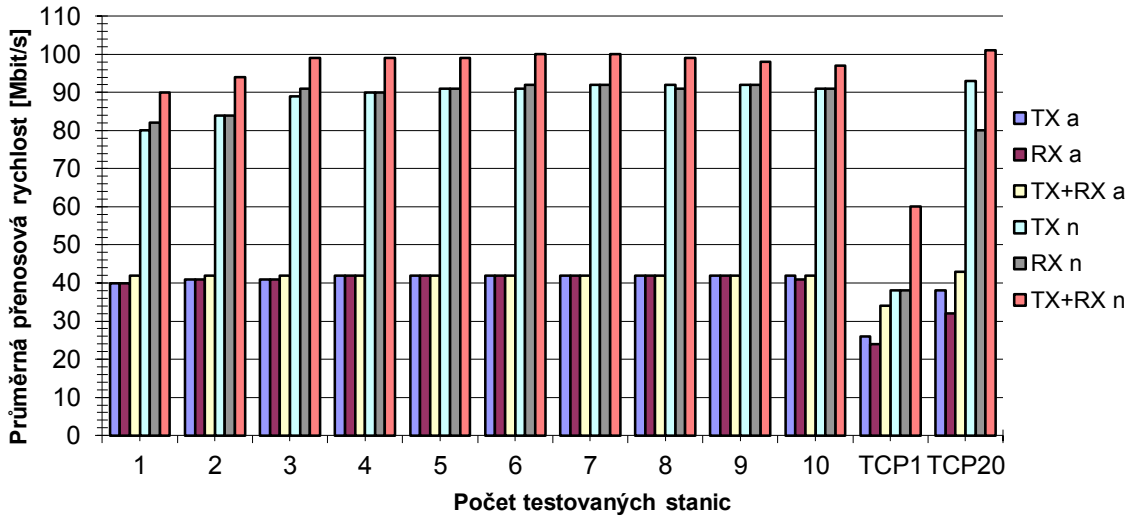
3.6.2 Nstreme

Vliv počtu komunikujících stanic na dosaženou rychlost u protokolu Nstreme je zobrazen v grafu na obr. 3.15. U sítě dle 802.11a jsou rychlosti vyrovnané a změna počtu stanic nemá na rychlost žádný vliv. U sítě dle 802.11n opět nedochází k žádné změně rychlosti, navíc celková rychlost při obousměrném přenosu mírně převyšuje rychlost jednosměrného přenosu. Podobné zlepšení je patrné i u TPC přenosu. Při dvaceti spojeních se maximální rychlost blíží rychlosti dosažené UDP protokolem. Závislost průměrné odezvy na počtu komunikujících stanic je zobrazena na obr. 3.16. Průběh je podobný jako v předchozím případě u klasické 802.11, dosažené odezvy jsou však nižší.

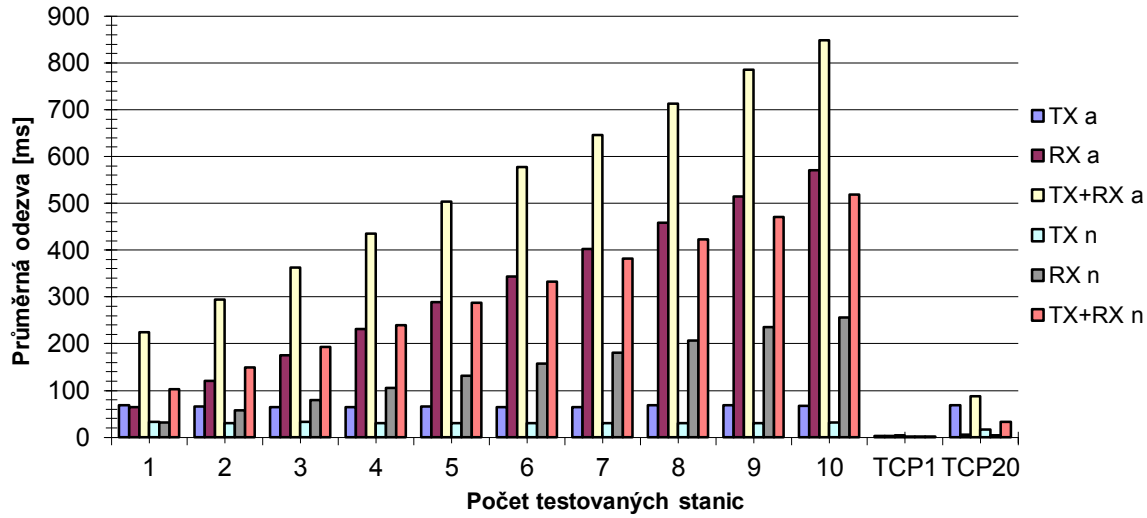
3.6.3 NV2

Závislost přenosové rychlosti na počtu komunikujících stanic pro poslední testovaný protokol nalezneme na obr. 3.17. Na první pohled je patrné výrazné snižování rychlosti downloadu s přibývajícím počtem komunikujících stanic. Při deseti stanicích je propustnost pro oba standardy přibližně poloviční. U uploadu dochází též ke snižování, ale není tak výrazné. Toto chování je důsledkem nízké hodnoty TDMA Period Size. Je možné ji nastavit v intervalu 1-10 ms nebo na automatiku, která byla použita v tomto měření. Informace o tom, jak automatické nastavování funguje, není k dispozici. Nicméně lze vysledovat, že preferuje spíš nižší odezvu na spoji než dosažení maximální přenosové rychlosti. Pokud tento parametr nastavíme na maximální hodnotu 10 ms, snižování rychlosti nebude tak výrazné, ale dojde k několikanásobnému nárůstu odezvy. Její průběh

pro nastavení TDMA Period Size na automatiku nalezneme na obr. 3.18. Z grafu je patrné, že odezva se drží na velmi nízkých hodnotách pro všechny varianty přenosu.



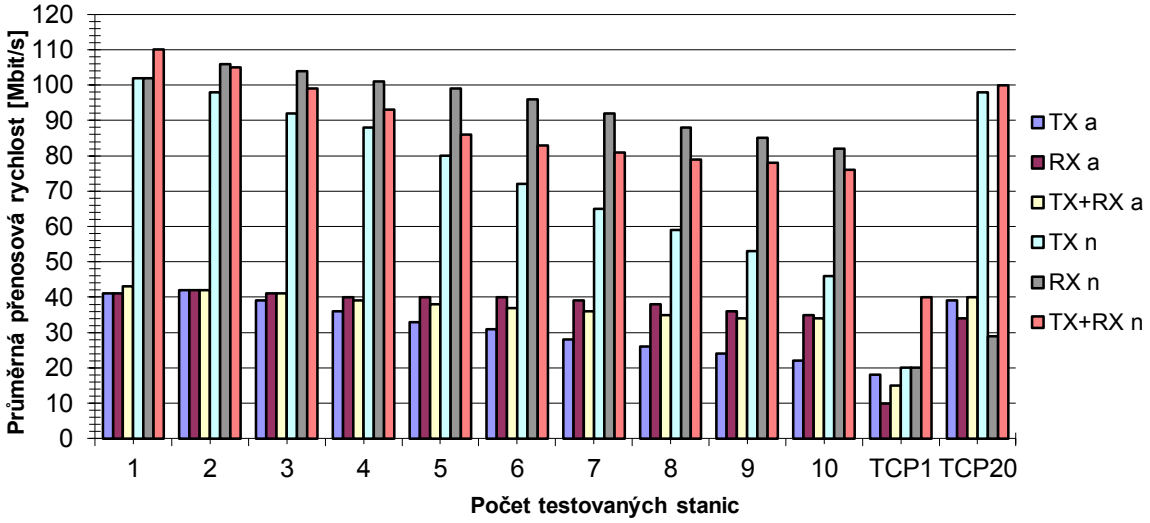
Obrázek 3.15: *Závislost rychlosti na počtu stanic u 802.11a/n Nstreme*



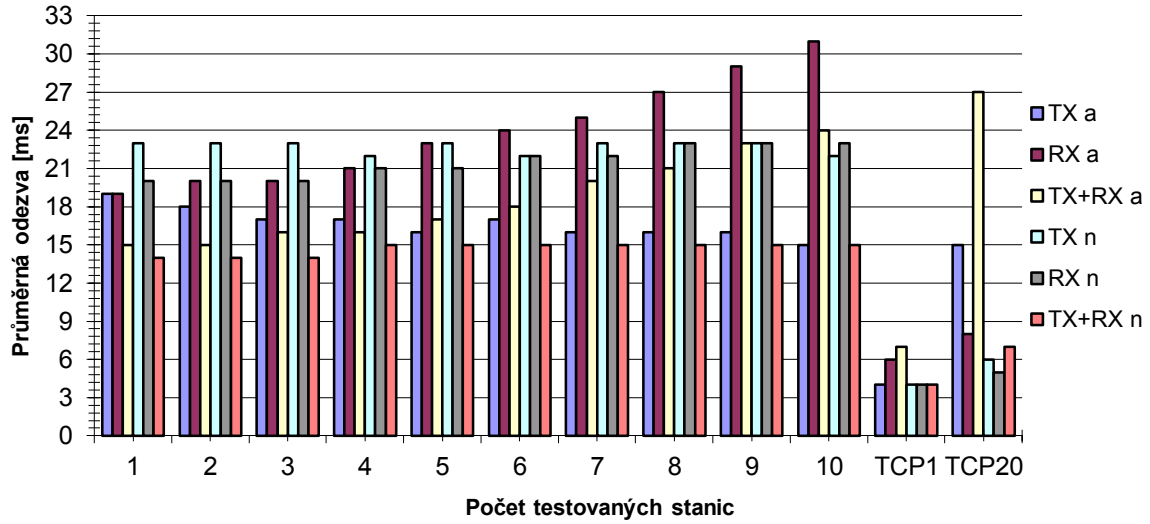
Obrázek 3.16: *Závislost odezvy na počtu stanic u 802.11 a/n Nstreme*

3.6.4 **Srovnání protokolů**

Nasazení protokolů Nstreme a NV2 do sítí 802.11a způsobí cca třetinový nárůst propustnosti. Je to způsobené především zvětšenou velikostí rámců, které mohou mít velikost až 4000. Díky tomu, že není použita klasická přístupová metoda CSMA/CA, nedochází ke snižování rychlosti uploadu při zvyšujícím se počtu komunikujících stanic. Tím se snižuje také odezva, kterou je možné u protokolu NV2 navíc ovlivňovat parametrem TDMA Period Size. U sítí 802.11n byla zvětšena velikost rámce na hodnotu 8192 a zavedeno shlukování paketů, čímž došlo k navýšení propustnosti. Problémy způsobené použitou přístupovou metodou to však, jak je vidět také z testu, neodstranilo.



Obrázek 3.17: *Závislost rychlosti na počtu stanic u 802.11a/n NV2*



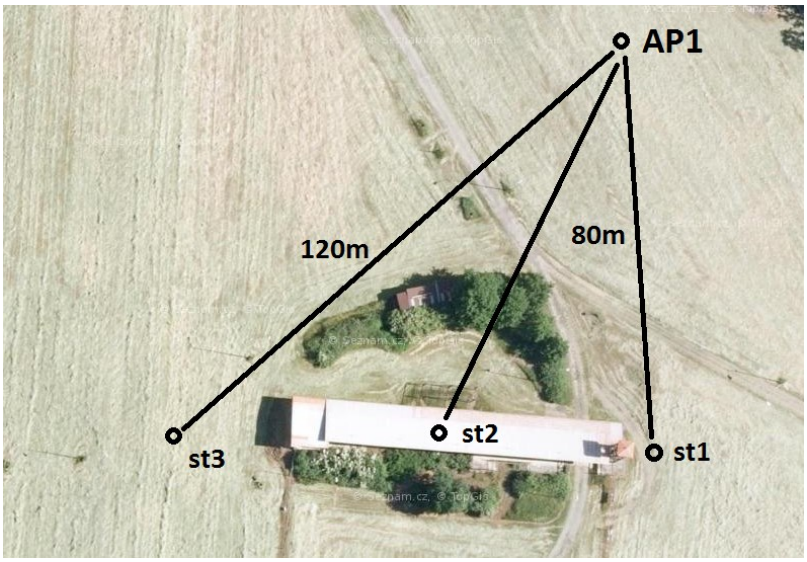
Obrázek 3.18: *Závislost odezvy na počtu stanic u 802.11a/n NV2*

3.7 Skrytý uzel

V předchozím měření bylo otestováno, jak se mění propustnost sítě s počtem komunikujících stanic. Všechny stanice byly umístěny na společném stožáru, takže se navzájem slyšely a nedocházelo tak ke kolizím při potřebě vysílat současně. V praxi však tato situace nastane zřídka. Díky členitému terénu, okolní zeleni a husté zástavbě dochází k tomu, že většina klientských stanic slyší jen přístupový bod. Signál z ostatních stanic vlastní sítě je výrazně potlačen, nebo není přítomný vůbec. Takové umístění stanic je navíc žádoucí, aby se co nejvíc minimalizovalo rušení od cizích sítí. Pokud o sobě stanice neví, dochází ke kolizím ve vysílání, jak již bylo popsáno v teoretické části práce. V tomto měření tedy budu zkoumat, jak si jednotlivé protokoly poradí s tímto problémem.

Topologie sítě byla jiná, než v předchozích dvou měřeních a je zobrazena na obr. 3.19. Testovací síť se skládala z jednoho přístupového bodu osazeného sektorovou anténou s úhlem pokrytí 60° a tří stanic, které jsou umístěny tak, aby se navzájem neslyšely. Všechny stanice měly přímou

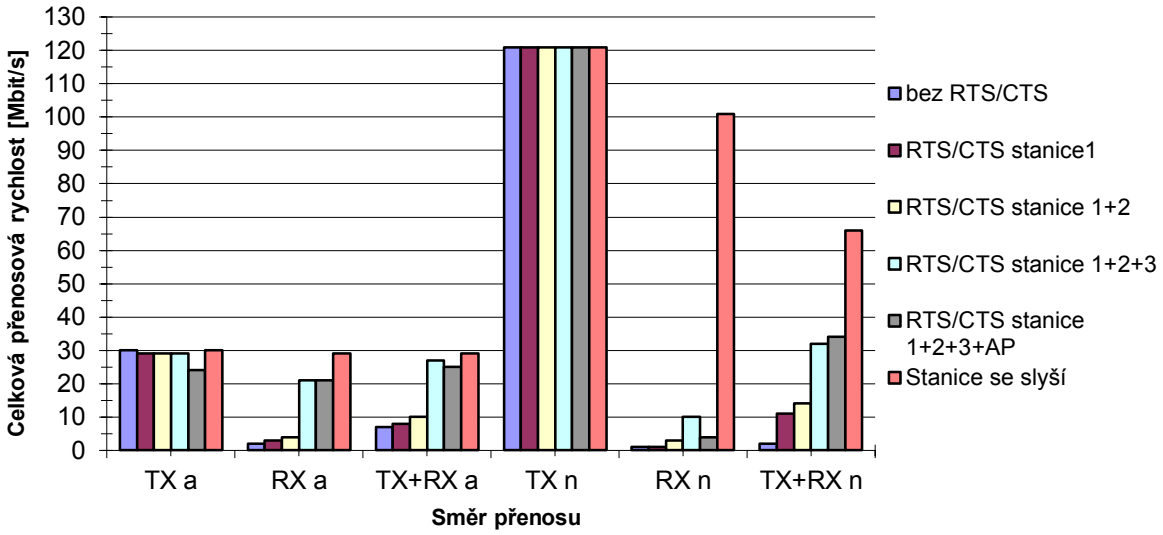
viditelnost na AP. To bylo ověřeno nástrojem Wireless Snooper, který je součástí ROS. Tento nástroj zobrazí AP i stanice v okolí měřeného zařízení, spolu s úrovní signálu. Jelikož se změnilo umístění jednotek, byl u každé znovu proveden spektrální scan okolí, aby se vyloučil vliv cizích sítí. Na testování byly opět použity nástroje Bandwith test a Fping. Před samotným měřením bylo ověřeno, že každá jednotka je schopna dosáhnout maximální rychlosti. Poté byl proveden test pro TX, RX a TX/RX současně s měřením odezvy. Způsob provedení testů byl stejný jako v předchozím měření propustnosti. Měnily se parametry klíčové pro chování jednotlivých protokolů. Pro srovnání se situací, kdy se stanice slyší, byly do grafu vloženy i výsledky předchozího testu propustnosti pro tři stanice.



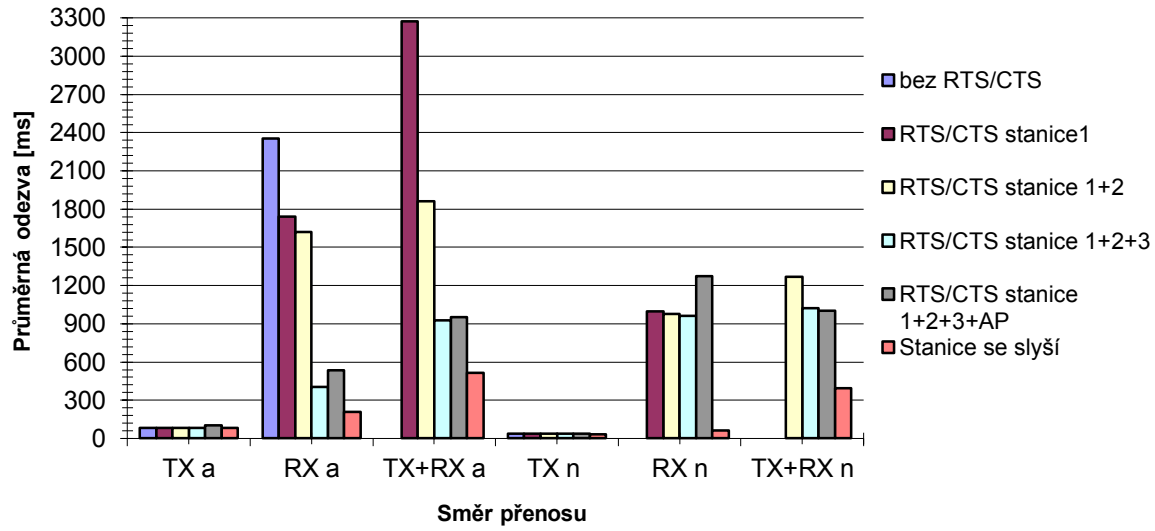
Obrázek 3.19: *Testovací síť při měření se skrytými uzly*

3.7.1 **802.11**

Na obrázcích 3.20 a 3.21 jsou vidět výsledky testů rychlosti a odezvy pro různé nastavení mechanismu RTS/CTS. Princip fungování RTS/CTS a důvody jeho použití byly vysvětleny v kapitole 1.4.2. Nejdříve byla testována síť bez zapnutého mechanismu RTS/CTS, následně byl mechanismus aktivován postupně na všech stanicích a nakonec i na AP. Z grafu je patrné, že u downloadu se rychlost nemění. Jediný případ změny je snížení rychlosti z 30 na 24 Mbit/s při aktivaci RTS/CTS na AP. Je tedy zřejmé, že aktivace tohoto mechanismu na AP nic nepřinese, a naopak je nežádoucí. U přenosu opačným směrem, tedy od stanic směrem k AP, je situace jiná. Mechanismus CSMA/CA nefunguje, protože se stanice navzájem neslyší a dochází ke kolizím. AP není schopno vysílání přijmout, je nutné je opakovat a tím dochází k nárůstu zpoždění a snížení rychlosti. Z grafů je patrné, jak postupná aktivace RTS/CTS na stanicích zlepšuje parametry přenosu. Jediné v praxi použitelné nastavení je aktivace RTS/CTS na všech stanicích v síti, které se navzájem neslyší s ostatními. Aktivace jen u části zařízení způsobuje vysoký packet loss, který není v grafu znázorněn. Podrobnější hodnoty viz Tabulka 1.5: *Výsledky měření skrytého uzlu u 802.11* v příloze. Z grafů je také patrné, že aktivace RTS/CTS u sítí 802.11n přináší minimální zlepšení. Tento problém nebyl podrobněji zkoumán, ale lze se domnívat, že podpora tohoto mechanismu je u produktů od firmy Mikrotik na velmi nízké úrovni.



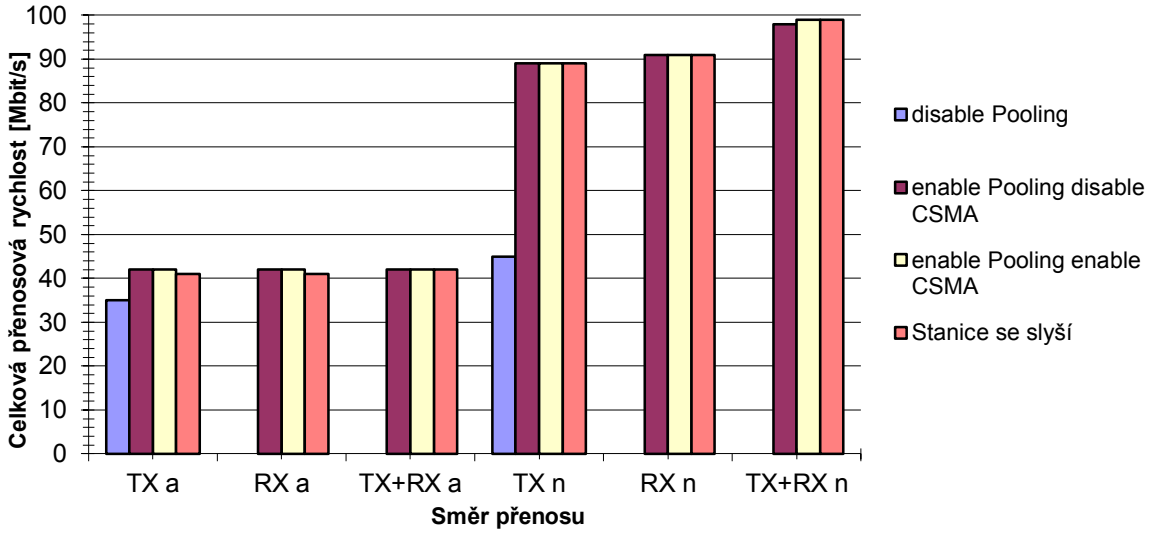
Obrázek 3.20: *Závislost rychlosti na nastavení mechanismu RTS/CTS u 802.11a/n*



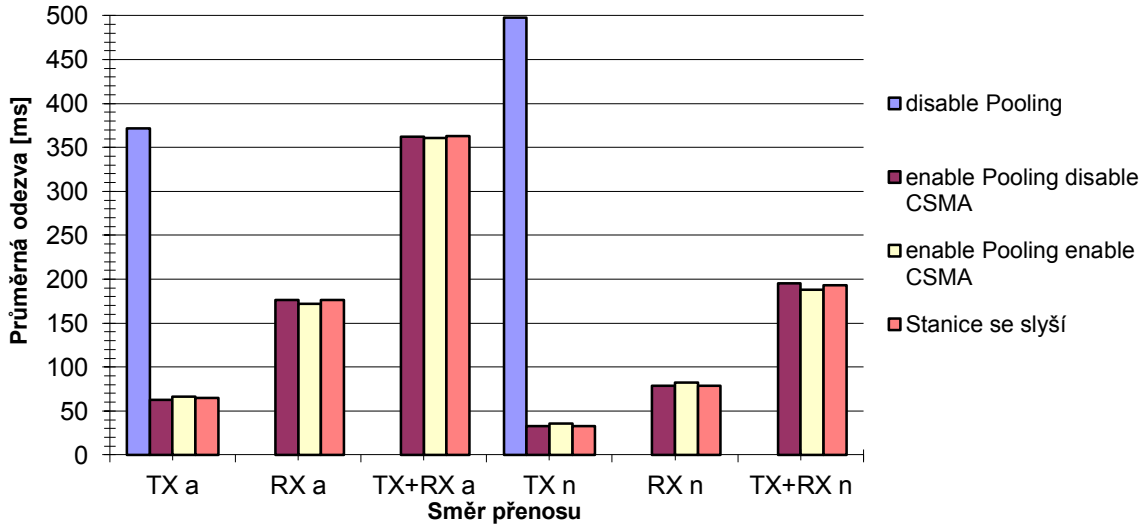
Obrázek 3.21: *Závislost odezvy na nastavení mechanismu RTS/CTS u 802.11a/n*

3.7.2 Nstreme

U sítí s protokolem Nstreme se nepoužívá přístupová metoda CSMA/CA, ale řešení nazývané pooling, kdy AP postupně oslovuje stanice a dává jim prostor k vysílání. Podrobnosti o protokolu naleznete v kapitole 2.3. Díky tomu nedochází u stanic, které se neslyší, ke kolizím. Jak je vidět z grafů na obrázcích 3.22 a 3.23, pokud je pooling zapnutý, rychlost i odezva je stejná jako u stanic, které se slyší. U vypnutého poolingu se spoj při testech RX a TX+RX rozpadal, takže výsledky těchto testů nejsou v grafu zahrnuty. Změna parametru disable CSMA neměla na přenos měřitelný vliv. Tento parametr by měl mírně zvyšovat propustnost v místech bez rušení, protože zbavuje stanici před vysíláním povinnosti poslouchat, zda je médium volné.



Obrázek 3.22: *Vliv skrytých uzlů na rychlost u Nstreme*



Obrázek 3.23: *Vliv skrytých uzlů na odezvu u Nstreme*

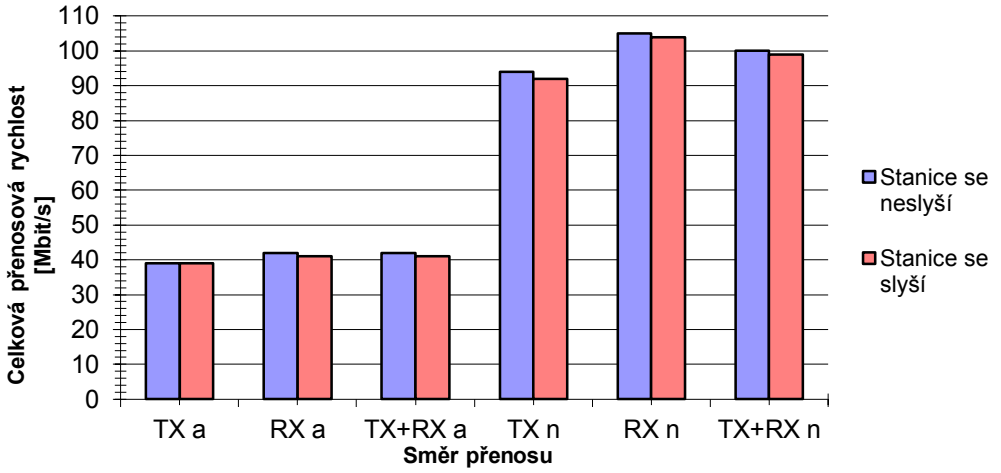
3.7.3 **NV2**

U protokolu NV2 byly testovány jen varianty, kdy se stanice slyší a neslyší. Změna ostatních parametrů nemá na chování sítě v této situaci vliv. Jak je vidět na obrázcích 3.24 a 3.25, u přenosů nedochází k žádným změnám. Provoz je u protokolu NV2, stejně jako u protokolu Nstreme, řízen přístupovým bodem a ke kolizím tudíž taktéž nedochází. Více o protokolu NV2 popsáno v kapitole 2.5.

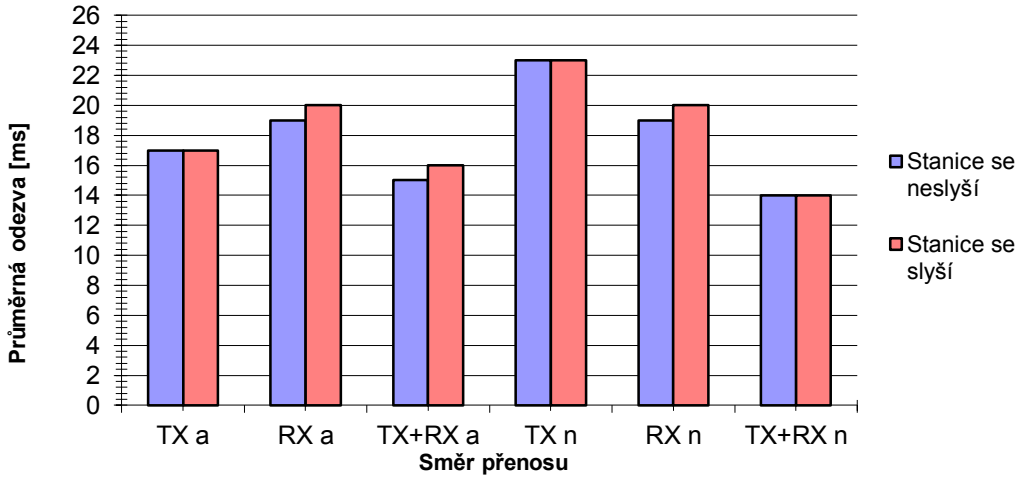
3.7.4 **Srovnání protokolů**

U tohoto testu se ukázala velká výhoda protokolů Nstreme a NV2 při použití u sítí PtMP ve venkovním prostředí. U těchto protokolů je provoz řízen přístupovým bodem a nedochází tak k problému se skrytými uzly. U klasické sítě 802.11 existuje řešení v podobě mechanismu RTS/CTS,

ale jak bylo ukázano na testu, dochází k citelnému zhoršení parametrů přenosu. Navíc u sítí 802.11n je tento mechanismus u ROS v podstatě nefunkční.



Obrázek 3.24: *Vliv skrytých uzlů na rychlost u NV2*



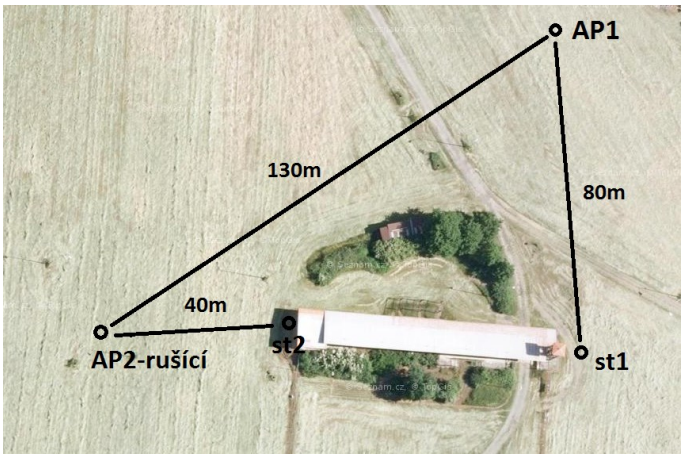
Obrázek 3.25: *Vliv skrytých uzlů na odezvu u NV2*

3.8 Rušení

Po otestování, jak se chová síť v momentě, kde se stanice rádiově neslyší, se práce dále zabývá další situací, ke které v praxi velmi často dochází. Tou je rušení od jiné WiFi sítě. Bude testováno rušení přístupového bodu jiným přístupovým bodem na stejném a sousedním kanále. Protože se přístupové body umísťují na místa s dobrou viditelností do okolí a osazují se anténami s velkým úhlem pokrytí, nastává tato situace poměrně často a nelze ji úplně eliminovat. V tomto měření bude zkoumáno, jak si jednotlivé protokoly s tímto rušením poradí.

Testovací síť se skládala ze dvou AP a dvou klientských stanic (viz obr. 3.26). AP měly vzájemně přímou viditelnost a stanice byly umístěny tak, aby každá slyšela jen vysílání svého AP. To bylo opět ověřeno nástrojem Wireless Snooper. Na rušícím AP byl spuštěn TX Bandwith Test UDP protokolem o rychlosti 40Mbit/s pro normu 802.11n 2x2 MIMO a 10 Mbit/s pro normu 802.11a. Rušené AP přijímalo rušící signál na úrovni -60 dB a ke stanici bylo připojeno s úrovní signálu

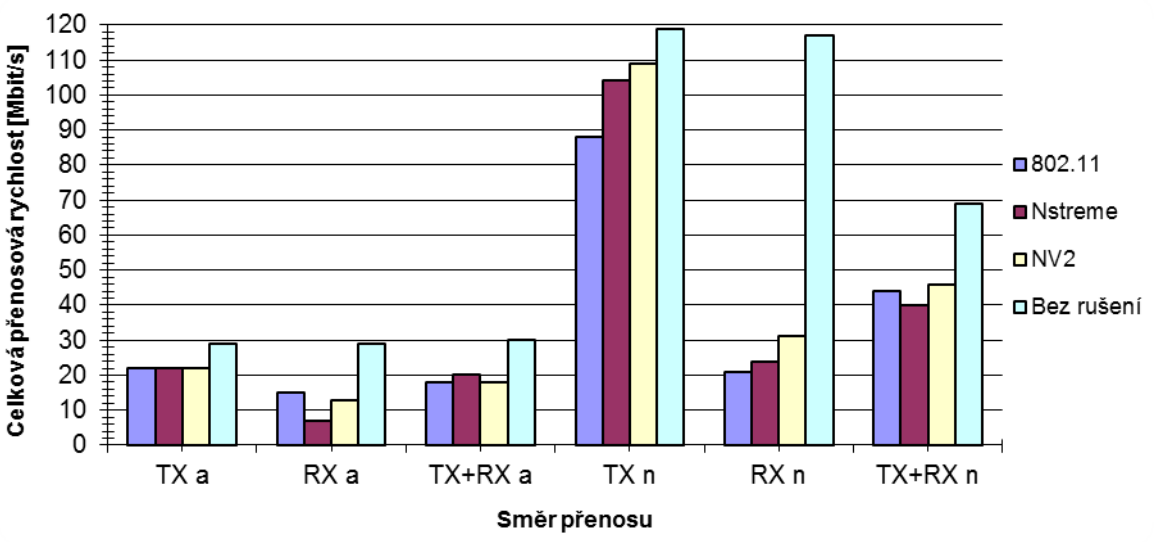
-50/-50 dB. Malý odstup signálů byl zvolen záměrně, aby byl vliv rušení co nejlépe měřitelný. Navíc se v praxi s podobnými případy běžně setkáváme. Byla otestována kombinace všech tří protokolů, jak u rušené, tak i u rušící sítě. Způsob provedení testů a zaznamenané parametry byly opět stejné, jako u předchozího měření. U protokolu NV2 byl navíc proveden test, při kterém se měnila úroveň rušícího signálu, přičemž byl zkoumán vliv této změny na parametry přenosu rušené sítě. Hodnota parametru HW Retries byla zvýšena na 15, aby nedocházelo k tak rychlému přepínaná na nižší rychlosti. Do grafů byly pro porovnání zaneseny i výsledky přenosu nerušené sítě z předchozího měření propustnosti.



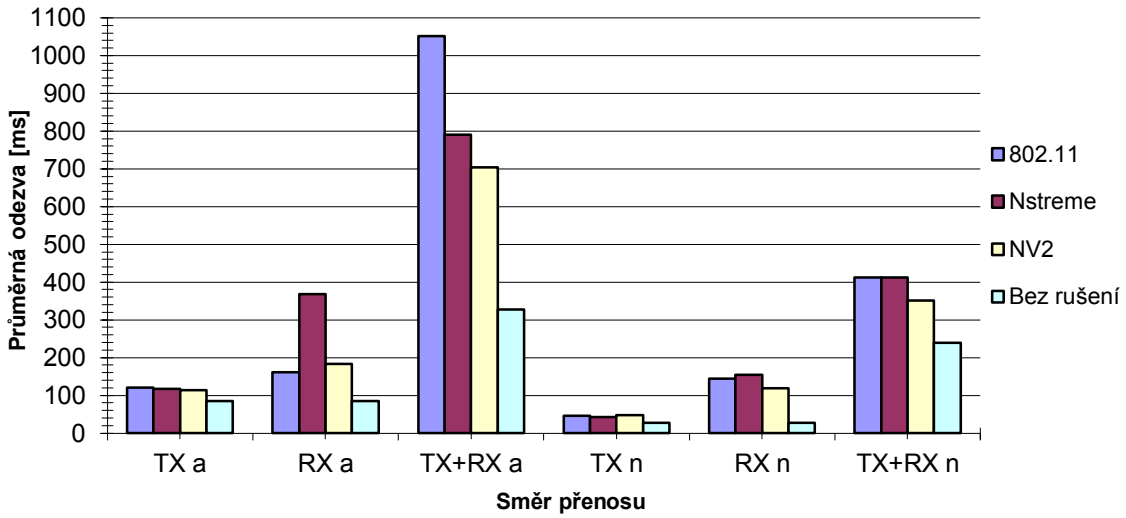
Obrázek 3.26: *Testovací síť při měření se rušení*

3.8.1 **802.11**

Na obr. 3.27 je znázorněno, jak se mění přenosová rychlost u klasické sítě 802.11 při rušení klasickou sítí 802.11 a při rušení sítěmi s nasazeným protokolem Nstreme a NV2. Obr. 3.28 ukazuje vliv rušení na průměrnou odezvu. Jelikož byl rušen přístupový bod, největší změny jsou patrné na uploadu směrem od stanice k AP. Na AP přicházejí nekoordinovaně rámce z rušící sítě i od vlastní stanice a dochází ke kolizím, přenos se musí opakovat a tím se snižuje maximální propustnost a zvyšuje odezva. Nejlépe test dopadl při rušení sítí s protokolem NV2, ale rozdíly nejsou zásadní. U obousměrného přenosu docházelo ke ztrátám paketů, které nejsou z grafu patrné. Podrobnější informace obsahuje Tabulka 1.6: *Výsledky rušení u 802.11*.



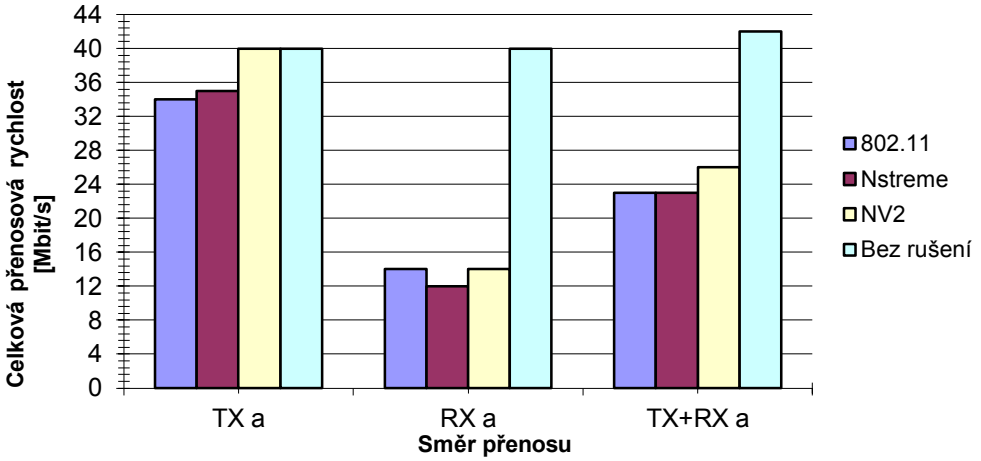
Obrázek 3.27: *Vliv rušení na rychlost u 802.11a/n*



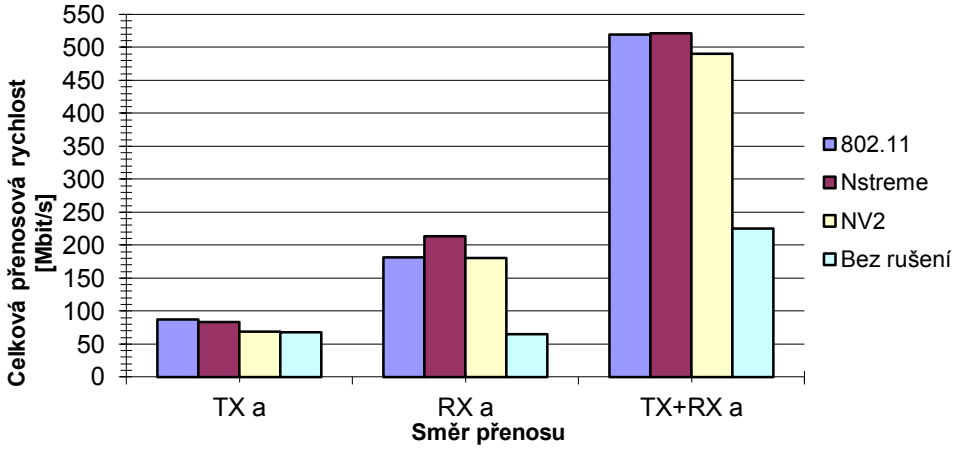
Obrázek 3.28: *Vliv rušení na odezvu u 802.11a/n*

3.8.2 **Nstreme**

U protokolu Nstreme byl proveden test jen pro normu 802.11a, protože práce je zaměřena hlavně na protokol NV2. Jak je vidět na obrázcích 3.29 a 3.30 opět test nejlépe dopadl pro rušení sítí s protokolem NV2, ale rozdíly mezi protokoly jsou ještě menší, než v předchozím případě. Velkou změnou je, že nyní již nedochází ke ztrátám paketů.



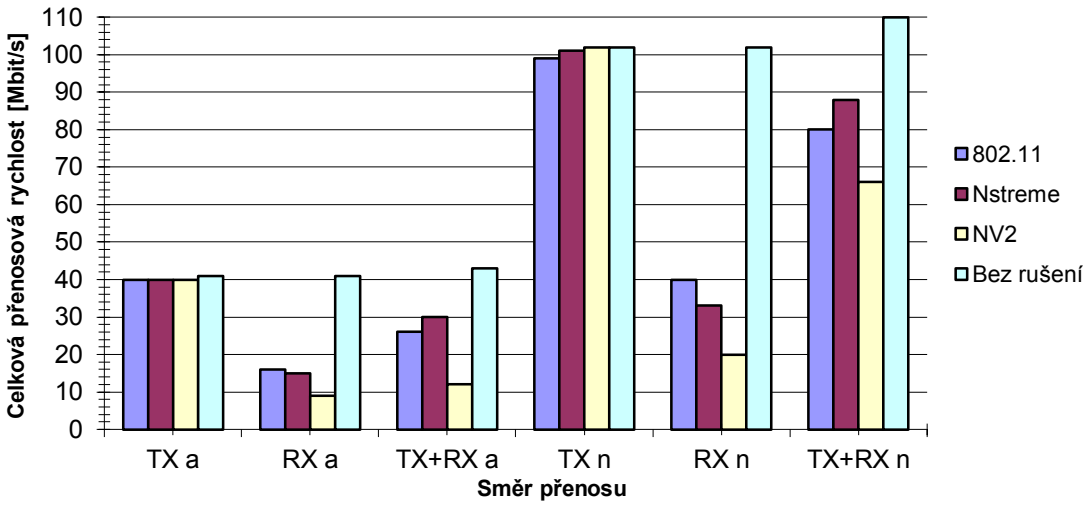
Obrázek 3.29: *Vliv rušení na rychlost u Nstreme*



Obrázek 3.30: *Vliv rušení na odezvu u Nstreme*

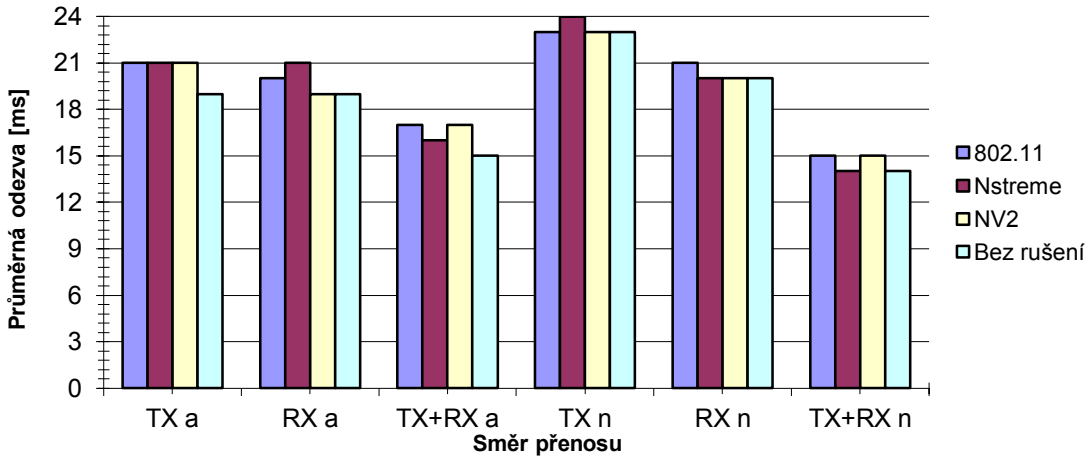
3.8.3 **NV2**

Na obr. 3.31 je znázorněn graf průměrných dosažených rychlostí při rušení sítě s protokolem NV2. Je vidět, že u downloadu nedochází ke změnám v rychlosti. U uploadu je rychlost snížena cca na třetinu maximální propustnosti. Nejvýraznější pokles nastává u rušení sítí s protokolem NV2 u uploadu a v obousměrném přenosu. Z grafu odezvy na obr. 3.32 je patrné, že při rušení dochází k minimální změně odezvy. To je důsledkem vestavěného mechanismu QoS, který v defaultní verzi používá vlastní algoritmus založený na typu a velikosti paketů (viz kapitola 2.5.4.).

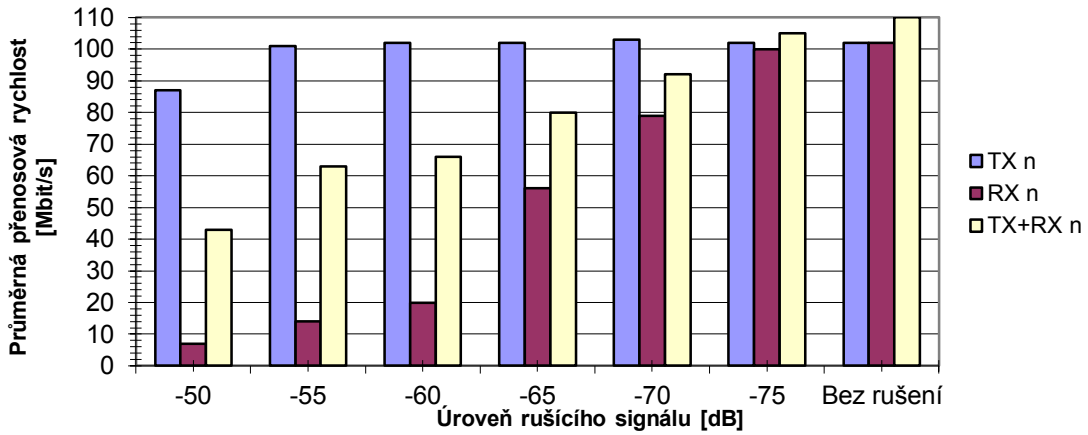


Obrázek 3.31: *Vliv rušení na rychlost u NV2*

Na obr. 3.33 je znázorněna závislost průměrné rychlosti na úrovni rušícího signálu. Na rušící síti byl spuštěn protokol NV2 a prováděna změna výkonu. Pro nastavení nejnižší úrovně signálu bylo nutné provést korekci v nasměrování antény. Z grafu je patrný postupný nárůst rychlosti až do dosažení maximální propustnosti spoje, které nastalo při úrovni -75 dB. To odpovídá odstupu vlastního a rušícího signálu ve výši 25 dB.



Obrázek 3.32: *Vliv rušení na odezvu u NV2*



Obrázek 3.33: *Vliv úrovně rušení na rychlost u NV2*

3.8.4 **Rušení na sousedním kanále**

Mezi provozem na stejném a sousedním kanále je velký rozdíl. Při provozu na stejném kanále se snaží zařízení pásmo sdílet. Do jaké míry se jim to daří, záleží na nastavených parametrech a implementaci softwaru zařízení. To bylo zkoumáno v předchozím měření. Při provozu na sousedním kanále ke sdílení pásma nedochází. Signál pronikající z vedlejšího kanálu má charakter šumu, takže z něj nelze vyčíst žádnou informaci, díky které by mohly zařízení pásmo sdílet. Odolnost vůči rušení ze sousedního kanálu záleží především na HW parametrech vysílací části zařízení. Detailní rozbor problému rušení při použití sousedního kanálu přesahuje rámec této práce. Více informací o této problematice naleznete např. v práci *Adjacent Channel Interference in Dual-radio 802.11a Nodes and Its Impact on Multi-hop Networking* [18], která popisuje problém rušení při použití sousedního kanálu u dvouskokového spoje. V našem měření byla použita stejná síť jako u měření rušení na stejném kanále, pouze došlo k přeladění rušící sítě na vedlejší kanál. Byly změřeny opět všechny protokoly a nebylo zjištěno žádné ovlivnění parametrů přenosu rušící sítí.

3.8.5 **Srovnání protokolů**

Nejlépe si s rušením AP jiným AP poradil protokol NV2. U downloadu nedošlo k žádnému ovlivnění rychlosti, u uploadu byla propustnost snížena na cca třetinu maximální hodnoty. Bylo také ověřeno, že velmi záleží na odstupu signálů vlastní a rušící sítě. To je třeba brát na zřetel a stavět sítě tak, aby i při dodržení zákonných limitů byla dosažena dostatečná výkonová rezerva. Například použitá základní deska v přístupovém bodu umožňuje dle katalogových údajů na webu výrobce komunikaci plnou rychlostí již od úrovně přijímaného signálu -75 dB. V případě rušení signálem o stejné úrovni pak bude daný spoj schopný fungovat jen na desetině původní kapacity. Pokud však budeme počítat s rezervou, a stanice bude připojena s úrovní signálu -55 dB, bude ztráta jen 20 %. Spoj tak bude fungovat i zarušený téměř plnou rychlostí.

Závěr

Cílem této bakalářské práce bylo provést rozbor protokolu NV2, ověřit vhodnost jeho nasazení do venkovních sítí typu PtMP a provést jeho srovnání s klasickými sítěmi 802.11. Pro tento záměr bylo vhodné rozdělit vypracování do dvou částí. V první, teoretické části práce byly popsány principy fungování WiFi sítí standardů 802.11 a/n. Dále byly shrnuty dostupné informace o protokolu NV2 a objasněny principy jeho činnosti. Za účelem lepšího uplatnění výsledků pro praktické využití byl do porovnání a následného testování zahrnut i předchůdce protokolu NV2, Nstreme, protože je pro své solidní funkční vlastnosti dosud hojně využívaný. Následovalo srovnání obou protokolů s klasickou sítí 802.11. Závěr teoretické části byl věnován operačnímu systému RouterOS, jeho instalaci, konfiguraci a typickým způsobům využití, se zaměřením na parametry relevantní pro zkoumané protokoly.

Na základě nově získaných teoretických poznatků byly připraveny testy pro praktickou část práce. Úkolem těchto testů bylo ověření předpokladů definovaných v průběhu teoretické části práce. Pro potřeby testu jsme postavili WiFi síť s dvěma přístupovými body a deseti klientskými stanicemi. Jelikož bylo naším cílem se maximálně přiblížit reálným podmínkám provozu, testování probíhalo ve venkovním prostředí a s jednotkami, které běžně používají ISP ve svých sítích pro připojování koncových klientů. Ze stejného důvodu byl pro testování zvolen nástroj Bandwith Test, integrovaný v jednotkách s RouterOS. Tento nástroj se běžně používá pro rychlé zjištění stavu sítě a na základní analýzu vzniklých problémů. Při testech se měřila přenosová rychlost a dosažené zpoždění. Testovala se maximální dosažitelná propustnost, průběh odezvy a vliv počtu stanic komunikujících současně na jednom AP. Dále bylo testováno, jak si jednotlivé protokoly poradí s rušením a komunikací se skrytými uzly. Tato situace totiž nastává ve větší či menší míře u všech venkovních sítí v podmínkách ČR a přestavuje problém, který má protokol NV2 pomoci účinně řešit.

Hlavním cílem testů tedy bylo prakticky ověřit odpověď na otázku, zda má smysl nasadit do 802.11a/n sítě prototokol NV2. Po vyhodnocení všech testů lze jednoznačně potvrdit, že ano. A to hned z několika následujících důvodů. Z výsledku měření lze vypozorovat, že významnou výhodou protokolu NV2 je používání přístupové metody TDMA. Díky tomu je eliminován problém skrytých uzlů a při komunikaci více stanic nedochází k přílišnému poklesu propustnosti při uploadu. Ve spolupráci s vestavným mechanismem QoS je protokol schopen větší kontroly nad zpožděním. To se projeví především u hodně vytížených linek, jak bylo dokázáno na testu propustnosti. Protokol nabídl i nejlepší odolnost proti rušení, jak jsme si ověřili při simulovaném rušení cizí sítí. U sítí 802.11a je také schopen nabídnout vyšší propustnost díky technikám sdružování rámců a selektivnímu potvrzování rámců, které byly zavedeny u klasické sítě teprve s normou n. Naopak nevýhodou protokolu NV2 je vyšší odezva a její rozptyl u nezatížené sítě. To vyplývá z principu fungování protokolu a není tedy možné zvýšenou odezvu plně eliminovat. Závěrem, po kritickém zhodnocení výsledků testů, lze tedy konstatovat, že zůstat u klasické sítě má smysl v případech, kdy preferujeme nízkou odezvu před propustností. Podmínkou je však provoz v málo zarušeném prostředí s převahou provozu ve směru od AP ke stanicím. V ostatních případech, které jsou z hlediska výskytu mnohem častější, výhody nasazení NV2 do venkovních sítí typu PtMP jasně převládají.

Do budoucna by bylo zajímavé práci rozšířit o detailnější zkoumání zmíněné problematiky rušení a dále se zaměřit na řešení QoS u protokolu NV2.

Použitá literatura

[1] Český telekomunikační úřad. *Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění* [online]. [cit. 2015-11-28]. Dostupné z: http://www.ctu.cz/ctu-online/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni.html

[2] Český telekomunikační úřad. *Všeobecné oprávnění č. VO-R/12/09.2010-12* [online]. Praha, 2010 [cit. 2015-11-28]. Dostupné z: https://www.ctu.cz/cs/download/oop/rok_2010/vo-r_12-09_2010-12.pdf

[3] IEEE Std 802.11a-1999(R2003) *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band* [online]. 1990 [cit. 2015-11-29]. Dostupné z: http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

[4] Agilent Technologies. *An Overview of the Electrical Validation of 10BASE-T, 100BASE-TX, and 1000BASE-T Devices* [online]. 2011 [cit.2015-12-29]. Dostupné z: http://cp.literature.agilent.com/litweb/pdf/5989-7528EN.pdf

[5] ŠIMANDL, Martin. *IEEE 802.11n - Jak na rychlé Wi-Fi doma i venku* [online]. 2010 [cit. 2015-12-18]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/16921-ieee-802-11n-jak-na-rychle-wi-fi-doma-i-venku?start=2

[6] TUREK, Lukáš. *802.11n Cesta za rychlejším Wi-Fi* [online]. 2007 [cit. 2015-12-05]. Dostupné z: http://8an.praha12.net/talks/80211n.pdf

[7] KOVÁŘ, P. a V. NOVOTNÝ. *Time Division Multiple Access* [online]. 2008 [cit. 2015-12-12]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2008100003

[8] SVITÁK, Josef. *Modelování, simulace a analýza propustnosti protokolů rodiny 802.11* [online]. Zlín, 2007 [cit. 2015-12-06]. Dostupné z: http://zamestnanci.fai.utb.cz/dulik/diplomky/2006-2007/svitak2007.pdf

[9] IEEE *802 LOCAL AND METROPOLITAN AREA NETWORK STANDARDS* [online]. 2012 [cit. 2015-12-07]. Dostupné z: http://standards.ieee.org/getieee802/download/802.11-2012.pdf

[10] Wikipedia. *Time Division Multiple Access* [online]. [cit. 2015-12-12]. Dostupné z: https://cs.wikipedia.org/wiki/TDMA

[11] Mikrotik Web. *About us* [online]. [cit. 2015-12-13]. Dostupné z: http://www.mikrotik.com/aboutus

[12] Mikrotik Web. *Netinstall* [online]. [cit. 2015-12-13]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Netinstall

[13] Mikrotik Web. *License* [online]. [cit. 2015-12-13]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:License

[14] Mikrotik Web. *RouterOS features* [online]. [cit. 2015-12-13]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:RouterOS_features

[15] Mikrotik Web. *Wireless Matrix* [online]. [cit. 2015-12-16]. Dostupné z: http://wiki.mikrotik.com/wiki/Wireless_Matrix

[16] Mikrotik Web. *Interface Wireless* [online]. [cit. 2015-12-17]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless

[17] Mikrotik Web. *NV2* [online]. [cit. 2015-12-18]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Nv2#Nv2_vs_Nstreme

[18] Chen-Mou Cheng, Pai-Hsiang Hsiao, H.T. Kung, Dario Vlah. *Adjacent Channel Interference in Dualradio* [online]. Department of Electrical Engineering and Computer Science, Harward University, 2006 [cit. 2016-06-30]. Dostupné z: http://www.eecs.harvard.edu/~htk/publication/2006-globecom-cheng-hsiao-kung-vlah.pdf

Seznam příloh

Příloha A: *Naměřené hodnoty*

Tabulka 1.4: *Výsledky měření propustnosti u 802.11*

Počet stanic	ping					
	TX a	RX a	TX+RX a	TX n	RX n	TX+RX n
1	85	85	327	27	28	240
2	85	142	418	35	42	338
3	85	209	513	34	65	396
4	87	279	616	34	115	533 PL 15%
5	86	354	729	33	143	623 PL 18%
6	86	434	851	35	278	767 PL 19 %
7	87	520	984	35	424	882 PL 21%
8	88	-	-	33	-	-
9	87	-	-	37	-	-
10	87	-	-	36	-	-
TCP1	4	4	8	2	3	4
TCP20	105	90	217	18	10	26

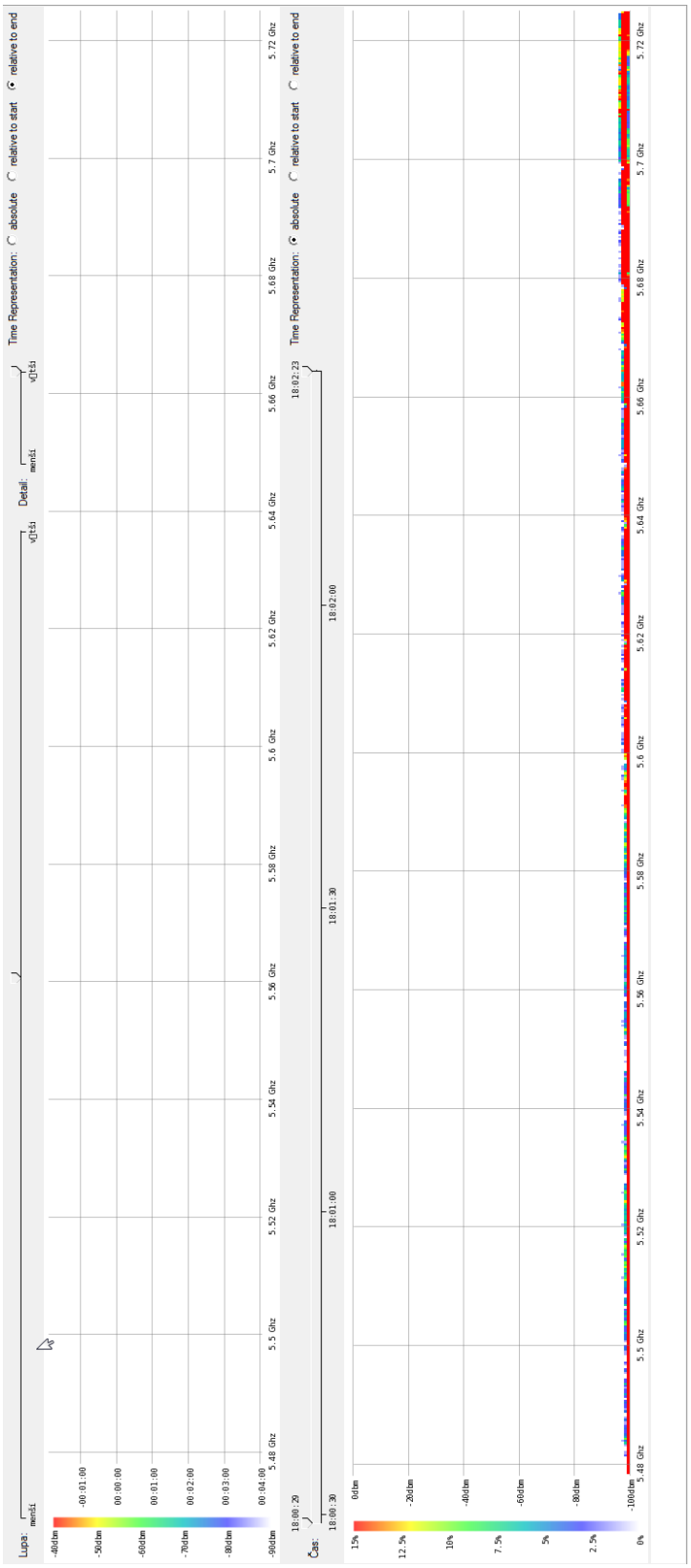
Tabulka 1.5: *Výsledky měření skrytého uzlu u 802.11*

Nastaveni protokolu	ping					
	TX a	RX a	TX+RX a	TX n	RX n	TX+RX n
bez RTS/CTS	85	2354 PL92%	PL 100%	39	PL 100%	PL 100%
RTS/CTS client1	85	1740 PL 84%	3276 PL 94%	38	998 PL 81%	PL 100%
RTS/CTS client1+2	85	1620 PL 58 %	1862 PL79%	37	979 PL 59 %	1268 PL 82%
RTS/CTS client1+2+3	85	407	926	40	961 PL 55%	1025 PL 86%
RTS/CTS client1+2+3+AP	103	533	954	39	1274 PL 66%	1001 PL 82%

Tabulka 1.6: *Výsledky rušení u 802.11*

Rušící síť	ping					
	TX a	RX a	TX+RX a	TX n	RX n	TX+RX n
802.11	120	162	1052 PL40%	46	145	413 PL10%
Nstreme	117	368	790 PL18%	42	155	412 PL16%
NV2	113	183	704 PL 8%	47	118	352 PL6%

Příloha B: *Spektrální scan*



Obrázek 3.34: *Spektrální scan okolí AP*