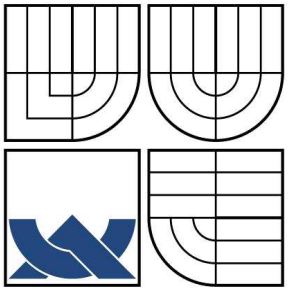
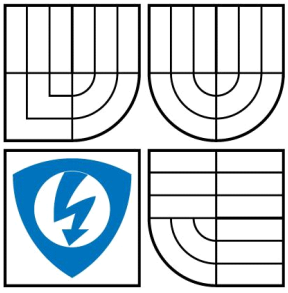


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

# STANDARDY 802.11N A 802.11E V BEZDRÁTOVÝCH SÍTÍCH

802.11N AND 802.11E STANDARDS FOR WIRELESS NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — ONDŘEJ NOVÁK
AUTHOR

VEDOUCÍ PRÁCE — Ing. LUKÁŠ RŮČKA
SUPERVISOR

BRNO 2009

**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky a komunikačních technologií**

**Ústav telekomunikací**

# Bakalářská práce

bakalářský studijní obor
**Teleinformatika**

| | | | |
|---|---|---|---|
| ***Student:*** | Ondřej Novák | ***ID:*** | 70348 |
| ***Ročník:*** | 3 | ***Akademický rok:*** | 2008/2009 |

**NÁZEV TÉMATU:**

## Standardy 802.11n a 802.11e v bezdrátových sítích

**POKYNY PRO VYPRACOVÁNÍ:**

Prostudujte standardy bezdrátových sítí 802.11. Zaměřte se především na standardy 802.11n a 802.11e. U standardu 802.11e se zaměřte na rozšíření Wi-Fi Multimedia. Proveďte praktické testy na zařízení D-Link DIR-655 podporující technologie 802.11n a Wi-Fi Multimedia. Navrhněte vhodnou metodiku měření, pomocí které otestujte výkonnostní možnosti zařízení. Testy proveďte v módu pouze s použití standardu 802.11n a dále pak ve smíšeném módu s použití standardů 802.11g/n. Dále pak navrhněte vhodnou metodiku měření, pomocí které otestujte dopad technologie Wi-Fi Multimedia na datové přenosy, které jsou citlivé na kvalitu služby.

**DOPORUČENÁ LITERATURA:**

[1] GAST, Matthew. 802.11 Wireless Networks: The Definitive Guide. 2nd ed. O'Reilly Media, Inc., 2005. 688 s. ISBN 0-596-10052-3.

[2] GANZ, Aura; GANZ, Zvi; WONGTHAVARAWAT, Kitti; Multimedia Wireless Networks: Technologies, Standards and QoS. Prentice Hall PTR, 2003. 352 s. ISBN 0-13-046099-0.

| | | | |
|---|---|---|---|
| ***Termín zadání:*** | 9.2.2009 | ***Termín odevzdání:*** | 2.6.2009 |

***Vedoucí práce:*** Ing. Lukáš Růčka

**prof. Ing. Kamil Vrba, CSc.**
*Předseda oborové rady*

# ABSTRAKT

Tato bakalářská práce je zaměřena na problematiku standardů bezdrátových sítí. Teoreticky popisuje nejznámější standardy skupiny standardů IEEE 802.11, jejich funkce a chování. Dále práce podrobněji rozebírá nový standard 802.11n a specifikaci standardu 802.11e, WMM. Práce obsahuje zprávu o praktických testech standardů 802.11n a WMM, které slouží pro objektivní posouzení schopností těchto standardů.



**Klíčová slova:** Wi-FI, AP, 802.11n, 802.11e, WMM, QoS



# ABSTRACT

This bachelor thesis is focused on broad issue of wireless network standards. It theoretically describes the most famous standards of IEEE 802.11 group, functions and behavior. It also closely analyzes the new standard 802.11n and the specification of 802.11e, WMM. The paper includes a report of practical tests of standards 802.11n and WMM, which serves for an objective appreciation of capabilities of these norms.



**Keywords:** Wi-FI, AP, 802.11n, 802.11e, WMM, QoS

# PROHLÁŠENÍ

Prohlašuji, že svojí bakalářskou práci na téma Standardy 802.11n a 802.11e v bezdrátových sítích, jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne …… ……

Podpis autora

# PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce Ing. Lukáši Růčkovi, za pomoc a rady při zpracování této bakalářské práce.


V Brně dne ……  podpis autora……

## SEZNAM ZKRATEK:

| | |
|---|---|
| AC | (Access Categories) |
| ADSL | (Asymmetric Digital Subscriber Line) |
| AIFS | (Arbitration Inter- Frame Space) |
| AP | (Access Point) |
| BSA | (Basic Service Area) |
| BSS | (Basic Service Set) |
| BSSID | (Basic Service Set Identifier) |
| CAP | (Controlled Access Periods) |
| CCK | (Complementary Code Keying) |
| CDMA | (Code Division Multiple Access) |
| CFB | (Contention Free Bursting) |
| CFP | (Contention-Free Period) |
| CP | (Contention Period) |
| CRC | (Cyclic Redundancy Code) |
| CS | (Carrier Sense) |
| CSMA/CA | (Carrier Sense Multiple Access / Collision Avoidance) |
| CSMA/CD | (Collision Detection) |
| CTS | (Clear To Send) |
| CW | (Contention Window) |
| DCF | (Distributed Coordination Function) |
| DHCP | (Dynamic Host Configuration Protocol) |
| DIFS | (Distributed Inter Frame Space) |
| DoS | (Denial Of Service) |
| DSSS | (Direct Sequence Spread Spectrum) |
| DVB-T | (Digital Video Broadcasting – Terrestrial) |
| EDCA | (Enhanced Distribution Coordinate Access) |
| EDCAF | (Enhanced Distributed Channel Access Function) |
| ESA | (Extended service area) |
| ESS | (Extended Service Set) |
| ESSID | (Extend Service Set Identification) |
| FCS | (Frame Check Sequence) |
| FFH | (Fast Hopping ) |
| FHSS | (Frequency Hopping Spread Spectrum) |
| GSM | (Groupe Spécial Mobile) |
| HC | (Hybrid Controller) |
| HCCA | (HCF Controlled Channel Access) |
| HCF | (Hybrid Coordination Function) |
| ICV | (Control Check Value) |
| IEEE | (Institute of Electrical and Electronics Engineers) |
| KSA | (Key Sheduling Algorithm) |
| MIMO | (Multiple input-Multiple output) |
| MPDU | (Mac Protocol Data Units Aggregation) |
| MSDU | (Mac Service Data Units Aggregation) |
| NAT | (Network Address Translation) |
| NAV | (Network Allocation Vector) |
| OFDM | (Orthogonal Frequency Division Multiplex) |
| p2p | (peer-to-peer) |
| PCF | (Point Coordination Function) |

| | |
|---|---|
| PDA | (Personal Digital Assistant) |
| PSK | (Phase-Shift Keying) |
| QAM | (Quadrature Amplitude Modulation) |
| QAP | (QoS Access Point) |
| QoS | (Quality of Service) |
| QPSK | (Quadrature Phase-Shit Keying) |
| QSTA | (QoS Station) |
| RIFS | (Reduced inter-frame space) |
| RSI | (Required Service Interval) |
| RTS | (Request To Send) |
| SFH | (Slow Hopping) |
| SISO | (Single input – Single output) |
| SNR | (Signal to noise ratio) |
| SS | (Spread Spectrum) |
| SSID | (Service Set Identifier) |
| TGn Sync | (Task Group N) |
| TID | (Traffic Identifier) |
| TS | (traffic Streams) |
| TSPEC | (Traffic Specification) |
| TXOP | (Transmission Opportunity) |
| VoIP | (Voice over Internet Protocol) |
| WEP | (Wired Equivalent Privacy) |
| WISH | (Wireless Inteligent Stream Handling) |
| WISP | (Wireless internet service provider) |
| WM | (Wireless Medium) |
| WPA | (Wi-Fi Protected Access) |
| WWiSE | (World Wide Spectrum Efficiency) |

**OBSAH**:

## SEZNAM OBRÁZKŮ:

# 1 ÚVOD

Tato semestrální práce se snaží přiblížit problematiku standardů bezdrátových sítí Wi-Fi. Popisuje principy standardů 802.11b/g, 802.11a, 802.11n a 802.11e, jejich fungovaní a technologie používané k jejich aplikování do dnešního světa bezdrátových komunikací.

První část pojednává o základních prvcích bezdrátové sítě, jejich vlastnostech a funkcích. V podkapitole jsou popsány metody přenosu signálu a mechanismy přístupu k médiu standardů 802.11. Zahrnuta je i kapitola zabývající se zabezpečením.

Druhá část se soustředí na problematiku standardu 802.11n. Úvodem je uveden krátký popis příčin a historie vzniku. V práci je také popsáno porovnání se staršími standardy rodiny standardů 802.11. První podkapitola prezentuje novou technologie vysílání MIMO a funkce této technologie. Kapitoly Fyzická vrstva a vrstva MAC popisují vylepšení technik šíření signálu a nové metody přístupu k médiu. Poslední kapitola druhé části specifikuje metody zpětné kompatibility standardu 802.11n .

Poslední část teoretického rozboru je zaměřena na standard 802.11e a jeho mnohá vylepšení v problematice správy kvality služeb. Struktura této části je orientována podobně jako u druhé části. V kapitolách jsou popsány základní změny a vylepšení. Detailněji je zpracována problematika nové metody přístupu k médiu EDCA.

Podkapitola sekce týkající se standardu 802.11e popisuje vznik a vztah standardu s WMM, certifikaci a metody používané k zajištění optimální kvality poskytovaných služeb.

Druhá polovina bakalářské práce rozebírá praktické testy se standardy 802.11n a WMM. Jsou uvedeny výsledky několika testů, jejichž cílem je přiblížit čtenářovi vlastnosti těchto standardů v praxi. Testy standardu 802.11n popisují dopad technik definovaných tímto standardem na propustnost dat, velikost odezvy a sílu signálu. Testy tohoto standardu jsou rozděleny do několika fází pro ověření vlastností jak samotného standardu, tak zpětné kompatibility se starším standardem 802.11g. Praktické testy normy 802.11e se snaží ozřejmit dopad specifikace standardu 802.11e-WMM na propustnost dat a výslednou kvalitu testované služby.

Práce předpokládá čtenářovo základní vědomosti v oboru bezdrátových a metalických sítí.

# 2 ÚVOD DO BEZDRÁTOVÝCH SÍTÍ

V současné době se technologie rozvíjí tak, že je téměř až nemožné tento rozvoj z hlediska běžného uživatele sledovat. Technologie se rozvíjí ve všech směrech. Velký důraz je při vývoji nových metod kladen speciálně na výpočetní techniku. Je to dáno neustále se zvyšujícími nároky na spolehlivost a flexibilnost dnešního digitálního světa. Lidé se s každou nově příchozí technologií snaží své životní podmínky zlepšit a zpohodlnit. Důležitou roli hraje při neustálém rozvoji obchodu mobilita. Když vyslovíme tento pojem, většina z nás si pod ním představí Internet mobilní telefon, notebook, PDA (*Personal Digital Assistent*) či podobná zařízení. K tomu aby lidé tyto vymoženosti mohli používat, je nezbytné využívat přitom počítačové sítě. Ať chceme nebo ne, prakticky veškerá naše činnost v reálném světě má svůj obraz i ve světě počítačů. A to ve formě jedniček a nul. Například když chcete v bankomatu vybrat hotovost, terminál od chvíle vložení karty uvědomí Vaši banku a informuje ji o vašem výběru, ať jste právě třeba na druhém konci světa. Všechny tyto možnost využívají komunikace mezi jednotlivými body. S nárůstem nároků na takovouto mobilitu došlo ke vzniku nových, bezdrátových technologií. Ať už vezmeme v potaz GSM (*Groupe Spécial Mobile*), CDMA (*Code Division Multiple Access*), Bluetooth, Wi-Fi či jednoduchý IR přenos, všechny tyto technologie vznikly v důsledku potřeby nezávislosti na metalických vedeních. Kromě světově nejrozšířenější technologie GSM, vysoké uplatnění ve světě získává technologie Wi-Fi. Termín Wi-Fi je akronym, který vznikl zkrácením spojení "Wireless Fidelity" (česky bezdrátová věrnost). Tato technologie nachází největší využití v oblasti bezdrátových počítačových sítí a existuje v několika verzích. Každá verze je definována normou, která je pak označena příslušným písmenem abecedy. Nejznámější jsou dnes standardy 802.11a, 802.11b a 802.11g. Každá norma se vyznačuje svými charakteristickými vlastnostmi, je to například frekvence, přenosová rychlost, modulace nebo šířka pásma. Jednotlivé normy se však liší i v mnoha jiných vlastnostech a mnoha případech se stávají tyto technologie, kvůli vlivům prostředí, velmi nestabilní a nespolehlivé. To může být způsobeno například vlivy rušení, nepřímou viditelností nebo počasím. Aby se těmto negativním vlivům dalo oponovat, byly vyvinuty technologie, které svými vlastnostmi bezdrátovou síť zpevňují, vylepšují a zabezpečují. Jsou to zejména standardy 802.11n a 802.11e. Standard 802.11n disponuje velikou propustností, malými náklady na režii a velikou spolehlivostí. Standard 802.11e zase pro bezdrátovou síť přináší několikerá zásadní vylepšení v oblasti podpory služeb a prioritizace síťových požadavků. Oba standardy byly vyvinuty za účelem inovace a zvýšení stupně mobility a v současné době jsou jejich metody běžně aplikovány do bezdrátových aktivních prvků.

## 2.1 Architektura

Nedílnou součástí každé bezdrátové sítě jsou prvky, pomocí kterých koncový uživatel bezdrátovou sít může nejen využívat, ale i ovládat. Těmi základními pojmy jsou bezdrátové médium a distribuční systém. Z hlediska koncových zařízení jsou to přístupový bod AP (*Access Point*) a klientská stanice (*client station*). V následujících kapitolách je popsána jejich funkce a možnosti využití.

### 2.1.1 Přístupový bod

Centrem bezdrátové sítě je přístupový bod AP, který plní funkci bezdrátového přepínače. Je nejdůležitějším prvkem v bezdrátové síti a vykonává mnoho důležitých operací,

především plní funkci bezdrátového média WM (*Wireless Medium*). Tím jsou v tomto případě rádiové vlny ve vzduchu. Bezdrátové klientské stanice spolu nikdy nekomunikují přímo, ale prostřednictvím AP (s výjimkou ad hoc sítí). Jelikož se jedná o bezdrátový přenos, je třeba definovat oblast pokrytí, kde se klient musí vyskytovat, aby mohl s AP komunikovat.

Hlavní funkce AP je pokrytí základní oblasti služeb BSA (*Basic Service Area*), které říkáme buňka. Určité uskupení klientských stanic a přístupového bodu v jedné buňce vytváří základní soubor služeb BSS (*Basic Service Set*). Určitý počet buněk potom vytváří síť, tak aby se dosáhlo pokrytí požadované oblasti. Buňky jsou prostřednictvím distribučního systému propojeny, vytváří spolu rozšířenou oblast služeb ESA (*Extended service area*), a zároveň rozšířený soubor služeb ESS (*Extened Service Set*). Při budování infrastruktury bezdrátové sítě je časté, že se buňky překrývají. Klientské stanici je potom umožněn volný přechod mezi buňkami. V reálném případě se v jedné oblasti může vyskytovat více bezdrátových sítí na sobě nezávislých. Proto je třeba, aby každý klient obsahoval informace o své síti.

Jako hlavní prvek, AP umí operovat v několika módech, jsou to most, směrovač, opakovač a mód bezdrátového poskytování internetu. [4]

#### 2.1.1.1 Operační módy přístupového bodu

MOST (*BRIDGE*)

U tohoto operačního módu AP funguje jako most propojující dvě části lokální sítě. Na obou přístupových bodech se obě rozhraní, bezdrátové a metalické, sloučí a vystupují pod jednou adresou IP a maskou podsítě. Síť funguje stejně, jako kdyby místo obou AP existovalo mezi oběma segmenty metalické propojení.

SMĚROVAČ (*ROUTER*)

Tento mód je základním módem přístupového bodu. Používá se k připojení bezdrátových klientů ke stávající metalické síti. V případě použití více přístupových bodů, budou připojení klienti navzájem komunikovat skrz metalickou síť.

OPAKOVAČ (*REAPEATER*)

Tato možnost představuje pro spolehlivý bezdrátový přenos určité nevýhody. Přístupové body musí v tomto režimu navzájem komunikovat, a to znamená, že minimální pokrytí oblastí kolem bodů je 50%, což znamená pokles pokryté plochy. Velkou nevýhodou je také fakt, že komunikace vzdálených klientů a metalické sítě způsobuje značný pokles propustnosti bezdrátové sítě.

WISP (*Wireless Internet Service Provider*)

Tato funkce se využívá v případě, kdy například poskytovatel internetu bezdrátovému koncovému uživateli dovolí použít pouze jedno zařízení, tedy jednu IP adresu. V situaci, kdy je potřeba zapojit více zařízení (více PC), je nutné zapojit směrovač, který by zprostředkovával překládání adres NAT. Vytvoří se dynamické IP adresy pro vnitřní síť, ve které si koncový uživatel může připojit větší množství počítačů. Směrovač je navíc v takovéto situaci schopen i předávat porty tzv. port-forwarding.

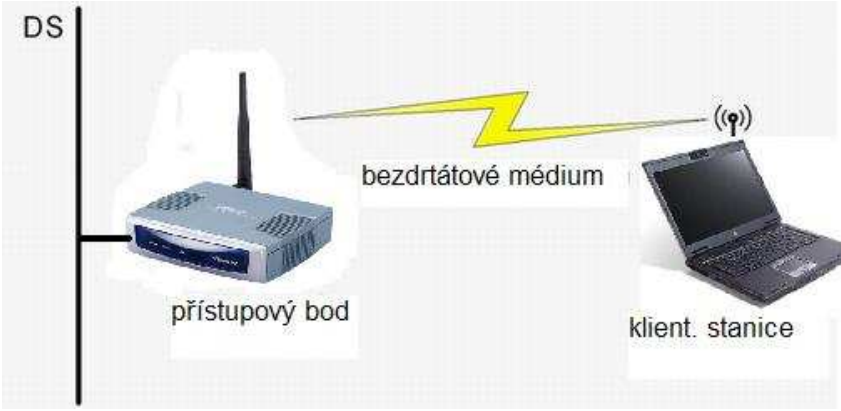
### 2.1.2 Distribuční systém

Pod pojmem distribuční systém si představíme logickou komponentu standardu 802.11, která je používána k přesměrování toku dat na stanici dle její aktuální polohy

v případě, kdy se stanice pohybuje mezi jednotlivými přístupovými body a tyto body musejí navzájem komunikovat. [4]

### 2.1.3 Klientská stanice

Klientskou stanicí rozumíme jakékoliv zařízené schopné pracovat v módu Client. Pci, PCMCIA, Cardbus, USB karty, dále Notebooky, PDA, MDA a jiné. Klientské stanice pracují v síti o topologii ad-hoc nebo infrastructure. Svými vlastnostmi musí být schopny komunikovat dle standardů 802.11x.



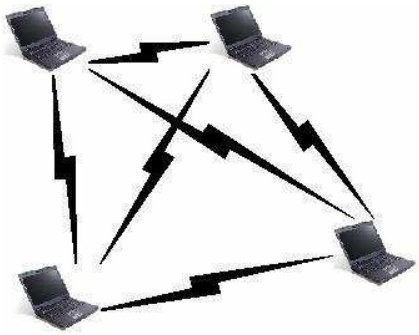

*Obrázek 1: funkce jednotlivých prvků v síti*

## 2.2 Základní typy bezdrátových sítí

### 2.2.1 Ad hoc – IBSS (Independent basic service set)

Tento typ bezdrátové sítě spočívá v propojení klientů p2p (*peer-to-peer*). To znamená, že jsou si všechny klientské stanice rovny. Ke vzájemné komunikaci není třeba AP, stanice komunikují přímo. Z toho však vyplývá, že všechny stanice musí být v dosahu signálu.
Roli hlavního počítače hraje první spuštěný klient, který vytvoří imaginární přístupový bod a má tudíž na starosti komunikaci ostatních klientů. Ostatní stanice sice komunikují navzájem bez hlavního klienta, ovšem v případě jeho odstavení či vypnutí, se síť rozpadne a role imaginárního přístupového bodu se ujímá další stanice.

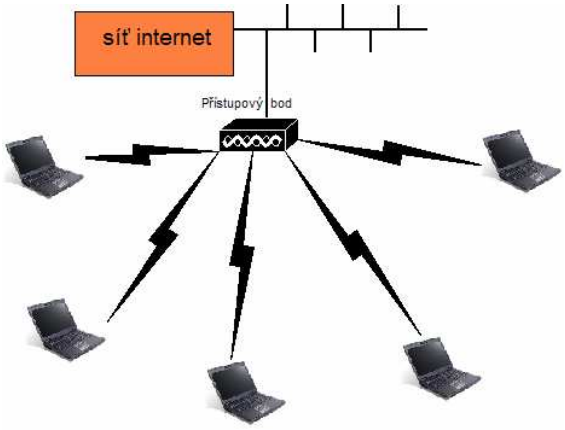
Tento způsob propojení se využívá jen zřídka, avšak výhodou této sítě je rychlé a jednoduché sestavení. Využití nalezne například při náhlé potřebě přenosu dat mezi notebooky na konferencích. Nevýhodou je maximální přenosová rychlost 11Mb/s. [4] [5]



*Obrázek 2: Zapojení prvků v síti typu ad hoc*

### 2.2.2 Infrastrukturní typ – BSS (Basic Service Set)

Tento typ sítě je základním nejrozšířenějším typem. Základním prvkem infrastrukturní sítě je přístupový bod AP, kterým probíhá veškerá komunikace. Je připojen do metalické sítě a v nejjednodušším možném případě slouží jako most mezi bezdrátovými klienty a metalickým vedením. V jiných případech může fungovat jako směrovač, zprostředkovávat překládání adres NAT (*Network Adress Translation*), DHCP server (*Dynamic Host Configuration Protocol*), kvalitu služeb QoS (*Quality of service*), provádět omezování rychlosti tzv. shaping. atd. U menších sítí se většinou využívá více funkcí a naopak u rozlehlých sítí plní tyto funkce servery. Proto se další funkce u AP nepoužívají. [4] [5]




*Obrázek 3: Zapojení prvků v infrastrukturní síti*

## 2.3 Identifikátory bezdrátové sítě

### 2.3.1 Identifikátor SSID (Service Set Identifier)

SSID rozumíme identifikátor bezdrátové sítě implicitně vysílaný v intervalech po přibližně 100ms v synchronizačním rámci (beacon) přístupovým bodem. Slouží uživateli k vyhledání a připojení k síti. Takto poslouží uživateli s povolením, avšak do sítě může proniknout i potenciální hacker. SSID je parametr složený z maximálně 32 znaků řetězce ASCII a můžeme si jej představit jako spojovací článek jednotlivých zařízení v bezdrátové síti. Všechna zařízení v síti, která spolu komunikují, si ve svých informacích tento klíč musejí předávat. V případě, že se SSID klientského zařízení od SSID přístupového bodu liší, klient

nedostane povolení k připojení do sítě. Nastavení odlišného parametru SSID na zařízeních, popřípadě přidělením různých kanálů zařízením, můžeme spolehlivě zprovoznit několik sítí v jednom místě nezávisle na sobě.
Existují dva základní typy toho identifikátoru. Pro ad-hoc a infrastrukturní síť. [4] [5]

### 2.3.2 Identifikátor ESSID (Extend Service Set Identifier)

Kromě SSID se v bezdrátové síti vyskytuje i pojem ESSID (*Extend Service Set Identification*). ESSID je metoda, která řídí vstup klientských zařízení do bezdrátové sítě. Slouží k analýze sítě v místě přístupového bodu. Tato informace není vysílána. To znamená, že pouze stanice, které tento identifikátor znají, jsou oprávněny ke vstupu do sítě.

### 2.3.3 Identifikátor BSSID (Basic Service Set Identifier)

Tento identifikátor charakterizuje bezdrátové zařízení (*wireless interface*) přístupového bodu pracující v módu infrastrukturního typu síťě BSS (*Basic Service Set*). Jedná se MAC adresu tohoto zařízení, generovanou ze 46 bitového náhodného čísla. Informace o hodnotě BSSID je vysílána jedině při průběhu vyhledávání sítí aktivním skenováním (*probe request*).

## 2.4 Fyzická vrstva

### 2.4.1 Datové přenosy

V bezdrátových sítích se informace přenášejí rádiovými přenosy. Ty mohou být s úzkou šířkou frekvenčního pásma nebo s velkou šířkou frekvenčního pásma. Důležitým faktorem u rádiového přenosu je také použitý kmitočet. Většího dosahu a lepšího průchodu překážkami se dosahuje na nižších frekvencích, a naopak vyšší frekvence jsou vhodnější pro větší přenosové rychlosti.

U bezdrátových sítí se používá širokopásmový přenos. Proto existují způsoby přenosu s cílem dosáhnout větší odolnosti proti rušícím vlivům, spolehlivosti a možnosti použití menších vysílacích výkonů. Jedná se o techniky rozprostřeného spektra – přímé sekvence DSSS (*Direct Semence Spread Spectrum*) a přeskoku kmitočtů FHSS (*Frequency Hopping Spread Spectrum*). [1]

### 2.4.2 SS (Spread Spectrum)

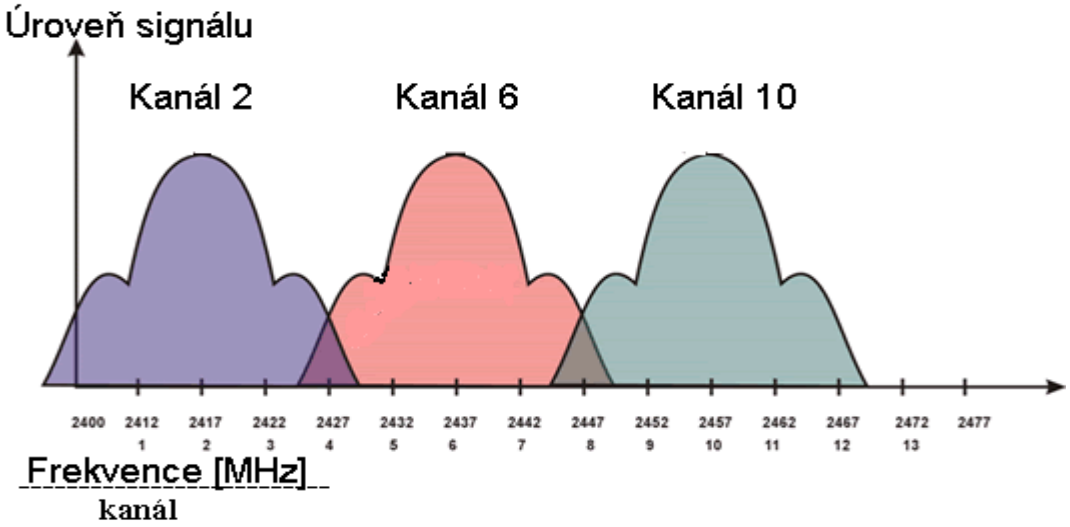
Komunikací s rozprostřeným spektrem se rozumí vysílání signálu s mnohem větší šířkou frekvenčního pásma, než je minimální šířka pásma potřebná k přenesení požadované informace. Rozdíl mezi úzkopásmovým rádiovým přenosem a rádiovým přenosem pomocí rozprostřeného spektra je v rozložení vysílací energie kolem své střední frekvence. U úzkopásmového přenosu je největší část vysílací energie soustředěna kolem své střední frekvence, zatímco u přenosu rozprostřeným spektrem je stejně velká vysílací energie rozložena na mnohem širším frekvenčním pásmu. Touto vysílací technikou se stává přenášená informace nedetekovatelná normálními přijímacími technikami, protože užitečná informace je pod hranicí šumu, kterou nedokáží úzkopásmové přijímače zpracovat. V praxi to znamená, že tyto systémy jsou mnohem odolnější proti interferencím generovanými jinými signály přítomnými ve stejném frekvenčním pásmu. Kmitočtové pásmo není efektivně využito, avšak

je dosáhnuto spolehlivějšího přenosu. Systém pracující s rozprostřeným spektrem musí splňovat podmínku, že vysílací šířka pásma musí být nejméně 10krát větší, než je šířka pásma přenášené informace. [1] [6] [7]

### 2.4.3 DSSS (Direct Sequence Spread Spectrum)

Přímá sekvence DSSS spočívá v tom, že jednotlivé bity jsou přenášeny pomocí chipů. Chipem rozumíme bitovou pseudonáhodnou sekvenci. V jednom chipu lze přenést 1, 2, 4 nebo 8 bitů podle zvolené rychlosti přenosu. Tato sekvence bitů je vysílána jako celek. Přenosový kód má délku 11 bitů a tyto kódy jsou vzájemně inverzní. Tento fakt zaručuje přímé sekvenci rozprostřeného spektra větší odolnost proti rušení. Použití odlišných sekvenčních kódů umožňuje umístění více systému do jednoho místa.

Tento systém využívá 11 kanálů, jejichž šířka je 22MHz. Povolené pásmo u frekvence 2,4GHz je však pouze 83,5MHz což znamená, že jednotlivé kanály se musí překrývat.
DSSS umožňuje, aby spolu existovaly maximálně tři systémy bez rušení. Aby mohlo spolu existovat více systému, bylo by nutné navýšit počet chipů, což by ale znamenalo potřebu několikanásobně rychlejšího rádiového přenosu. Nevýhodou této techniky je tzv. Near-Far Problem což znamená, že vysílače které jsou blíže k přijímači, mohou svým silným signálem porušit slabší signál vzdálenějšího vysílače, se kterým právě komunikuje.
Tento mechanismus se používá u standardů 802.11b a 802.11g. [1] [3] [6] [7]




*Obrázek 4: Překrývání kanálů u metody DSSS*

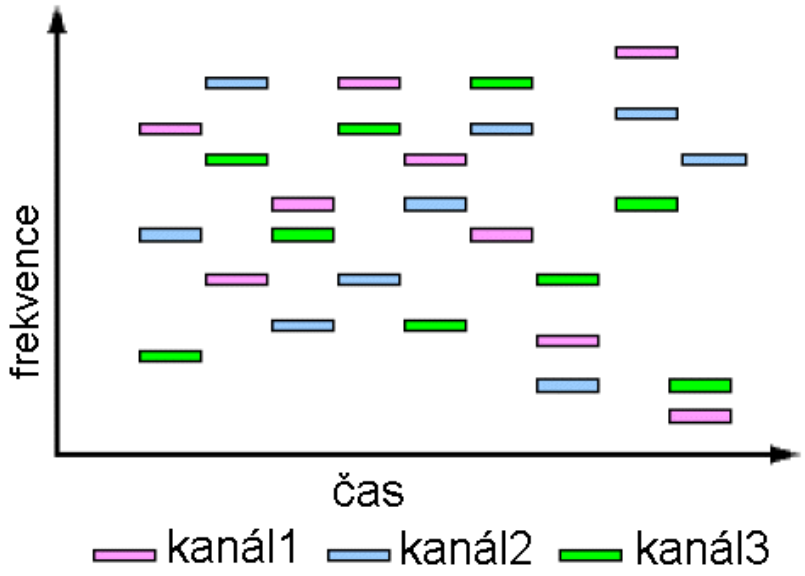
### 2.4.4 FHSS (Frequency Hopping Spread Spectrum)

Tzv. metoda přeskakování FHSS (*Frequency-hopping spread spectrum*) je metoda přenášení rádiových signálů, kde dochází k přepínání nosného kmitočtu mezi mnoha kanály za použití pseudonáhodné sekvence známé přijímači i vysílači. Jejím cílem je současná komunikace více zařízení.

Existují dvě varianty přeskoků frekvencí. Rychlé přeskoky FFH (*Fast Hopping* ), kde dochází k přeskokům i v průběhu přenosu jednoho bitu a pomalé přeskoky SFH (*Slow Hopping*), kde dojde ke změně frekvence až po přenosu několika bitů. Vysílaný signál je přenášen na určité frekvenci o šířce 1MHz po dobu přibližně 100-200ms (přeskoky

minimálně 2,5 krát za sekundu). Tuto dobu označujeme výrazem “dwell time”. Pro dobu přeskoku existuje výraz “hop time” a její přibližná hodnota je 200-300µs. Přeskoky, tzv. hops rozumíme přelazení na jiný kanál. Těchto kanálů může být až 79. Přeskok však musí být větší než 6MHz. Vysoké spolehlivosti je dosaženo díky faktu, že nepotvrzené - chybně přenesené rámce jsou přenášeny s jinou nosnou frekvencí v dalším přeskoku. Tato metoda dovoluje umístění více systému v jednom místě díky použití různých sekvencí v každém systému, teoreticky 26, prakticky 15.

Nevýhodou FHSS oproti přímé sekvenci je, že má menší propustnost a spotřebovává určitý čas na přeskok a synchronizaci na jinou frekvenci. Výhodou je lepší schopnost poradit si s vícecestným šířením signálu a menší citlivost na zpoždění přijímaných signálů. Rovněž zde neplatí Near-Far Problem. [1] [6] [7]




*Obrázek 5: přeskakování frekvence v závislosti na čase při použití metody FHSS*

### 2.4.5 OFDM (Orthogonal frequency-division multiplex)

U této techniky nedochází ke změně frekvence nosného signálu, avšak tato technika pracuje rovněž s rozprostřeným spektrem, jak tomu bylo u předešlých systémů. Tento kódovací mechanismus se používá především u standardů 802.11g a 802.11a, u standardu 802.11b se nazývá CCK (*Complementary Code Keying*). Dále své uplatnění nachází u systému digitálního pozemního vysílání DVB-T (*Digital Video Bradcasting – Terrestrial*), nebo u digitální technologie ADSL (*Asymmetric Digital Subscriber Line*).

Základem této techniky je rozložení frekvenčního spektra na menší části. Přenášená data jsou průběžně rozkládána do sub-kanálů a signál je přenášen na více nezávislých frekvencích. Tento fakt zvyšuje odolnost proti interferenci. Použitých nosných kmitočtů mohou být stovky i tisíce. Tyto nosné jsou dále modulovány modulacemi QPSK, 16QAM, 64QAM.

Tento mechanismus je téměř imunní proti chybám, způsobeným vícecestným šířením a různými odrazy. [1] [3]

## 2.5 Vrstva MAC a přístup k médiu

Vrstvu MAC u bezdrátové sítě můžeme rozdělit na dvě základní skupiny. První, hlavní metodou přístupu k médiu je DCF (*Distributed Coordination Function*). Základním přístupovým mechanismem této metody je CSMA/CA (*Carrier Sence Multiple Access / Collision Avoidance*). Metoda přístupu DCF je užita v každé bezdrátové stanici v síti v obou možných režimech, ad hoc i v módu infrastrukturním. Druhou metodou přístupu k médiu je PCF (*Point Coordination Function*). Tato metoda se na rozdíl od DCF používá pouze v infrastrukturní síti. Tento způsob přístupu koordinuje přístupový bod, který určuje oprávnění stanicím vysílat. Komunikace je realizována mechanismem virtuální nosné a nastavování indikátoru virtuálního naslouchání tzv. NAV (*Network Allocation Vector*) prostřednictvím rámců beacon. Metoda PCF je schopna pracovat v sítích, kde je použita metoda DCF. PCF je pouze volitelný mechanismus, který slouží pro přenos aplikací citlivých z hlediska času, tj, videa a hlasu.

### 2.5.1 DCF (Distributed Coordination Function)

Jak bylo již zmíněno, tato metoda umožňuje sdílení média přístupovým mechanismem CSMA/CA. CS (*Carrier Sence*) znamená, že stanice před vysíláním naslouchá na médiu a vysílá v případě, že je médium volné. MA (Multiple Access) znamená, že je umožněn přístup více stanic k médiu zároveň. Hlavní rozdíl bezdrátového a metalického Ethernetu je, že metalický Ethernet využívá mechanismus detekce kolizí CSMA/CD (*Collision Detection*), zatímco bezdrátový Ethernet využívá mechanismus předcházení kolizí CSMA/CA (*Collision Avoidance*). Důvodem je fakt, že v případě, že jsou stanice propojeny metalickým vedením, je každá stanice schopna rozpoznat vysílání jiné stanice a zjistit kolizi. Tento fakt u Ethernetu bezdrátového neplatí. Stanice je sice schopna detekovat volné médium, avšak to nemusí být volné i u přijímače. Jelikož veškerá komunikace stanice je směrována na přístupový bod, nemusí daná stanice rozpoznat komunikaci stanice jiné. Proto je nutno kolizím přecházet.
Celý proces začne tak, že stanice naslouchá a v případě, že je médium volné počká ještě určitý čas DIFS (*Dsitributed Inter Frame Space*), po kterém následuje vysílání. V případě, že stanice detekuje cizí signál nebo rušení, čeká do doby odstranění problému. Navíc okolní stanice dostávají zprávu o tom, na jak dlouho vysílací stanice obsadí přenosové médium. Tato informace je obsažena v hlavičce každého rámce. Doba, na kterou si jiná stanice rezervovala médium musí vypršet, aby další stanice mohl zahájit vlastní vysílání. Poté co vysílač uskuteční vysílání a přijímač přijímaní, provede přijímač kontrolní součet (CRC) paketu a odesílá paket potvrzovací (ACK) zpátky vysílači. Vysílací stanice přijímá potvrzovací paket (ACK) a to znamená, že nedošlo ke kolizi. V případě nepřijetí (ACK) paketu vysílací stanicí, opakuje vysílání.

Protokol CSMA/CA je určen pro snížení možnosti kolize tam kde je pravděpodobnost kolize největší, tzn. v době po ukončení předchozího vysílání. Ostatní stanice tuto dobu pomocí detekce nosné CS detekují a čekají. V situaci, kdy by stanice svá data začaly v této době vysílat, nastala by kolize. Stanice proto před vysíláním čeká určitou dobu, protože jakmile započne vysílání, není již schopna detekovat kolizi.

Nevýhodou metody CSMA/CA je citlivost na rušení. Mechanismus DCF také umožňuje realizovat útok typu zamezení využití služeb DoS (*Denial Of Service*) na bezdrátovou síť. Rušení může způsobit zablokování celé sítě až do doby odstranění rušení. [3]

### 2.5.2 PCF (Point Coordination Function)

Tato metoda je další metodou přístupu k médiu, kterou nabízí standard 802.11. Umožňuje, jak už bylo zmíněno výše, přenos dat citlivých na zpoždění. Základním prvkem je koordinátor, který určuje stanicím, kdy mají vysílat. Vysílání dat je prováděno synchronizovaně s definovanými prodlevami. Standard 802.11 umožňuje aplikování DCF i PCF zároveň tak, že stanice využívající DCF pravidelně předávají řízení sítě koordinátoru PCF.
Při použití režimu PCF je doporučováno vybírat aktivní síťové prvky od jednoho dodavatele, protože by mohly vzniknout problémy s komunikací zařízení od různých výrobců. [1]

### 2.5.3 Virtuální detekce nosné a rámce RTS/CTS

Základem metody virtuálního naslouchání nosné je předávání informací během přenosu a udržování těchto informací stanicemi v jejich vnitřní proměnné NAV. Pro informace o době obsazení média jsou definovány dva typy rámců RTS (*Request To Send*) a CTS (*Clear To Send*). Tyto obsahují informace o délce časového intervalu, který je potřebný pro přenos následujícího datového rámce.

Okolní stanice zachytí rámec RTS nebo CTS a zjistí z nich informaci o době obsazení média a nemají povolení v této době vysílat. I když některá stanice mechanismus RTS/CTS nevyužívá je povinna na tyto zprávy reagovat. V případě že stanice nedostane na svůj požadavek RTS odpověď CTS do stanovené doby aCtsTimeout, je rámec RTS znovu odesílán. Opakované zaslání rámce RTS trvá menší dobu, protože je tento rámec kratší.
Mechanismus řízení provozu RTS/CTS byl zaveden z důvodu potřeby minimalizace pravděpodobnosti kolize v bezdrátové síti. Protože standard umí využívat různé přenosové rychlosti, musí být RTS/CTS vysíláno tak, aby je byly schopny zachytit všechny stanice. [3] [4] [5] [8]

### 2.5.4 Seznam nejdůležitějších rámců

**Beacon** – tento rámec provádí synchronizaci bezdrátové sítě, nese informace o SSID (S*ervice Set Identifier*), o vodorovných rychlostech. Dále je v něm uvedeno o jaký typ sady služeb se jedná (ESS, BSS, IBSS), informace o zabezpečení WEP (*Wired Equivalent Privacy*) a MAC adresa přístupového bodu BSSID.

**RTS (Request To Send)** – žádost o přístup ke komunikačnímu kanálu pro přenos rámce

**CTS (Clear To Send)** – Potvrzení žádosti přístupu ke komunikačnímu kanálu

**Association Request & Association Responce** – žádost a potvrzení asociace

**Probe Request & Probe Responce** – vyhledávání sítí pomocí aktivního skenování a odpověď na tento dotaz

**PS Poll** – stanice, která se nachází v režimu snížené spotřeby, vyžaduje data uložená ve vyrovnávací paměti přístupového bodu

**ACK** – potvrzení bezchybně přijatého rámce

**Data** – datový rámec

## 2.6 Bezpečnost v bezdrátové síti

Jedním z nejdůležitějších témat v problematice bezdrátové sítě je i její zabezpečení. Tím rozumíme ochranu zranitelných míst a minimalizaci pravděpodobnosti možných útoků. Jelikož je komunikace vedena bezdrátově, je zabezpečení mnohem obtížnější než u sítí metalických, a proto je třeba s vylepšováním technologií bezdrátového přenosu vymýšlet i nové metody ochrany. Při studování této problematiky je důležité si uvědomit, že jedna ideální metoda ochrany dat neexistuje. Z toho důvodu je zabezpečení aplikováno ve více vlnách. Kromě přenášených informací a používaných služeb, potřebují ochranu i hardwarové zařízení a jejich uživatelé. Častým výsledkem útoku na bezdrátovou síť je poškození či zničení, v nejhorším možném případě ztráta poskytovaných služeb a informací.

Historie zabezpečení sítě začínala u velmi slabých metod zabezpečení, avšak s technickým pokrokem vznikly nové možnosti a metody ochrany informací a dnes lze síť Wi-Fi zabezpečit několika způsoby.

Jednoduchými a ne příliš bezpečnými metodami jsou například ukrytí identifikátoru sady služeb SSID (*Service Set Identifier*) nebo vytvoření pravidel pro filtraci přístupu MAC adres. Mezi ty složitější metody patří WEP nebo WPA (*Wi-Fi Protected Access*), která implementuje velkou část standardu 802.11i v podobě WPA verze 2.

### 2.6.1 Metoda skrytí SSID

Tato metoda zabezpečení sítě je častým způsobem ochrany sítě proti vniknutí neoprávněných uživatelů. Ve skutečnosti tento způsob nepředstavuje pro síť kvalitní zabezpečení a zkušený uživatel je schopen SSID odhalit během okamžiku.

Celý proces funguje tak, že po nastavení přístupový bod přestane vysílat název sítě SSID v synchronizačních rámcích a síť se stane skrytou. Toto nastavení se na většině přístupových bodů provádí aktivací položky “Enable SSID broadcast”. Tato varianta je prvním stupněm zabezpečení, tvoří pouze ochranu před nenakonfigurovanými zařízeními. [5]

### 2.6.2 Aplikování filtru řízeného přístupu (Access Control)

Dalším, ne příliš spolehlivě bezpečným způsobem ochrany sítě je zavedení seznamu povolených, nebo naopak zakázaných adres MAC klientských stanic v síti. Adresa MAC každého síťového rozhraní je 12ti místné hexadecimální číslo, které je jedinečné. Vytvoření seznamu těchto adres jasně určuje přístupovému bodu jaké stanici udělit a jaké neudělit povolení k připojení do sítě. V případě založení pravidla pro povolení uvedených adres (*Access list-Allow listed*), se AP chová tak, že jakákoliv jiná zařízení (jiné MAC) odmítá a uvedené v seznamu povolí. V opačném případě, kdy je na přístupovém bodu nastaveno pravidlo zakázaných adres (*Access list- Deny listed*), bude přístupový bod uvedené adresy ignorovat a všechny ostatní povolí.

Jelikož MAC adresa určitého zařízení by se neměla shodovat s žádnou jinou, od výroby přidělenou adresou jiného zařízení, zdá se, že by tato metoda měla mít hlavní roli v problematice zabezpečení sítě. Opak je pravdou. Tato metoda zabezpečení by měla sloužit rovněž jako doplňková. [5]

### 2.6.3 WEP (Wired Equivalent Privacy)

Zabezpečení WEP je definováno standardem 802.11 z roku 1999 a jak již český překlad (soukromí srovnatelné s drátovými sítěmi) napovídá, jedná se o techniku, která se snaží přiblížit kvalitu zabezpečení bezdrátové sítě kvalitě sítě metalické.

WEP pracuje na jednoduchém principu. Základem je algoritmus a statický klíč, který se používá jak u přístupového bodu, tak u všech stanic. Tento klíč je 40 bitový a k němu je ještě připojen inicializační vektor o 24 bitech, celkem 64 bitový klíč. Rozšířenou variantou je 104 bitová verze, která spolu vektorem inicializace tvoří 128 bitový klíč. Nadstandard poskytují výrobci zařízení o podpoře 256 bitového klíče. Tyto klíče se včetně adresy MAC používají k identifikaci a přihlášení k přístupovému bodu. K aplikaci klíče používá WEP proudovou šifrovací metodu s označením RC4, která zabezpečí informace a pro následné ověření správnosti provede výpočet ICV (*Control Check Value*) metodou cyklického kódu CRC-32 (*Cyclic Redundacy Code*). Poté dojde k inicializaci stavového pole KSA (*Key Sheduling Algorythm*), která klíč rozvrhne a přidělí kontrolní hodnotu rámce FCS (*Frame Check Sequence* ). Na straně příjemce se tento proces opakuje v opačném pořadí.

Metoda WEP má však mnoho slabostí jako například délku kódu, kolize inicializačních vektorů, nebo útoky prováděné zasláním změněných paketů, a proto je dnes spíše doporučováno používat důmyslnější metody jako WPA a WPA2. [1] [5]

# 3 STANDARD 802.11n

## 3.1 Úvod do standardu 802.11n

V posledních letech se technologie bezdrátových sítí o mnoho změnily. Jsou lepší, spolehlivější a sofistikovanější oproti předchozím standardům 802.11x. S průběžným vylepšováním a doplňováním standardů každých pár let, se rychlost a spolehlivost sítí mnohonásobně zvyšuje. Mnoho běžných domácích uživatelů technologií počítačových sítí je ochotno se vyrovnat se ztrátou rychlosti a dalších vlastností metalické sítě ve prospěch bezdrátových technologií. Možnost pohybovat s počítačem bez nutnosti použít metalické připojení je pro ně velmi lákavé. S rozvojem technologií se zvyšuje i nárok na rychlost a spolehlivost a tento požadavek útočí na společnosti, které vyrábí bezdrátový hardware, aby své výrobky neustále zlepšovali a těmto požadavkům přizpůsobovali. Nová technologie, ustanovená standardem IEEE 802.11 se tyto požadavky snaží v plném rozsahu splnit. Označuje se písmenem *n*. Rychlost, kterou si klade za cíl, by měla dosahovat na fyzické vrstvě až 540Mb/s, v budoucnu až 1Gb/s.

Podle této normy, 802.11n, jako tomu bylo u předchozích standardů, bude možné zařízením od různých výrobců udělovat certifikaci a garantovat schopnost spolupráce se zařízeními od různých výrobců. V současné době se na trhu vyskytují produkty podporující standard 802.11n několika značek podporující rychlosti až 300Mb/s. Certifikace těchto produktů se v průběhu doby konala ve více fázích. Od nástupu prvních zařízení podporujících tuto novou technologii na trh, se označení těchto zařízení průběžně měnily. První zařízení měly označení *pre-standard n*, poté *standard* a v současné době jsou některá zařízení v prodeji pracující pod standardem *802.11n (Draft2.0)*, který tvoří nadstavbu původnímu návrhu a přináší několik vylepšení. Celá historie návrhu 802.11n byla poněkud komplikovaná.

## 3.2 Vznik 802.11n

Celý proces vzniku nového standardu 802.11n začal v roce 2003 a v roce 2004 byli ustanoveny návrhy společností Wi-Fi Aliance, které stanovovali takové cíle, aby se dosáhlo rychlosti, jako u metalické sítě, to znamená 100Mb/s. Těchto návrhů se nejrůznějšími požadavky na nový standard objevovalo čím dál tím více a v roce 2005 bylo rozhodnuto a ustanoveny byly návrhy dva. Jeden skupinou WWiSE (*World Wide Spectrum Efficiency*) a druhý TGn Sync (*Task Group N*). Návrhy se shodovali v použití více antén, ale lišily se v šířce kanálů, v rychlosti přenosu a možnostech kódování.

Skupina WWiSE se ve svém návrhu snažila ponechat šířku komunikačního kanálu na 20MHz, jelikož by se tím dosáhlo i větší rychlosti přenosu, přibližně 135Mb/s. Rovněž tento návrh prosazoval použití většího komunikačního výkonu použitím technologie MIMO (*Multiple input-Multiple Output*). Teoretická přenosová rychlost byla 540Mb/s. Naopak návrh skupiny TGn Sync počítal s použitím dvojnásobné šířky kanálu, tedy 40 MHz. Tento fakt by ovšem znamenal úbytek kanálů ve frekvenčním pásmu 5GHz, a proto se od tohoto návrhu upustilo zpět na 20MHz. V návrhu byla také zahrnuta technologie MIMO s teoretickou rychlostí až 600Mb/s.

Zásadní krok ve vzniku standardu 802.11n přišel v podobě návrhu Draft 1.0 a hned poté v roce 2007 následovala nadstavba s názvem Draft 2.0. Toho samého roku byl zveřejněn návrh Draft 3.0. Návrh Draft 4.0 a následující Draft 5.0 byly odsouhlaseny v roce 2008.

## 3.3 Porovnání standardů

Prvním standardem, který ohromil trh, byl standard 802.11b, jehož vlastností byly kódovací techniky, které poskytovali rychlosti přenosu dat až 11Mb/s. Standard využíval techniku modulace CCK a také metodu přímé sekvence DSSS, který využívala také první verze standardu, 802.11. Dalším standardem, který vešel na trh je 802.11a, ustanovený přibližně ve stejnou dobu jako 802.11b. Modulace, kterou tento standard využívá je OFDM. Tato metoda umožňovala přenosovou rychlost až 54Mb/s. Standard pracuje na frekvenčním pásmu 5GHz. V roce 2003 byl ustanoven nový standard 802.11g. Využívá modulaci OFDM v pásmu 2,4GHz a maximální přenosová rychlost je 54Mb/s. Hardware využívající standard 802.11g byl rychle rozšířen mezi uživatele a firmy, jelikož byl standard s vyšší výkonností horlivě očekáván.

Většina dnešní bezdrátové síťové techniky podporuje standard 802.11g. Se stále se vyvíjející technologií se stává tato technika méně náročná na výrobu a také zařízení podporující oba standardy 802.11a i 802.11g v rámci jednoho procesoru, se zlevňují.
Podobně jako tomu bylo u standardu 802.11g přichází na trh nová technologie 802.11n. Společnosti specializující se na vývoj zařízení pro bezdrátové sítě, se na nový standard 802.11n plně soustřeďují již od roku 2006.

## 3.4 Charakteristika standardu 802.11n

Hlavní předností standardu 802.11n je, že umí využívat, jako tomu bylo u standardu 802.11b/g, frekvenci 2.4GHz i frekvenci 5GHz (802.11a). Zároveň je zpětně kompatibilní s těmito standardy a umožňuje současné využití standardů 802.11a i 802.11n na frekvenci 5GHz nebo 802.11b/g a 802.11n na frekvenci 2.4Ghz. Možností konfigurace tohoto standardu je také znemožnit zpětnou kompatibilitu se standardy 802.11a/b/g. Krom toho, disponuje také technologiemi, které kladou důraz na větší propustnost dat, spolehlivost a pokrytí. Tyto technologie se nazývají MIMO, agregace paketů a sdružování kanálů. [9] [10]

## 3.5 MIMO (Multiple input – multiple output)

### 3.5.1 Základ rádiového přenosu

Jádrem celé problematiky standardu 802.11n je technologie vícenásobného vstupu a vícenásobného výstupu MIMO. Pro správné pochopení této techniky je třeba ovládat problematiku klasických rádiových přenosů starších standardů.

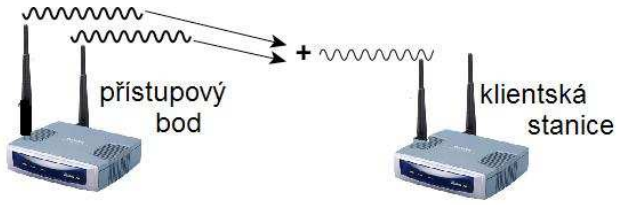
V klasické, jednovstupní – jednovýstupní technice SISO (*Single input – single output*), je informace přenášená rádiovým signálem závislá na velikosti jakou překročí přijatý signál hluk v přijímači, který se nazývá odstup signálu a šumu SNR (*Signal to Noise Ratio*). Jeho jednotkami jsou decibely (*dB*). Míra hodnoty tohoto odstupu značí množství informací, které je rádiovým signálem přenášeno a přijímačem obnoveno. Vysoká velikost hluku v cestě šíření rádiového signálu znamená nižší hodnotu SNR a tím snížené množství přenášených informací. Hluk je častým jevem, vzniká v přírodě i uměle. [9] [10] [11]

### 3.5.2 Formování vysílaného signálu (Beamforming)

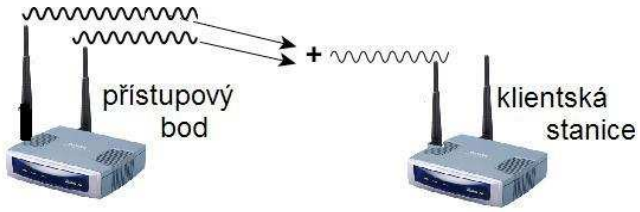
Cílem technologie MIMO je zvyšování hodnoty odstupu SNR a k tomu využívá několik technik. Jedna z nich se nazývá formování vysílaného signálu (*beamforming*).
K přenosu signálu je použito více antén a tím je umožněno řídit vysílaný signál tak, že výsledkem je výrazně lepší signál na straně přijímače. Hlavní využití nachází tato technika v případech, kdy přijímač používá pouze jednu anténu nebo v případě odrazů signálu. Proces se dá vysvětlit tak, že si představíme signál jako vlnu s vlastní určitou vlnovou délkou, která se spolu s vlnou z druhé antény vysílače šíří směrem k anténě přijímače, kde jsou tyto vlny sečteny. Ovšem v závislosti na vzdálenosti, kterou se vlny pohybují, je pravděpodobné, že na cílové místo dorazí ve fázovém posunu, a to ovlivní celkovou intenzitu celého signálu. Technika beamforming se snaží vyladit fáze rádiových signálu tak, aby signál v přijímači byl maximální s vysokým odstupem šumu.

Formování signálu může být aplikováno na straně vysílače bez informací z přijímače o přijatém signálu. Tato informace, je zpětně vysílači zasílána pouze ze zařízení pracujících na standardu 802.11n a je platná jen určitý čas.

Použití této techniky je efektivní pouze v případě, kdy je připojen pouze jeden přijímač. Vylazovaní fází není možné v případě vysílání na všechny přijímače (broadcast) nebo výběrového vysílání (*multicast*). Z toho důvodu jsou nastavení formování signálu v uživatelských aplikacích dost omezené. Technika se výhradně používá při nutnosti rychlého přenosu dat na větší vzdálenost. [9]




*Obrázek 6: Signál bez formování*




*Obrázek 7: Vyladění fáze pomocí techniky Beamforming*

### 3.5.3 Diverzní mód (Diversity mod)

Základem chování tohoto módu je použití více antén ke zvýšení kvality signální cesty mezi vysílačem a přijímačem. Tato metoda může být implementována na jednom nebo na obou koncích bezdrátového spoje. Antény jsou nastaveny, aby byly schopny přijímat signál z různých cest a v případě, že se detekuje zvýšená hodnota šumu či oslabení signálu vlivem rušení, je anténa okamžitě přepnuta. Funkce této metody je zkomplikována, protože vysílač neobsahuje primární informaci o přijímači, díky které by mohl sestavit a optimalizovat cestu šíření signálu. Řešením je proto použít pro vysílání anténu, ze které byl předtím signál nesoucí informaci úspěšně doručen na přijímací stanici.

Výhodou tohoto módu je zvýšení dosahu, pokrytí bezdrátové sítě, zlepšení propustnosti a vetší schopnost při hledání kvalitních cest pro šíření signálu, tak aby jednotlivá

zařízení mohly pracovat spolehlivě a vyhnuly se chybám v přenosu a následným opakovaným vysíláním. [9]

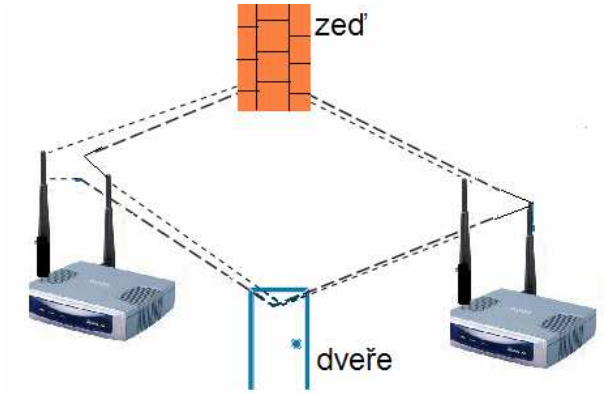
### 3.5.4 Diverzní kódování (Diversity Coding)

Metoda diverzního kódování se používá v případě použití diverzní módu k zakódování signálu technikou, která se volným překladem z angličtiny nazývá časoprostorové kódování (*Space-time Coding*). Tato metoda se používá k optimalizaci šířeného signálu a může být také kombinována s vícecestným šířením SP. [9]

### 3.5.5 Vícecestné šíření (Spatial Multiplexing Mode)

Hlavní předností technologie MIMO je, že využívá princip šíření rádiové vlny, který cíleně vybírá cestu, tak aby přenesená informace byla v nejlepší kvalitě.

Technika vícecestného šíření funguje na základě rozdělení signálu o vysoké rychlosti na více toků o menších rychlostech, kde každý je přenášen jinou anténou na stejném kanále. Metoda vícecestného šíření se používá ke zvýšení kapacity bezdrátové sítě na vyšších odstupech signálu od šumu SNR. V prostředích kde jsou signály oslabené vzdáleností, hladinou šumu nebo interferencí není tuto metodu výhodné použít, protože v takovém případě je identifikace cest jednotlivých signálů pro vysílač i přijímač obtížnější. V případě takové situace technologie MIMO vrací k módu diversity. [9]




*Obrázek 8: Chování technologie vícecestného šíření signálu*

### 3.5.6 Antény v technologii MIMO

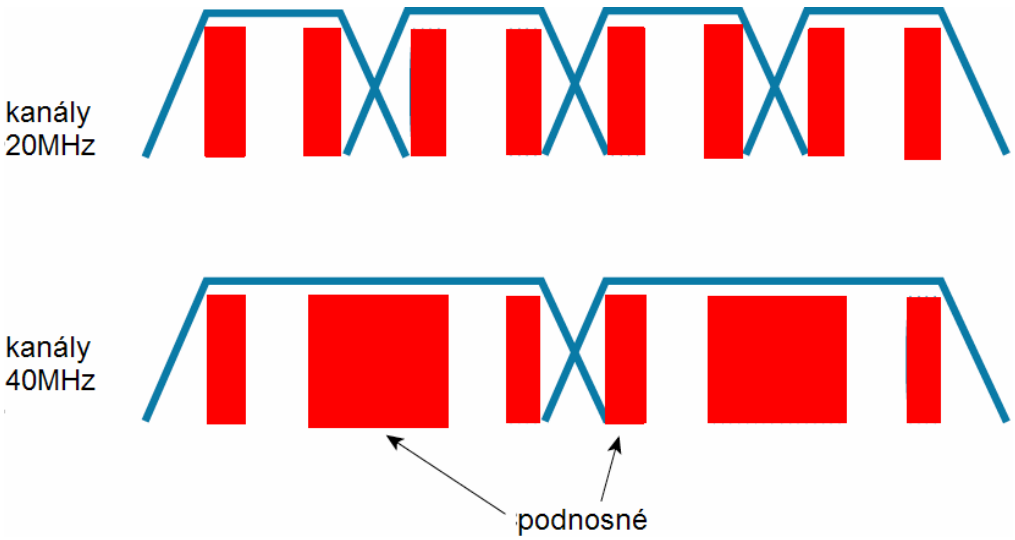
Systémy MIMO využívají, jak již bylo řečeno, větší počet antén. Počet vysílacích a počet přijímacích se označuje AxB kde počet A značí počet vysílacích a B přijímacích antén, například (2x2). Standard definuje více možností počtu antén, základní (2x1) je typický pro techniku formování signálu a největší počet, který je v současné době definován je 4x4. Větší počet antén znamená vetší schopnost vypořádat se s šumem a tím zvýšit i odstup SNR. Rozdíly v odstupu šumu při použití většího počtu antén jsou velmi znatelné. Tato metoda je největším přínosem standardu 802.11n. [9]

## 3.6 Fyzická vrstva

Standard 802.11n definuje oproti standardům 802.11a/b/g mnoho změn v technice bezdrátového vysílání. Jsou to především změny šířky kanálu, modulace a snížené náklady na režii.

### 3.6.1 Sdružování kanálů (Channel bonding)

Původní standardy používají pouze jeden z kanálů o šířce 20MHz. Standard 802.11n k vysílání využívá techniku, která se nazývá sdružování kanálů (*Channel bonding*) tak, že kombinuje dva sousední kanály o šířce 20MHz a spojuje je do jediného kanálu o šířce 40MHz. Tato technika je nejefektivnější v pásmu 5GHz, kde existuje větší množství kanálů, oproti pásmu 2,4GHz, ve kterém existují pouze 3 nepřerývající se kanály. Výsledkem je pouze dvoutřetinové využití celkové kapacity. Standard proto definuje jasná pravidla pro práci s kanály o šířce 40MHz a 20MHz tak, aby byla zajištěna maximální kapacita a optimalizace sítě. Obrázek níže zobrazuje rozdíl mezi použitím kanálu o šířce 20MHz a 40MHz. [9] [10]




*Obrázek 9: znázornění rozdílu mezi využitím kanálu o šířce 20Mhz a 40Mhz*

### 3.6.2 Agregace paketů (Packet Aggregation)

Metoda agregace paketů spočívá ve zvýšení efektivity bezdrátového přenosu agregací aplikačních dat do jednotlivého přenosového rámce. Takto může síť posílat vícenásobné pakety s fixními režijními náklady v jednom rámci. Metoda agregace paketů je výhodná pro aplikace, jako je kopírování souborů. Na druhou stranu například pro aplikace jako je přenos hlasu příliš přínosem není, protože by agregace paketů mohla způsobit, že budou pakety roztroušené v jednotlivých pravidelných intervalech. To by pro takovou aplikaci znamenalo větší hodnotu odezvy (latency). [9] [10]

### 3.6.3 OFDM

Pomocí metody přímé sekvence, která je standardem 802.11 definována, je každou mikrosekundu vysílán jeden symbol skládající se z 11 chipů. Jednotlivé chipy jsou pomocí modulační techniky PSK (*Phase-shift keying*) modulovány a v závislosti na rychlosti přenosu je každou mikrosekundu zaslán určitý počet symbolů. U 1Mbit/s je přenášen jeden symbol každou mikrosekundu a u rychlosti 2MBit/s jsou už symboly dva ovšem za použití nadstavby modulační techniky QPSK (*Quadrature phase-shit keying*). Standard 802.11b vylepšuje metodu přímé sekvence, tím že v rámci jednoho symbolu je zakódováno více bitů. To způsobí nárůst přenosové rychlosti až na 11Mb/s.

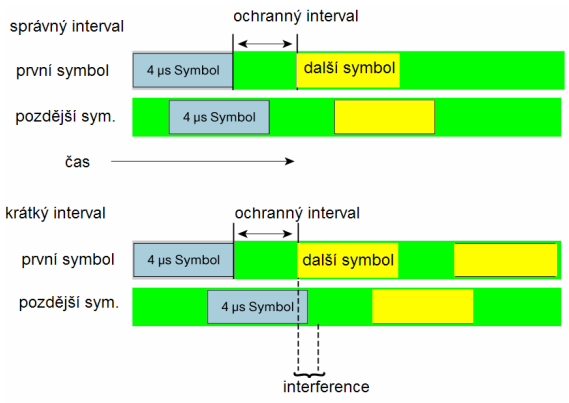
Standardy 802.11g a 802.11a k přenosu symbolu radiovým signálem využívají metodu OFDM, kde každý symbol trvá čtyři milisekundy a při nejvyšší možné rychlosti 54MB/s obsahuje 216 bitů. Ty se rovnoměrně rozprostřou mezi 48 nosných, které jsou modulovány metodou 64QAM (*Quadrature amplitude modulation*).

Podobně jako u 802.11a a 802.11g i standard 802.11n využívá metodu OFDM a přenášený symbol trvá čtyři mikrosekundy. Vylepšení spočívá v nárůstu počtu nosných na 52, které připadají na každý kanál šířce 20MHz. Tím dochází i k zvýšení rychlosti z 54Mb/s na 65Mb/s. Standard 802.11n také definuje několik dostupných rychlostí přenosu v závislosti na počtu antén. V případě použití kanálu o šířce 20MHz je například pro dvě antény maximální rychlost 130Mb/s, 3 antény 195Mb/s a pro 4 antény 260Mb/s. Použitím kanálu o šířce 40MHz se počet nosných rapidně zvyšuje až na 108. Tím se zvyšuje i maximální dostupná rychlost až na 540Mb/s. Celkem má standard 802.11n pro obě šířky kanálu definováno až 32 možných rychlostí. [9]

#### 3.6.3.1 Ochranný interval (guard interval)

Součástí symbolu je tzv. ochranný interval (*guard interval*), jehož rolí v problematice OFDM je zabránit interferenci jednotlivých symbolů. Ta vznikne, když se tyto symboly k přijímači dostávají různými cestami a první symbol má cestu k přijímači delší než symbol následující. Výsledkem je, že nový symbol dorazí k příjemci v době, kdy předchozí symbol ještě není zcela přijat. Tato interference snižuje odstup šumu SNR celého rádiového spoje. Z toho důvodu existuje mezi jednotlivými symboly ochranný interval, který zabezpečuje symboly vyslané dlouhými cestami. Tento interval je označován jako doba klidu. Jeho velikost definovaná standardy 802.11g a 802.11a je 800 nanosekund na rozdíl 800 stop.

Standard 802.11n také využívá ochranný interval o délce 800 nanosekund, ovšem používá i zkrácený interval 400 nanosekund v případě, kdy to podmínky prostředí bezdrátové sítě dovolují. [9]




*Obrázek 10: rozdíl mezi správným přijímáním symbolů a interferencí*

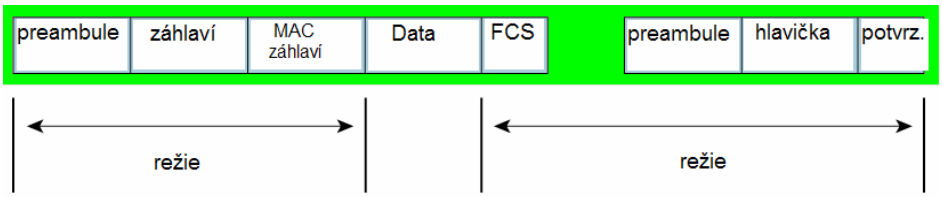
## 3.7 Vrstva MAC a přístup k médiu

Podobně jako ve fyzické vrstvě, obsahuje standard 802.11n oproti dřívějším standardům 802.11 ve vrstvě MAC několik úprav. Důvodem proč bylo nutné standard upravit, je především mnohonásobně vyšší přenosová rychlost.

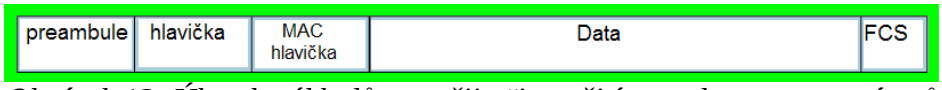
Vrstva MAC obsahuje množství režie důležité pro funkci bezdrátové sítě. V případě vysokých rychlostí, jakých je u tohoto nového standardu používáno, by mohlo dojít k tomu, že by režijní náklady byly větší než vysílané datové rámce. Proto je standardem definována úprava s názvem agregace rámců, jejímž cílem je tyto náklady na režii snížit.

### 3.7.1 Agregace rámců (Frame aggregation)

Vysílané rámce obsahují pevnou režii, úvodní část a rámcové pole. Tyto snižují propustnost celé sítě. Za účelem zamezení tohoto problému byla vyvinuta metoda agregace rámců, která se snaží náklady na režii redukovat. Principem je vkládání dvou nebo více rámců do jednoho přenosu. Také velikost rámců byla zvětšena, z původních 4KB na 64KB. Výsledné agregované rámce však musejí být při vysílání zaslány do stejného místa. To znamená, že všechny rámce uvnitř agregovaného rámce musejí být směrovány k jedinému koncovému zařízení. Další podmínkou této metody je, že všechny rámce, které jsou agregovány, musejí být před vysíláním připraveny ve stejném čase. Také velikost rámce není libovolná. Maximální velikost je ovlivněna časem (*channel coherence time*), který nesmí být menší než čas po který trvá přenos. Zjednodušeně řečeno, v případě, že se obě strany bezdrátového spoje pohybují, velikost vysílaného rámce se zmenšuje a tím klesá i maximální přenosová rychlost. Agregace rámců existuje ve dvou verzích, MSDU (*MAC Service Data Units Aggregation*) a MPDU (*Mac Protocol Data Units Aggregation*). [9]




*Obrázek 11: Režijní náklady bez použití metody agregace rámců*

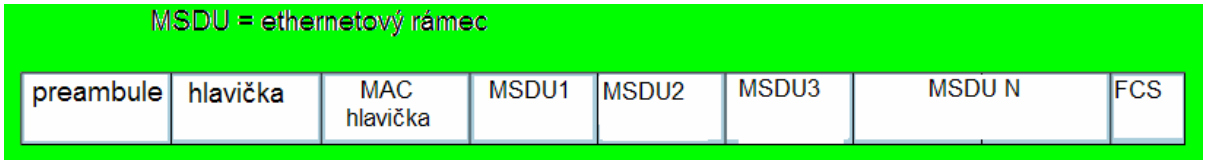



*Obrázek 12: Úbytek nákladů na režii při použití metody agregace rámců*

#### 3.7.1.1 MSDU (Mac Service Data Units Aggregation)

Přístupový bod na svém Ethernetovém rozhraní přijímá Ethernetové rámce, které následně musí přeložit do rámce definovaného standardem 802.11 a až poté vyšle k cíli. Také klientské stanice vytváří Ethernetové rámce, které musejí být přeloženy. Metoda agregace MSDU shlukuje Ethernetové rámce a agreguje je do jednoho rámce standardu 802.11 bez překládání. V případě, že agregovaný rámec vyšle klientská stanice přístupovému bodu, jednotlivé Ethernetové rámce jsou směrovány do svých cílů. Pokud je to naopak, agregovaný rámec vyšle přístupový bod, všechny obsažené Ethernetové rámce mají jediný stejný cíl a tím je klientská stanice. Podmínkou použití této metody je, že všechny rámce musejí být na stejné

úrovni kvality služeb. Tato technika je efektivnější než MPDU, protože nemá vysoké náklady na režii. [9]

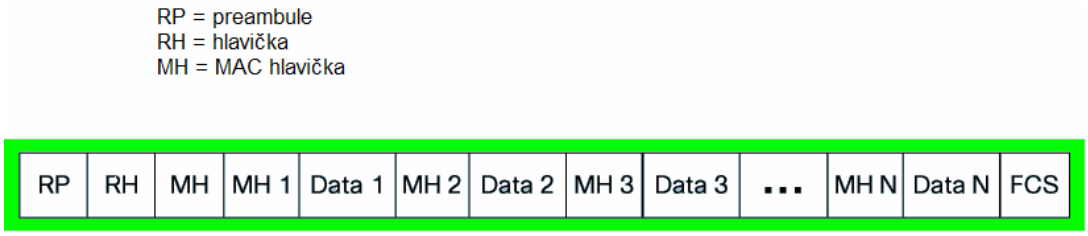



*Obrázek 13: Rozvržení rámce metodou MSDU*

### 3.7.1.2 MPDU (Protocol Data Unit Aggregation)

Tento mechanismus na rozdíl od MSDU agreguje překlady Ethernetových rámců do jednoho rámce 802.11 a poté je zasílá do jejich cílových stanic. Metoda MPDU nevyžaduje, aby rámce byly vysílány do stejného cíle. Pokud je rámec zaslán klientskou stanicí, cílem je přístupový bod, kde jsou rámce 802.11 přeloženy na Ethernetové rámce a dále směrovány do cíle. V případě, že rámec vyšle přístupový bod, je jediným cílem klientská stanice.
Agregace MPDU podporuje zabezpečení jednotlivých rámců pomocí bezpečnostní asociace ke svému cíli. Použití této agregace je rovněž podmíněno tím, že všechny rámce musejí mít stejnou úroveň kvality služeb.

Tato technika agregace je méně efektivní než první zmíněná MSDU, protože při procesu agregace musí být individuálně na každý rámec aplikována zvláštní režie. Její efektivita ještě více klesne při použití zabezpečení, které potřebuje další režii. [9]




*Obrázek 14: Rozvržení rámce metodou MPDU*

### 3.7.1.3 Blokové potvrzování (block acknowledgement)

Jelikož metoda agregace MPDU vyžaduje potvrzování každého rámce zvlášť, byl vyvinut mechanismus blokového potvrzování, který sestavuje všechna potvrzení všech rámců agregovaných metodou MPDU do jediného rámce. Ten je jako potvrzení příjemcem zasílán odesílateli. Tento mechanismus umožňuje opětovné selektivní vysílání rámců, které nebyly potvrzeny. Uplatnění nachází v problémových, zarušených oblastech, kde zvyšuje efektivitu a celkovou propustnost. [9]

### 3.7.1.4 Zmenšení mezirámcového prostoru

Existují případy, kdy není možné zmíněnou agregaci rámců aplikovat, v tomto případě by tedy znovu vyvstal do popředí problém příliš velikých nákladů na režii potřebnou při zasílání rámců do různých cílů. Za potřebou odstranění tohoto problému byl vyvinut jiný mechanismus, který zmenšuje prostor mezi rámci přijatými, potvrzeními a rámci odeslanými. Tento prostor je označován jako RIFS (*Reduced interframe space*). Nevyužitý čas mezi rámci

je zkrácený a získaný čas použitý k vysílání rámců. Tento mechanismus je možno použít pouze u standardu 802.11n. [9]

## 3.8 Kompatibilita

Kompatibilita standardů 802.11 a/b/g/n je velmi podstatným tématem v problematice každého nově příchozího standardu. Standard 802.11n disponuje několika mechanismy zpětné kompatibility se staršími standardy, jejichž základem je domluva na společné komunikaci, aby jednotlivá zařízení rozuměla mezi sebou přenášeným informacím. Jelikož současně nejrozšířenějším standardem je 802.11g, je pochopitelné, že se nový standard 802.11n bude muset ještě dlouho přizpůsobovat a to až do doby kdy budou všechna zařízení vyměněna za zařízení podporující standard 802.11n. Důvodem je fakt, že se aplikace metod zpětné kompatibility odráží na režijních nákladech, celkové propustnosti a výsledné kvalitě vylepšení, které standard 802.11n přináší.

### 3.8.1 Sdružený mód (mixed mode)

Mechanismus zpětné kompatibility 802.11n vychází z mechanismu zpětné kompatibility standardu 802.11g se standardem 802.11b. Podobnost tkví v tom, že standard 802.11 vysílá signál, který není možné dekódovat pomocí zařízení starším standardů, avšak je mimo to schopný vysílat i v tzv. módu smíšeném (*mixed mode*). Tento mód přenáší úvodní část rámce a signální pole, kterým standardy 802.11a a 802.11g rozumí a mohou je dekódovat. Tyto postačí zařízením se staršími standardy, aby zjistili informaci o chování rádiového přenosu. Zbytek rámce nový standard vysílá již ve formě 802.11n pomocí metody vícecestného šíření. [9]

### 3.8.2 CTS-to-self

Další metodou pro zpětnou kompatibilitu je mechanismus, který zařízením v síti umožňuje rozeznat, kdy mají povolení vysílat a kdy nikoli. Jeho anglický název je CTS-to-self. Funguje tak, že zařízení standardu 802.11n vysílá krátký rámec CTS, jehož cílem je vlastní adresa a obsahem informace o časování vysílání. Tato chrání vysílání standardem 802.11 a musí být přenášena mezi ostatní zařízení pracující na starších standardech rychlostí, kterou tyto standardy podporují, aby ji mohli přijmout a dekódovat. [9]

# 4 STANDARD 802.11e

## 4.1 Úvod do standardu 802.11e

Jako každá nově příchozí technologie má i standard 802.11 své slabé stránky. V porovnání s klasickými metalickými sítěmi jsou méně spolehlivé a často se chovají nepředvídatelně. To je z většiny způsobeno vlivy rušení nebo špatnými podmínkami prostředí. Důvodem je vzduch, který je jako bezdrátové medium mnohem obtížnější na koordinaci a řízení sítě než metalické vedení. Technologie bezdrátových sítí dále omezuje šířku pásma a má veliké náklady na celkovou režii. Nevýhodou standardu 802.11 je také to, že funguje v bezlicenčních pásmech. Proto je současné době velmi pravděpodobné, že právě naše síť bude omezována jinými bezdrátovými sítěmi. Z hlediska hardwaru, jsou zařízení omezována svou velikostí, váhou nebo výkonem. Všechny tyto zmíněné nevýhody jsou pro bezdrátovou síť velmi limitující. O vytvoření ideálního řešení a předcházení problémů s omezenou šířkou pásma se v bezdrátové síti stará správa kvality služeb Qos (Quality of Service).QoS se snaží splňovat požadavky využívaných aplikací a řízení datových zdrojů. Za tímto účelem využívá určité mechanismy, které kontrolují přístupy a využití bezdrátového média. Tyto metody zakládají na faktu, že každá aplikace ke své práci potřebuje šířku pásma, určitou úroveň latence a minimální chybovost paketů. Například pro přenos hlasu po síti VoIP (Voice over Internet Protocol) je podstatná velikost odezvy, a proto je této aplikaci udělena velká priorita pro přístup k médiu. Na druhou stranu například přenos videa je priorizován zvláště pro šířku pásma, velikost odezvy v tomto případě klíčová není. Aplikace jako je textová komunikace (email, ICQ) je správou služeb zvýhodněna pro co nejmenší chybovost paketů.

Původní standard 802.11 nedefinuje rozdíly ani priorizaci. Proto nedokáže optimalizovat síť pro efektivnější a spolehlivější využívání aplikací jako jsou video nebo hlas. Tento nedostatek v hierarchii doplňuje standard 802.11e. Hlavním rysem je, že definuje změny a vylepšení ve správě QoS. Nejdůležitější vylepšení je vylepšení efektivního využití šířky pásma a snížení množství režie. Dále je to snížení odezvy pomocí prioritizace paketů podle typu přenosu a rozdělení zdrojů podle potřeby odezvy.

Standard 802.11e mimo jiné také upravuje názvy aktivních prvků sítě. Přístupový bod, který podporuje správu kvality služeb QoS se nyní nazývá QAP (QoS Access Point) a stanice s podporou QoS je QSTA (QoS Station). Zároveň i základní sada služeb BSS je přejmenována na QBSS (Qos Basic Service Set). Počínaje těmito změnami, standard 802.11e představuje i novou metodu přístupu k médiu za účelem komplexního vylepšení vrstvy MAC a správy QoS.

## 4.2 Vrstva MAC a přístup k médiu

### 4.2.1 HCF (Hybrid Coordination Fiction)

Tato nová norma představuje hybridní koordinační metodu přístupu k médiu HCF (Hybrid Coordination Function), která kombinuje funkce již zmíněných metod DCF a PCF s rozšířenou podporou kvality služeb a novými typy rámců. Tato metoda funguje ve dvou módech. Vylepšený distribuční koordinovaný přístup EDCA (Enhanced Distribution Coordinate Access) a hybridní přístup HCCA (HCF Controlled Channel Access). Tyto módy pracují na principu kontroverze (contention-based) a dotazování (polling-based).

Standard dále definuje pojem TXOP (Transmission Opportunity), který je specifikován dobou, po kterou je QSTA v právu vysílat. Jinými slovy, jakmile dostane

příslušná stanice právo na přístup k mediu, je jí přiděleno povolení TXOP. TXOP je charakterizován začátkem časového úseku a maximální délkou časového úseku, který se nazývá TXOP limit. Jakmile stanice QSTA obdrží právo TXOP, může začít vysílat pouze však do té doby než vyprší časový limit TXOP limit. Časový úsek tohoto limitu je nastaven přístupovým bodem QAP. [12] [13]

#### 4.2.1.1 EDCA (Enhanced Distributed Channel Access)

Tento mód obsahuje změny v přístupu k médiu vylepšením původní metody DCF. Základem je prioritizace různých datových toků. Definuje čtyři možnosti přístupu, kterým se říká přístupové kategorie AC (*Access Categories*). Ty jsou přidělovány různým typům přenosu, pro které jsou specifikovány různé služby a aplikace. [12] [13]

##### 4.2.1.1.1 Přístupové kategorie (Access Categories)

Pro každou přístupovou kategorii jsou přiděleny rámce různých datových toků a to podle požadavků na kvalitu služby určité aplikace. Jedná se o aplikace na pozadí (background) AC_BK, aplikace s požadavkem na největší výkon (best effort) AC_BE, aplikace pro přenos hlasu (voice) AC_VO a aplikace pro přenos videa (video) AC_VI. Kategorie AC_BK nejmenší prioritu a naopak AC_VO největší. Každý rámec si nosí informaci o vlastní prioritě. Hodnota této priority odpovídá prioritě uživatelské UP (User priority) a podle typu komunikace nebo aplikace určuje původ každého rámce. Existuje celkem 8 úrovní priorit.

Dalším tématem v problematice standardu 802.11e je přidělování těchto priorit na vyšších vrstvách. Standard 802.11e totiž nedefinuje metodu jak přidělovat tyto priority ve vyšších vrstvách než je vrstva MAC. O to by se tedy měla starat aplikace, která datový tok vytváří. Jedním řešením by bylo, že by v budoucnu byly všechny aplikace kompatibilní s tímto standardem, aby bylo využití sítě co nejefektivnější. Druhá možnost by byla prioritu adaptivně přiřazovat na aplikační vrstvě. To by probíhalo na základě údajů o velikosti paketů, intervalů mezi pakety, nebo velikosti datového toku. To by ovšem znamenalo zásadní úpravy vyšších vrstev. [12] [13]

##### 4.2.1.1.2 EDCAF (Enhanced Distributed Channel Access Function)

Každá stanice definuje pro každou přístupovou kategorii přenosovou frontu a funkci metody přístupu EDCAF (*Enhanced Distributed Channel Access Function*). EDCAF je vylepšením původní DCF. Funguje také na stejném principu přístupu k mediu. Základem jsou ovšem parametry, které jsou specifické pro kategorie přístupu. Jinými slovy, jsou jakýmsi prostředkem při určování kategorie přístupu. [12] [13]

##### 4.2.1.1.3 Parametry EDCA

Metoda přístupu EDCA je založena na parametrech, které jsou přiřazeny přístupovým kategoriím. Parametry jsou následující: TXOP limit je maximální časový limit, během kterého má stanice přístup k médiu a tudíž může probíhat přenos. Zkratkou AIFS (*Arbitration Inter-Frame Space*) je označována domluvená doba naslouchání k médiu před zahájením přenosu. Parametry $CW_{max}$ a $CW_{min}$ označují maximální a minimální velikost prostoru ke kontroverzi (*Contention Window*).

Hodnoty těchto parametrů jsou pro každou přístupovou kategorii individuální. Kategorie s nízkou prioritou musí čekat delší čas AIFS, zatímco časová perioda provozu s vysokou prioritou je velmi krátká. Velikost časového limitu TXOP limit závisí také na úrovni priority. Přenos s větší prioritou má oprávnění vysílat po delší dobu oproti přenosu s nižší prioritou.

Kategorie s vysokou prioritou mají přidělenou nižší hodnotu CW, u nízké priority je to naopak. Pravidlem je, že se zvyšující se úrovní priority klesají hodnoty AIFS a CW, a naopak hodnota TXOP se zvyšuje.

Často bývají tyto parametry označovány zkratkami AIFS[AC], $CW_{min}$[AC], $CW_{max}$[AC] a TXOP limit [AC]. O pravidelné zasílání hodnot těchto parametrů se stará přístupový bod podporující správu služeb QoS. Jeho schopností je také tyto hodnoty upravovat v závislosti na prostředí s cílem zajistit maximální efektivitu. Pro případ, že by QAP nebyl schopný hodnoty pravidelně stanicím zasílat, definuje standard základní hodnoty těchto parametrů. [12] [13]

#### 4.2.1.1.3.1 AIFS (Arbitration Inter- Frame Space)

Tento pojem specifikuje minimální časový interval, po který musí stanice na médiu nečinně naslouchat. Po jeho vypršení se může u kategorie s vysokou prioritou spustit daný přenos. U méně prioritní kategorie se spustí časovač, po který se bude přenos doslova držet zpátky. Oproti fixní hodnotě DIFS je velikost tohoto intervalu proměnná a závisí na přístupové kategorii. Hodnota intervalu AIFS je určena výrazem (1)

$$\mathbf{AIFS = AIFSN \,.\, aSlotTime + aSIFSTime} \quad (1).$$

aSlotTime značí časový úsek, aSIFSTime je časová perioda SIFS (*Short Inter-Frame Space*) a pojem AIFSN (*Arbitration Inter-Frame Space Number*) značí počet přebývající časových slotů. Pro každou přístupovou kategorii je definováno různé AIFSN, tedy různé množství slotů. Se zvyšující se úrovní priority, hodnota AIFSN klesá. U nízké priority je množství time-slotů vyšší. Nejnižší možná hodnota čísla AIFSN je 2. Po sečtení zjistíme, že se tato minimální velikost shoduje s minimální velikostí intervalu DIFS u metody DCF. Metoda HCCA definuje minimální možnou hodnotu čísla AIFSN a to je 1.
Přístupová kategorie s vyšší prioritou má definovanou nižší hodnotu čísla AIFSN. Ve výsledku to znamená, že na započetí vysílání je třeba čekat kratší dobu. Pro kategorii s nižší prioritou to znamená, že se přenos po tento čas nesmí probíhat a to až do doby vypršení časovače (backoff timer).

Kategorie s vysokou prioritou mají takto zajištěnou velkou šířku pásma. Výhodou pro tyto kategorie je také nízký časový interval AIFS, který zaručuje, že bude provoz bez zpoždění. Zpoždění by mohlo totiž u určitých aplikací vyvolat velké problémy. Na druhou stranu kategorie s nízkou prioritou mají vyšší interval AIFS a tudíž i větší zpoždění, to však v určitém množství jejich výkon pod přijatelný limit nesníží. [12] [13]

#### 4.2.1.1.3.2 $CW_{min}$ & $CW_{max}$

Hodnota těchto parametrů není pevná jako u metody DCF, ale mění se v závislosti na přístupové kategorii. Nižší priorita má menší hodnotu parametru $CW_{min}$ a $CW_{max}$ a naopak vyšší priorita má hodnotu větší. Čím je hodnota tohoto parametru nižší, tím se sníží i velikost časového intervalu, po který je zakázáno vysílat (backoff time). Výsledkem je, že daná přístupová kategorie musí čekat na uvolnění média kratší čas, než kategorie s nižší prioritou,

která má hodnotu časovače backoff vyšší. Nevýhodou nízkých hodnot CW, u vysokých priorit je častý výskyt kolizí. Se snižující se hodnotou CW totiž roste pravděpodobnost přidělení stejné hodnoty backoff. To by způsobilo vypršení časovače ve stejnou chvíli a kolizi dvou přístupů.

Hodnoty $CW_{max}$ u kategorií s vysokými prioritami jsou nastaveny tak, aby byly menší než hodnoty $CW_{min}$ u kategorií s malými prioritami. To znamená, že v případě kolize a zdvojnásobení velikosti CW, je tato hodnota $CW_{max}$ stále nižší než hodnota $CW_{min}$ u kategorií s nižší prioritou. Kromě toho to také znamená, že kategorie s nízkou prioritou musí hodnotu CW zdvojnásobovat po každém neúspěšném přenosu do doby, než dosáhne hodnoty $CW_{max}$ a musí si nastavit na vyšší hodnotu také časovač backoff. Hodnota CW kategorií s vysokou prioritou se po několik neúspěšných přenosech stává konstantní s nízkou hodnotou časovače backoff, a proto obdrží povolení k přístupu k médiu. Tímto způsobem je kategoriím s vysokou prioritou poskytnuta větší šířka pásma v případech nestability a velké vytíženosti sítě. Toto řešení samozřejmě na druhou stranu způsobuje újmu kategoriím s nižší prioritou a to až do doby, kdy si budou moci časovače backoff přenastavit na nižší hodnoty. [12] [13]

#### 4.2.1.1.3.3 TXOP (Transmission opportunity)

Po úspěšném získání přístupu k médiu následuje vysílání, které je definováno časovým úsekem. Ten se nazývá TXOP a jeho maximální hodnota je charakterizována hodnotou TXOP limit. Jakmile je uděleno oprávnění TXOP může začít vysílání, pouze však do doby, kterou charakterizuje TXOP limit. Doba mezi těmito mezemi zahrnuje vysílání rámců RTS/CTS, potvrzení ACK i časové periody SIFS.

Pro různé přístupové kategorie jsou přiděleny různé limity TXOP. Nenulová hodnota parametru TXOP limitu znamená, že je kategorii umožněno v tomto časovém úseku vysílat své vícenásobné rámce až do hodnoty TXOP limit. Toto se nazývá nekontroverzní impuls CFB (*Contention Free Bursting*). Sousledný tok rámců je rozdělen a mezi jednotlivé rámce jsou vloženy časové periody SIFS místo period AIFS+backoff. Důležitý je fakt, že tyto vícenásobné rámce musí spadat pouze pod jednu přístupovou kategorii.
V některých případech je také spolu s mechanismem CFB aplikována metoda RTS/CTS. Výhodou je, že ověřování RTS/CTS nemusí probíhat před vysíláním každého rámce v impulsu CFB, ale pouze před prvním rámcem.

Je-li mechanismu CFB aplikován, je také v záhlaví rámce v poli *Duration* uložen záznam o zbývajícím čase TXOP. Díky tomu si každá stanice nastaví parametr virtuálního naslouchání nosné NAV (*Network Allocation Vector*) na celou velikost časového úseku TXOP, namísto doby trvání pouze jednoho rámce. Tímto způsobem je v tomto případě aplikováno virtuální naslouchání nosné.

Je-li hodnota limitu TXOP rovna nule, je nemožné mechanismus přenosu vícenásobných rámců CFB použít. V takovém případě může být přenesen pouze jeden rámec. Existuje-li navíc riziko, že dojde k přesáhnutí časového limitu TXOP limit. Je nezbytné, aby byl tento rámec rozdělen.

U přístupových kategorií s nízkou prioritou jsou základní hodnoty parametru TXOP nula. To znamená, že u nich není možné aplikovat mechanismus CFB. Naopak u kategorií s vysokou prioritou jsou hodnoty TXOP nenulové, tudíž je možné mechanismus CFB použít a tím obsadit médium na určitý čas. Ve výsledku to znamená výrazně nižší zpoždění. Příliš vysoké limity TXOP ale mohou kategoriím s nižší prioritou způsobit velké zpoždění.
Parametr TXOP je zásadní veličinou, která tvoří velké rozdíly mezi kategoriemi s velkou a malou prioritou v problematice přístupu k médiu. [12] [13]

#### 4.2.1.2 HCCA (HCF Controlled Channel Access)

Tato přístupová metoda je definována standardem 802.11e za účelem parametrizace kvality služeb QoS. Metoda HCCA řeší zásadní problémy metody PCF, které vedly v rámci této metody k velmi špatnému výkonu správy kvality služeb.

Metoda HCCA prezentuje různé přenosové třídy, které se nazývají přenosové proudy TS (traffic streams). Díky tomu mohou firmy navrhovat vícetřídové algoritmy pro různé typy aplikací. Ty jsou z hlediska implementace považované za závislé na HCCA a mohou být neustále vylepšovány. Novým vylepšením, které standard 802.11e přináší je, že stanice QSTA nesmí vyslat paket v případě, že není možné dokončit přenos rámce před dalším synchronizačním rámcem beacon. Tento fakt řeší zásadní problém zpoždění rámců beacon u metody PCF. Další úpravou metody HCCA je použití časového limitu TXOP limit k stanovení délky časové periody, při které je dotázané stanici umožněno vysílat.

Přístupový bod QAP během synchronizačního intervalu beacon může vysílat několik impulsů CFB, které se u metody HCCA nazývají kontrolované přístupové periody CAP (*Controlled Access Periods*). Toto může provést v jakémkoliv čase po detekci nečinného kanálu, pouze však na určenou dobu, která je označována jako PCF mezirámcový prostor PIFS (*PCF Inter-Framce Space*). V případě že je interval PIFS delší než interval AIFS, zvolí přístupový bod QAP místo metody EDCA metodu HCCA. Metoda HCCA je oproti původní PCF více flexibilnější a to z toho důvodu, že původní PCF může být aplikována pouze v rámci nekontroverzní časové periody CFP (*Contention-Free Period*), zatím metoda HCCA může být inicializována kdykoliv v době trvání celého beacon intervalu. Metoda PCF se v porovnání s novou HCCA stává zbytečnou, avšak v rámci standardu 802.11e zůstává volitelnou možností. Maximální dobu trvání přístupu HCCA definuje veličina $T_{CAPlimit}$.

Před každým datovým přenosem se provádí proces, při kterém dochází ke specifikaci přenosového proudu. Každý proud má určitou prioritu a každá stanice má maximálně 8 různých priorit těchto proudů. QSTA za cílem inicializace datového proudu, vysílá přístupovému bodu QAP dotaz (QoS Request Frame), který obsahuje informaci o daném přenosu TSPEC (*Traffic Specification*). TSPEC definuje požadavky daného přenosového proudu na kvalitu služeb QoS. Jsou to požadavky na datovou rychlost, maximální velikost rámce, zpoždění a velikost servisního intervalu RSI (*Required Service Interval*). Servisním intervalem rozumíme maximální dobu mezi jednotlivými časovými úseky TXOP, kterou je určitá aplikace ochotna tolerovat. Přístupový bod QAP po přijetí informace o požadavcích nejprve určí tento servisní interval. Jeho velikost by měla být největší zlomkovou částí celkové velikosti synchronizačního intervalu beacon. Zároveň však nesmí jeho velikost překročit maximální dobu, kterou definují přijaté požadavky na RSI od různých stanic. Poté je interval beacon rozdělen na určitý počet servisních intervalů, během kterých jsou jednotlivě dotazovány všechny stanice. Tímto způsobem jsou jednou během nejnáročnějšího požadavku na zpoždění zvoleny všechny přenosové proudy. Nakonec přístupový bod díky požadavkům na kvalitu služeb jednotlivých přenosových proudů vypočítá pro každou stanici hodnotu TXOP a přiřadí ji. [12]

## 4.3 Architektura

Standard 802.11e kromě zmíněných EDCA a HDCA obsahuje i metody DCF a PCF definované původním standardem 802.11. Důvodem je, podobně jako u standardu 802.11n, zpětná kompatibilita. Stanice podporující správu služeb QSTA je schopna pracovat v základní sadě služeb BSS podporující QoS tzn. QBSS, ale zároveň je také zpětně kompatibilní a tudíž může pracovat i v základní sadě služeb nepodporující QoS tzv. non-QoS BSS (nQBSS). Umožněno je to tím, že je daná stanice schopná asociovat se s přístupovým bodem

nepodporujícím QoS tzv. non-QoS AP (nQAP) a to v případě že QAP není pro stanici dostupný. Kromě tohoto je také stanice nQSTA schopna komunikovat s QAP v QBSS tak, že se chová jako klasická stanice definovaná standardem 802.11 a z druhé strany i přístupový bod QAP pro komunikaci s touto stanicí nepoužívá rámce podporující QoS.

Metoda HCF používá k centrálnímu řízení hybridní koordinátor HC (*Hybrid Controller*). Je umístěn na přístupovém bodu a jeho přední činností je spolupracovat s metodou EDCA. Každá metoda má však trochu jinou funkci. EDCA pracuje během periody kontroverze CP (*Contention Period*), zatímco HC operuje navíc i během periody CFP. Můžeme si jej představit jako řídící mechanismus metod EDCA a HCCA. [13]

### 4.3.1 Formáty rámců

#### 4.3.1.1 Pole QoS subfield v kontrolním rámci

Pro správnou komunikaci je důležitá informace o jednotlivých stanicích, jestli pracují s podporou QoS či nikoliv. Jinými slovy jestli se jedná o QSTA nebo nQSTA. Tato informace je přenášena v hlavičce v poli kontrolního rámce *Frame Control field*. Název této informace je QoS subfield. Je-li hodnota nula, znamená to že, stanice je typu nQSTA, jeli hodnota této informace 1, daná stanice QoS podporuje a je tudíž QSTA. Následující obrázek prezentuje datový rámec a pozici informace o podpoře QoS dané stanice. [13]

#### 4.3.1.2 Identifikátor provozu TID (Traffic Identifier)

Každému rámci je na vrstvě MAC přiřazena určitá priorita. Ta je definována veličinou, která se jmenuje identifikátor provozu TID (*Traffic Identifier*). Tato informace je uložena v poli TID Filed, které je obsaženo v poli QoS Control Field. Na základě této hodnoty je definována uživatelská priorita, která se určuje čísly 0-7. prioritizace TID může být aplikována pouze v případě, že má daná stanice podpole QoS Subfield v poli kontroly rámce nastaveno na hodnotu 1. V případě, že je nastavena hodnota 1, funguje spojení mezi stanicí a přístupovým bodem se službou podpory služeb, tedy QAP- QSTA. Je-li hodnota 0, znamená to, že stanice nemá v dosahu přístupový bod QAP ale pouze AP (nQAP). V takovém případě stanice funguje pouze jako klasická STA (nQSTA) a identifikátor TID nemá význam. Rámce jsou stanicí, podobně jako tomu je u metody DCF u standardu 802.11, vysílány s kontroverzní priorizací a na straně AP je s nimi nakládáno jako s běžnými rámci. Stejně tak i v případě, když existuje spojení mezi STA (nQSTA) a QAP, jsou stanicí vysílané rámce přístupovým bodem priorizovány hodnotou 0, tedy nejnižší hodnotou. [13]

#### 4.3.1.3 Velikost front (Queue size field)

Kromě pole TID Field je v poli QoS Control Field uložena hodnota velikosti front (Queue size field). Tato hodnota definuje počet rámců konkrétní priority, které daná stanice obsahuje ve frontě přenosu přístupových kategorií. [13]

#### 4.3.1.4 Hodnota požadované doby TXOP (TXOP duration requested)

V obou zmíněných metodách EDCA i HCCA se používá parametr, který definuje povolenou dobu vysílání, TXOP. U první z metod se tento parametr nazývá EDCA-TXOP a u druhé HCCA-TXOP. Je-li aplikována metoda EDCA je v případě povolení přístupu k médiu

použit parametr EDCA-TXOP. Hodnota HCCA-TXOP je přidělena jednotlivým stanicím hybridním koordinátorem HC během aplikace metody HCCA.

Stanice s podporou QoS může definovat požadavek na přenos vícenásobných rámců během doby trvání TXOP. Učiní tak tím, že nastaví hodnotu v poli Duration field na dobu požadovanou pro přenos dalších rámců. Je-li aplikována metoda HCCA mže stanice QSTA tento požadavek definovat nastavením pole požadované doby k přenosu (TXOP Duration Requested Field), které je umístěno v poli kontroly služeb (QoS Control). Následně může přístupový bod QAP přidělit požadovanou hodnotu TXOP. V některých případech určí menší než požadovanou hodnotu.

Při použití metody EDCA jsou hodnoty a parametry této metody definovány v tzv. sadě parametrů metody EDCA (EDCA Parametr Set). Ta je pravidelně v synchronizačních beacon rámcích rozesílána přístupovým bodem. Přístupový bod může také tyto hodnoty v závislosti na podmínkách prostředí přizpůsobovat. Parametry se ukládají do polí AIFSN, TXOP limit, $ECW_{min}$ a $ECW_{max}$ . Stanice, která tyto parametry přijme, s nimi začne pracovat a snaží se získat přístup k médiu. V případě že přístupový bod neumí tyto parametry nastavovat a rozesílat, jsou standardem 802.11e definovány základní hodnoty těchto parametrů.

Pro každé, nově vytvořené parametry metody EDCA, přístupový bod zvýší hodnotu pole, které nese informaci o současně vysílané sadě těchto parametrů a vysílá jej v každém rámci. Toto pole se nazývá počítadlo inovovaných sad parametrů metody EDCA (EDCA Parametr Set Update Count Field) a je uloženo v poli informací o podpoře kvality služeb (QoS Info Field). Tuto techniku používají stanice k tomu, aby vždy pracovali s nejaktuálnější sadou parametrů a nebyly znevýhodněny v přidělování přístupu k médiu. [13]

## 4.4 WMM – Wi-Fi Multimedia

Zájem a poptávka po multimediálních aplikacích a pokročilých schopností bezdrátových sítí Wi-Fi rychle vzrůstá. Je to podníceno především nově vznikajícími zařízeními a potřeby neustále rozšiřovat funkce sítí koncových zákazníků. V současné době jsou nejžádanější aplikace vyžadující podporu správy kvality služeb hlasové (VoIP), přenos streamovaného videa a hraní počítačových her. Podpora těchto aplikací ve firmách a na veřejných místech umožňuje poskytovatelům a vlastníkům těchto sítí optimalizovat infrastrukturu sítě tak, aby nabízela bohatší a rozmanité sady služeb.

Až donedávna byla velikou nevýhodou bezdrátových sítí skutečnost, že standard 802.11 nemá definovanou žádnou podporu služeb a řízení propustnosti dat pro jednotlivé protokoly a aplikace. Přestože to zprvu nevypadalo na zásadní problém, postupem času jak se Wi-Fi sítě staly hlavním standardem pro bezdrátové spoje, vznikl požadavek na priorizaci jednotlivých datových provozů a to především u multimediálních aplikací.

Z hlediska hardwaru se tento problém stal zásadním pro každý přístupový bod AP. Ten se snaží rozdělovat přenosové pásmo, dle algoritmu, který však neobsahuje žádná pravidla, kterými by se daný přístupový bod mohl řídit v případě většího zatížení sítě. První připojený klient obdrží od přístupového bodu veškeré zdroje, ale když se připojí více klientů, snaží se přístupový bod vyhovět všem. To může způsobit problémy pro aplikace, které jsou citlivé na vyrovnanou charakteristiku datového přenosu multimediální aplikace. Takový případ znamená ve Wi-Fi síti nerovnoměrný datový přenos, který může způsobit přerušování přehrávané hudby, videa nebo komunikaci VoIP.

Předním řešením tohoto problému je technika, která by zaručila poskytnutí podpory kvality služeb QoS. [15]

### 4.4.1 Vznik a vztah 802.11e a WMM

Počátkem roku 2001 se začalo připravovat řešení tohoto problému pod názvem 802.11e. Jedná se o další přírůstek do rodiny standardů 802.11, který byl však až v polovině roku 2005 skupinou TGe ustanoven. Jak již bylo řečeno v předcházející kapitole standard 802.11e tvoří velmi komplexní řešení, které je pro budoucí zařízení, domácnosti i náročné firmy velmi otevřené. V současnosti však takováto komplexnost a rozšiřitelnost není zapotřebí, jelikož většina nároků a požadavků pochází od domácích uživatelů. Z toho důvodu standard 802.11e řeší toto situaci vznikem jakési podmnožiny funkcí QoS, která se jmenuje WMM (Wi-Fi Multimedia).

WMM můžeme nazvat jakýmsi profilem, který obsahuje výběr funkcí standardu 802.11e. Tyto funkce jsou potřebné pro současně nejžádanější aplikace, tedy multimediální aplikace hlas, video nebo hudba. Architektura profilu WMM je stavěna tak, aby zařízení s podporou WMM byly plně kompatibilní se zařízeními podporující připravovaný standard 802.11e. V ideálním případě bude v budoucnu možné současným WMM zařízením vylepšit firmware aby plně podporoval standard 802.11e. [15]

### 4.4.2 Certifikace standardu WMM

Standardu WMM byl podobně jako tomu bylo u standardu 802.11n vypsán certifikační program za cílem kontroly zpětné kompatibility zařízení od různých výrobců. Certifikát jednotlivých zařízení by měl uvádět jakými funkcemi a standardy dané zařízení disponuje. Krom toho by měl certifikát informovat uživatele o možných rychlostech přenosu,

bezpečnostních standardech a standardech s podporou multimédií. V případě že je daný výrobek certifikován, je kompatibilní s jinými výrobky, které jsou rovněž certifikovány. Podobně jako u standardu 802.11n, WiFi Alliance se tímto snaží předejít možné nekompatibilitě a různým definicím standardů. Předními výrobci čipů, které standard WMM podporují, jsou: Cisco, Netgear, Intel, Zyxel, Atheros a Broadcom.

### 4.4.3 Spolupráce se zařízeními bez podpory WMM

Většina zařízení, které jsou uvedeny na trh, nepodporují správu kvality služeb QoS. Proto standard WMM umožňuje, aby v rámci jedné sítě mohli zařízení s podporou i zařízení bez podpory WMM spolupracovat. Aby tato zpětná kompatibilita mohla fungovat, musí přístupový bod standard WMM podporovat. Vlastník sítě tak musí tato zařízení do sítě aplikovat nebo do starších přístupových bodů instalovat software, který standard WMM podporuje. [15]

### 4.4.4 IETF DiffServ architektura

Standard WMM je založen na architektuře DiffServ, která je stavěná tak, aby poskytovala správu kvality služeb technologiím jako je Wi-Fi. Jejím cílem je poskytnout efektivní priorizaci provozu bez velkých nároků na režii.

Architektura DiffServ mimo jiné umožňuje funkci Universal Plug and Play QoS (UPnP QoS) za účelem řízení funkcí WMM. Umožňuje správcům sítí vytvořit a uplatnit po celé síti pravidla, které jsou aplikovaná na drátové i bezdrátové infrastruktuře. [15]

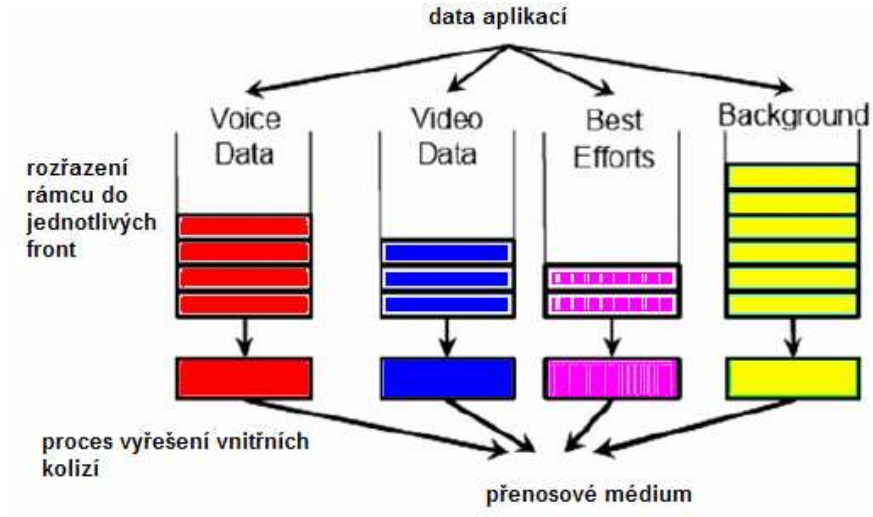
### 4.4.5 Přehled funkcí a operací standardu WMM

Standard WMM tvoří zásadní vylepšení vrstvy MAC u standardů bezdrátových sítí. Jedná se o vylepšení původního DCF mechanismu, který je založen na technice předcházení kolizím CSMA/CA. Původní DCF uděluje všem zařízením v síti stejnou prioritu tzv. best effort. To znamená, že každý klient čeká jistý čas, po jehož vypršení začne zařízení vysílat ovšem pouze v případě že současně nevysílá jiné zařízení. Metoda předcházení kolizím, umožňuje všem zařízením vysílat, avšak v případě velkých požadavků na přenos se stane síť přetížená a kvalita přenosu se výrazně sníží.

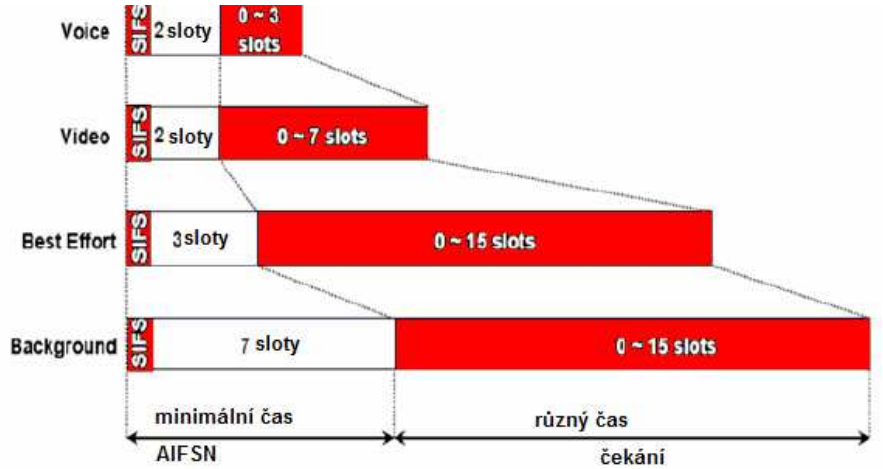
Standard WMM představuje priorizaci datového přenosu která se podobně jako u 802.11e zakládá na čtyřech přístupových kategoriích. Tato technika řeší nedostatky mechanismu DCF s cílem podpory multimediálních aplikací. Přístupové kategorie jsou nastaveny tak, aby odpovídaly prioritám standardu 802.11d a současně vypomohly mechanismům, které řídí správu kvality služeb QoS. Jak je vidět na obrázku, aplikace přiřazují datové pakety do jednotlivých přístupových kategorií. Pakety jsou poté na straně klienta řazeny do čtyř nezávislých front. Jednotliví klienti mají vnitřní mechanismus (Internal collision resolution mechanism), který směruje kolize mezi jednotlivé fronty a umožňuje vysílat rámce s největší prioritou. Stejný systém klienti používají na řešení externích kolizí za účelem určování, kterému klientovi bude umožněno vysílat.

Tyto mechanismy se starají o priorizaci datového přenosu a závisí na dvou časových parametrech. První se nazývá minimální mezirámcový prostor AIFSN (Arbitary Inter-Frame Space Number). Druhým parametrem je tzv. prostor kolize CW (Contention Window). Obě hodnoty se se zvětšující se prioritou zmenšují. Pro každou přístupovou kategorii je vypočítána doba nečinnosti, která je rovna součtu periody AIFSN a hodnoty, která se pohybuje mezi

nulou a hodnotou CW. Hodnota CW se s časem mění. Původní hodnota CW je definována pro každou přístupovou kategorii zvlášť. Při každé kolizi je hodnota CW zdvojnásobena do doby než dosáhne své maximální hodnoty.




*Obrázek 15: Fronty přístupových kategorií*




*Obrázek 16: Časování u přístupových kategorií*

Po úspěšném přenosu nabyde hodnota CW opět své původní hodnoty. Povolení k započetí přenosu dostávají ty rámce, které mají vysokou prioritu a nejnižší hodnoty doby nečinnosti. Jakmile klient dostane povolení k přenosu TXOP, může vysílat, avšak pouze po dobu která je definována dle dané kategorie a rychlostí na fyzické vrstvě. Například hodnota TXOP se v síti standardů 802.11a/g pohybuje mezi 0,2ms (aplikace na pozadí) a 3ms (video přenos) a v síti standardu 802.11b přibližně mezi 1.2ms a 6ms. Tato vlastnost výrazně vylepšuje efektivnost velkých přenosů dat. [14] [15]

Standard WMM byl navržen současně se standardem 802.11e. Jedná se o podmnožinu funkcí, které umožňují správu kvality služeb a jsou v širším měřítku obsaženy v současném návrhu standardu 802.11e. Standard WMM je založen na mechanismu EDCA rovněž definovaného standardem 802.11e. Komplexní standard 802.11e navíc zahrnuje funkce, které budou pravděpodobně v budoucnu do profilu WMM přidány jako volitelné moduly.

# 5 ZAŘÍZENÍ 802.11n a 802.11e

## 5.1 Směrovač D-Link DIR-655

Tento bezdrátový směrovač patří mezi přední výrobky prezentující standard 802.11n. Přesněji řečeno podporuje návrh 802.11n (Draft 1.0). To umožňuje oproti standardu 802.11g až o 650% rychlejší přenos dat. Teoretická propustnost je až 300Mb/s. Jeho předností je technologie, která minimalizuje rušivé efekty při provozu více aplikací v bezdrátové síti. Dále směrovač disponuje podporou 802.11e - WMM, díky které se priority nastavují během provozu na základě situace, za cílem dosáhnutí vysoké kvality přenosu bez výpadků a zpoždění. Výhodou je i technologie zúžení požadovaného rádiového spektra, jejímž cílem je potlačení rušivých efektů vůči ostatním bezdrátovým sítím v okolí.

Směrovač obsahuje funkce k zabezpečení bezdrátového přenosu, jsou jimi WEP WPA a WPA2. Dále obsahuje funkce překládání síťových adres NAT, tiskový server a DHCP server. Vysílací vysokofrekvenční výkon je přibližně 15dB, který je obstaráván třemi odpojitelnými anténami. Pro připojení do metalického Ethernetu má směrovač 4 porty podporující 10/100/1000Mb/s a jeden port 10/100Mb/s pro připojení zařízení do internetu.

Svými funkcemi se toto zařízení staví na přední místo současné nabídky produktů pro bezdrátové sítě.


*Obrázek 17: Směrovač D-Link DIR-655*

## 5.2 Klientské zařízení D-Link DWA-643

Klientské zařízení D-Link DWA-643 pracuje rovněž na technologii 802.11n o návrhu (Draft 2.0). Je určeno notebookům se slotem ExpressCard/34. Oproti starším zařízením určeným do slotů PCMCIA, disponuje menší velikostí a rapidně zvýšenou rychlostí mezi zařízením a notebookem.

Podporuje maximální teoretickou přenosovou rychlost 300Mb/s a svým výkonem poskytuje přibližně 5 krát větší pokrytí než standard 802.11g. Podporuje metodu rozprostřeného spektra DSSS a metodu rozdělení nosné frekvence OFDM. Z metod zabezpečení disponuje toto zařízení funkcemi WEP, WPA, WPA2. Maximální vyzařovací

výkon je 17dB. Zpětná kompatibilita je zajištěna se standardy 802.11b a 802.11g. Toto zařízení podporuje správu kvality služeb, které zajišťuje standard 802.11e.


*Obrázek 18: Klientské Zařízení D-Link DWA-643*

# 6 ÚVOD DO PRAKTICKÉ ČÁSTI

Tato část bakalářské práce se čtenáři snaží přiblížit problematiku moderních standardů bezdrátových sítí 802.11n a 802.11e. Jednotlivé testy ozřejmují chování a schopnosti standardů v praxi. Práce se zaměřuje na vlastnosti bezdrátového spoje z hlediska propustnosti dat, velikosti odezvy a síly signálu v závislosti na vzdálenosti či použitých překážkách.

U jednotlivých měření jsem použil stejnou metodiku a stejné typy zařízení, aby nedošlo ke vzniku negativních vlivů na výsledné hodnoty měření. V prostoru, kde měření probíhalo, se nacházely aktivní rádiové prvky, které mohly měření ovlivnit.

K měření jsem sestrojil PC stanici o procesoru Core 2 Duo E8500, základní desce Gigabyte s čipem P35, disku o kapacitě 120GB s rozhraním SATAII Maxtor a gigabitovém Ethernetu od firmy Broadcom. Na druhé straně jsem použil notebook Acer Aspire 5662 s procesorem CoreDuo T2700 a slotem ExpressCard osazený klientskou radiovou stanici D-Link DWA-643 Extreme N Notebook ExpressCard pro měření vlastností standardu 802.11n a notebook Hewlett Packard Compaq nx6110 s rádiovým čipem Broadcom BCM4318bg pro měření vlastností standardu 802.11g. Na obr. jsou znázorněny vyzařovací charakteristiky všesměrových antén použitých. Jako hlavní rádiový prvek jsem použil D-Link DIR-655. K měření jsem volil záměrně výkonné komponenty, aby nedošlo ke zkreslení výsledných hodnot vlivem pomalejší schopnosti přenosu dat jednotlivých součástí. Za cílem větší věrohodnosti měření jsem na PC stanici nainstaloval operační systém Linux distribuce Debian, zkompilovaný pro dvě jádra procesoru. Notebook Acer pracoval pod operačním systémem Microsoft Windows XP Professional SP3 a notebook Hewlett Packard pracoval rovněž pod systémem Debian. Měření jsem prováděl zejména na straně PC stanice, kde jsem vytvořil skript (uveden níže), který výsledné hodnoty propustnosti dat obou směrů a velikosti odezvy měří a následně exportuje do textových souborů.

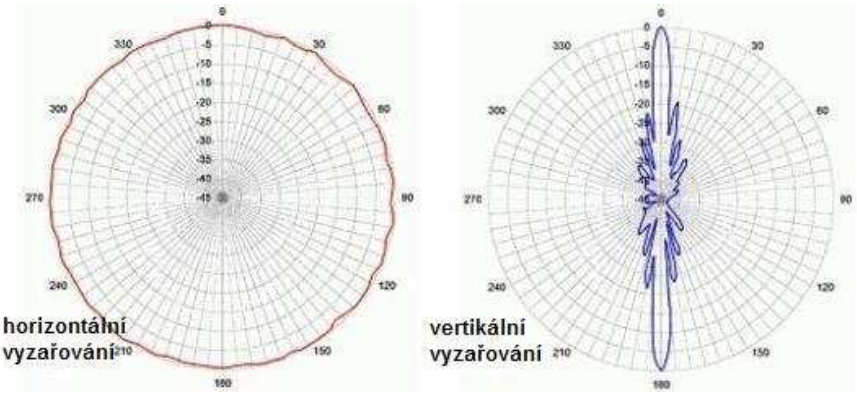
```
#!/bin/bash
while true; do
# Datum
ACT_DATE=`date`
# Statistika upload
POLE_UPLOAD=`iptables -L INPUT -v -x -Z -n | awk '
  NR > 2 && $1 != "Zeroing" {
         printf("%s#%s\n", $8, $2);
  }
'`
# Statistika download
POLE_DOWNLOAD=`iptables -L OUTPUT -v -x -Z -n | awk '
  NR > 2 && $1 != "Zeroing" {
         printf("%s#%s\n", $9, $2);
  }
'`
echo "=========================="
echo "$ACT_DATE"
# Zobrazeni vystupu
echo "$POLE_UPLOAD" | awk -vFS="#" '
  {
         $2 = $2 / 1024;
         printf("UPLOAD: %s %d KB\n", $1, $2);
  }
'
echo "$POLE_DOWNLOAD" | awk -vFS="#" '
  {
         $2 = $2 / 1024;
         printf("DOWNLOAD: %s %d KB\n", $1, $2);
  }
'
  sleep 1
       done
```

Z těchto jsem poté generoval výsledné grafy, které poskytují přehlednější informaci o chování spoje v daných podmínkách. K měření síly signálu jsem u systému Windows XP použil program NetSrumbler, který sice není konstruován pro měření standardu 802.11n avšak sílu signálu v pásmu 2,4 GHz dokáže spolehlivě určit. U stanice s operačním systémem Debian jsem sílu signálu určil užitím základního příkazu „`iwlist wlan0 scan`“.

Ke generování provozu jsem na PC stanici vytvořil 80GB soubor, který postačil ke generování datového provozu po celou dobu měření. Jako protokol pro měření downloadu dat jsem použil http a pro měření uploadu protokol SFTP.

U jednotlivých testů jsem dbal především na stejné vzdálenosti a prostředí, ve kterém se rádiové části nachází, abych minimalizoval chybu měření vzniklou různými vzdálenostmi mezi rádiovými prvky.

Tato zpráva o měření pomáhá čtenářovi představit si prostředí, ve kterém měření proběhlo, ozřejmit si další aspekty, které do měření zasahovali a vytvořit si vlastní pohled na danou problematiku.




*Obrázek 19: Vyzařovací charakteristiky všesměrových antén v notebooku*

# 7 Standard 802.11n v praxi

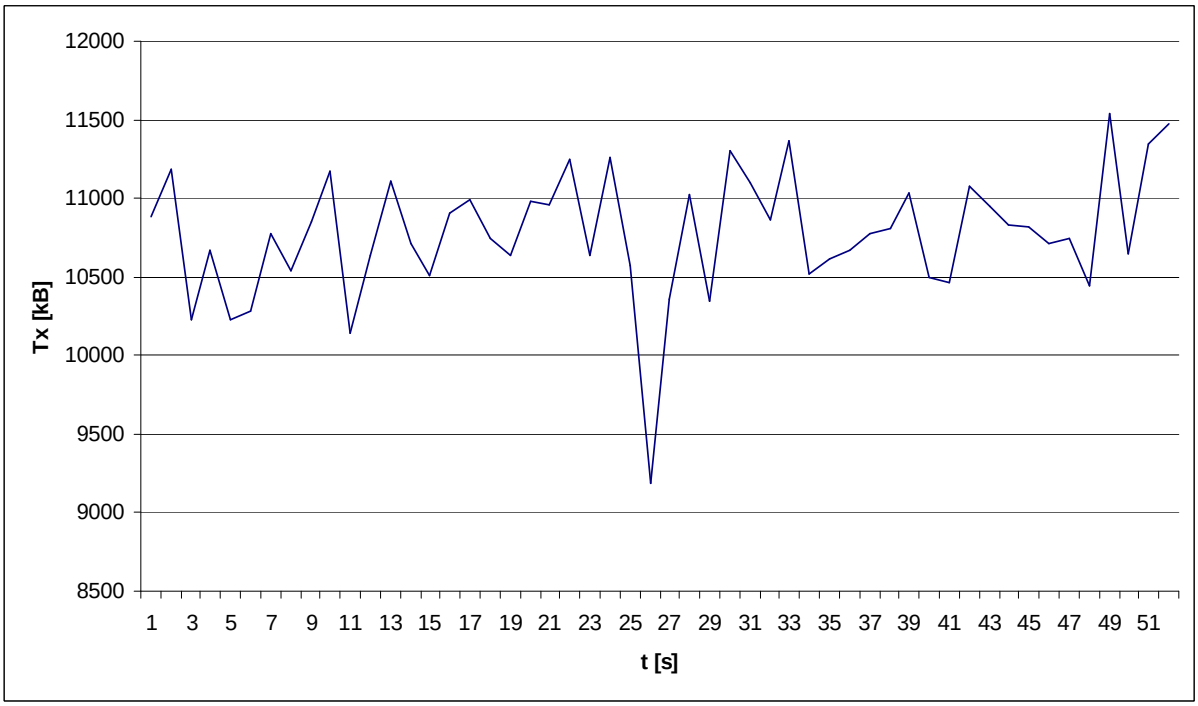
## 7.1 Mód 802.11n only - klient D-Link DWA-643

Měření chování standardu 802.11n jsem provedl v několika fázích a pro několik vzdáleností. V první fázi jsem měření provedl pro vzdálenosti 2 metry, 5 metrů, a jako překážky jsem použil cihlovou zeď a betonový strop obytného domu v přibližně stejných vzdálenostech.

Pro následující čtyři testy jsem přístupový bod DIR-655 nastavil do módu „802.11n only“ a jako klientské zařízení bylo použito DWA-643 s automatickým nastavením rychlosti podle okolních podmínek, ve kterých byly testy prováděny. Po celou dobu měření klientské zařízení signalizovalo připojení o rychlosti 300 Mbit/s.

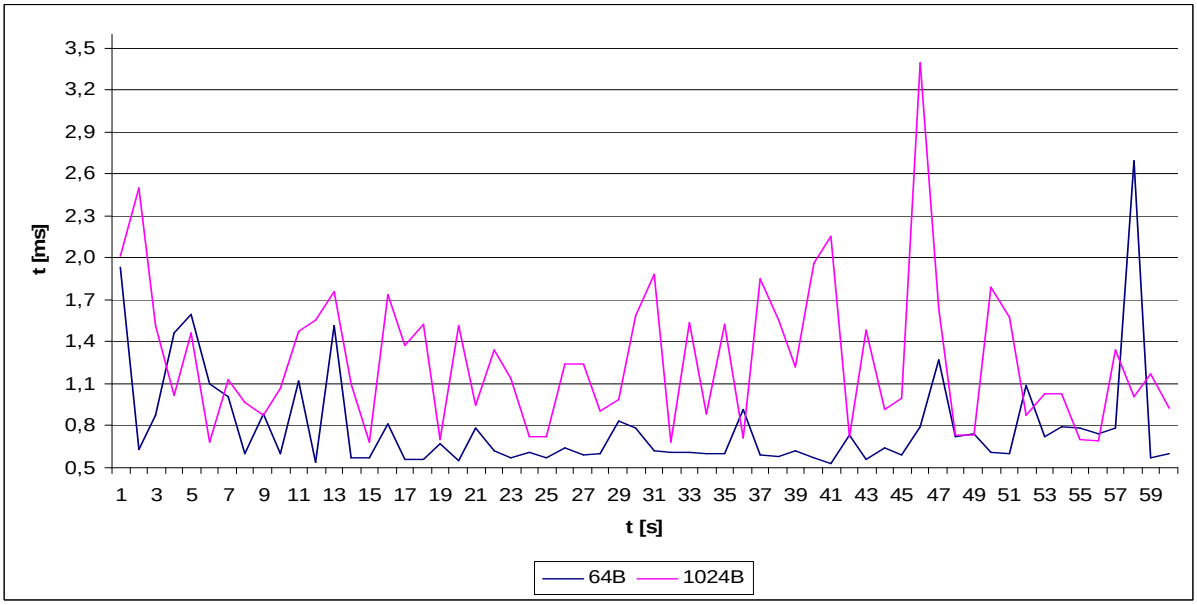
### 7.1.1 Test ve vzdálenosti 2 metry

Následující graf vykresluje chování propustnosti bezdrátového spoje vytvořeného na standardu 802.11n v uzavřené místnosti bez překážek ze strany přístupového bodu AP. Z grafu je vidět, že rychlost přenosu je oproti starším standardům z rodiny standardů 802.11 značně větší. Pokud odmyslíme špičky a velké výkyvy rychlosti vzniklé pohybem osob po místnosti můžeme říci, že se standard opravdu přibližuje rychlosti metalické sítě Fast Ethernet, tedy 100 Mbit/s. Z hlediska teoretických předpokladů, se však standard předpokládané rychlosti 300 Mbit/s během přenosu nepřiblížil. Po přezkoumání všech aspektů, které by propustnost bezdrátového spoje mohli oslabit, jsem došel k závěru, že nižší propustnost je způsobena velmi slabými vysílacími a přijímacími anténami integrovanými v klientském zařízení D-Link DWA-643. Síla signálu byla v tomto měření -41 dBm.



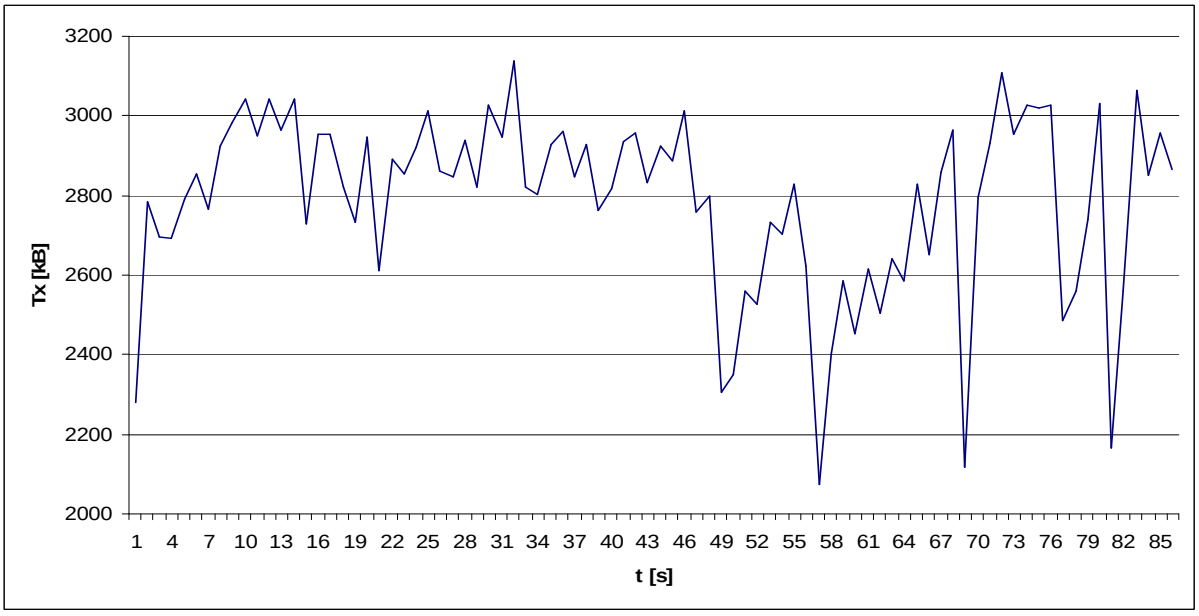

*Obrázek 20: 802.11n test propustnosti AP-klient ve vzdálenosti 2 m*

Grafické znázornění velikostí odezvy v závislosti na čase měření vypovídá o tom, že požadavek na měření velikosti odezvy o velikosti 1024 bajtů je mnohem náročnější na čas než požadavek o velikosti 64 bajtů. V průběhu měření se objevují značné výkyvy, které by se při předpokládané teoretické rychlosti 300 Mbit/s neměly oproti požadavku na odezvu o velikosti 64 B v takové míře projevovat.




*Obrázek 21: 802.11n test odezvy ve vzdálenosti 2 m*

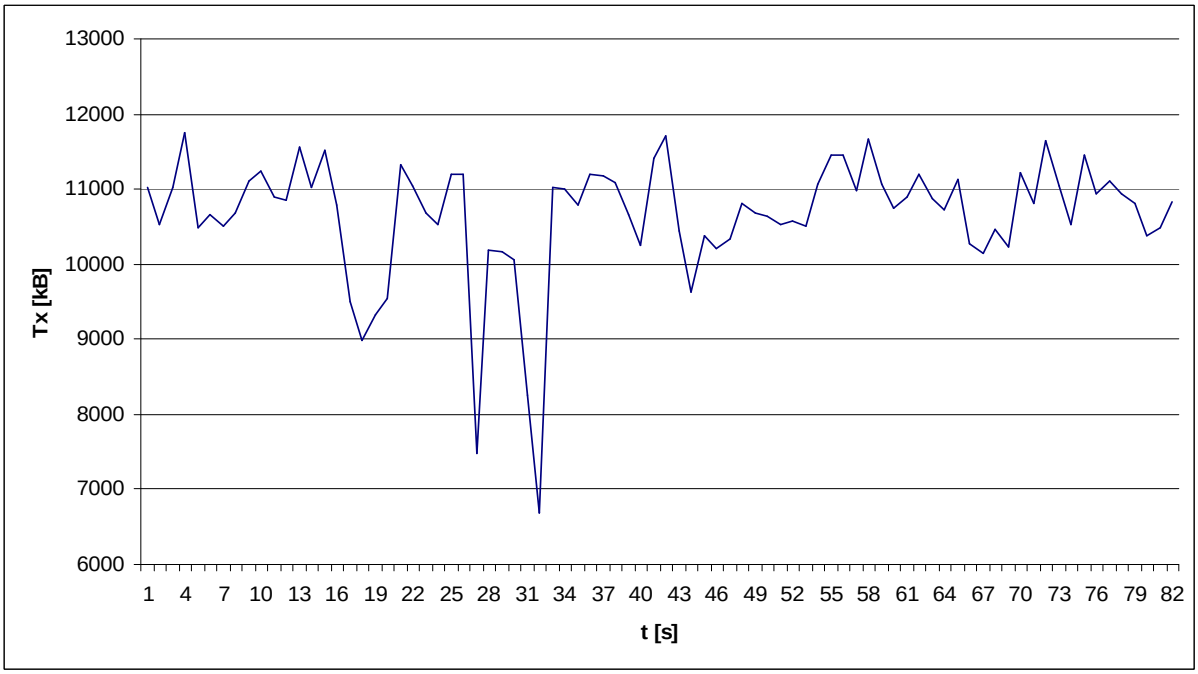
Následující grafické vyhodnocení prezentuje chování propustnosti bezdrátového spoje ze strany klientského zařízení DWA-643. Z grafu je na první pohled vidět značná nestabilita a oproti testu propustnosti ze strany AP veliké omezení datové propustnosti. Důvodem bude použití antén s malým ziskem uvnitř zařízení DWA-643. Signál se uvnitř místnosti chová chaoticky a šíří se převážně díky odrazům od zdí.




*Obrázek 22: 802.11n test propustnosti klient-AP ve vzdálenosti 2m*

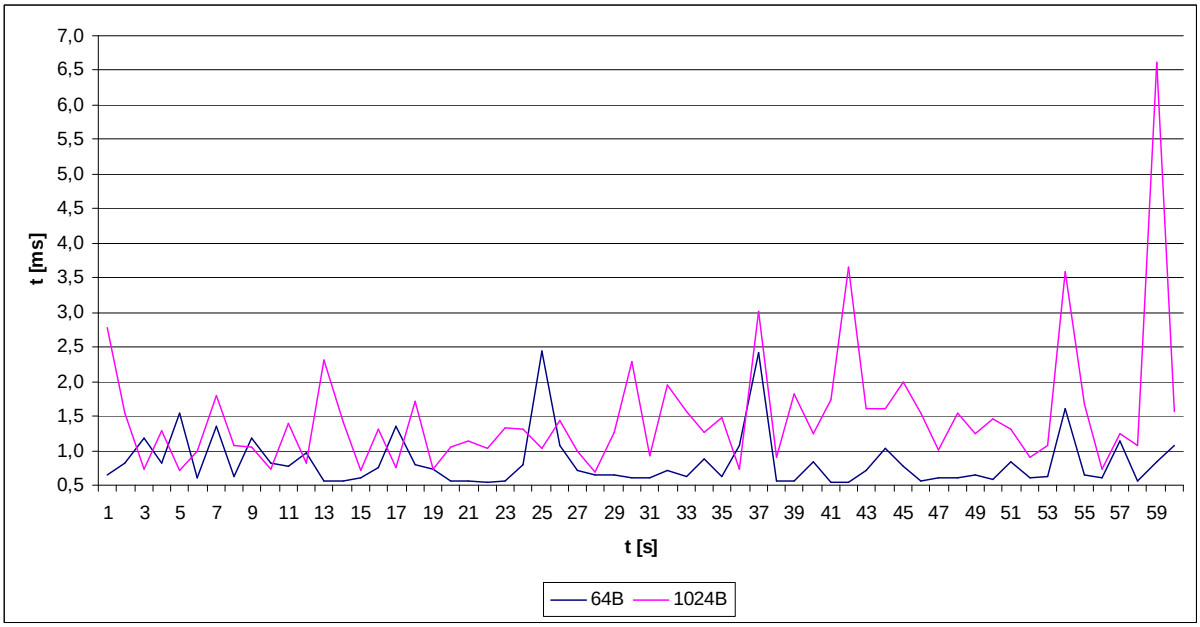
### 7.1.2 Test ve vzdálenosti 5m

Vyhodnocení závislosti propustnosti dat na čase na vzdálenosti 5 metrů vykazuje o málo větší výchylky. Z grafu jsou vidět i špičkové hodnoty o velmi nízké propustnosti, způsobené pravděpodobně pohybem v místnosti nebo rušením jiného rádiového zařízení pracujícím na stejné frekvenci. Pro toto měření byla síla signálu změřena na -45 dBm.



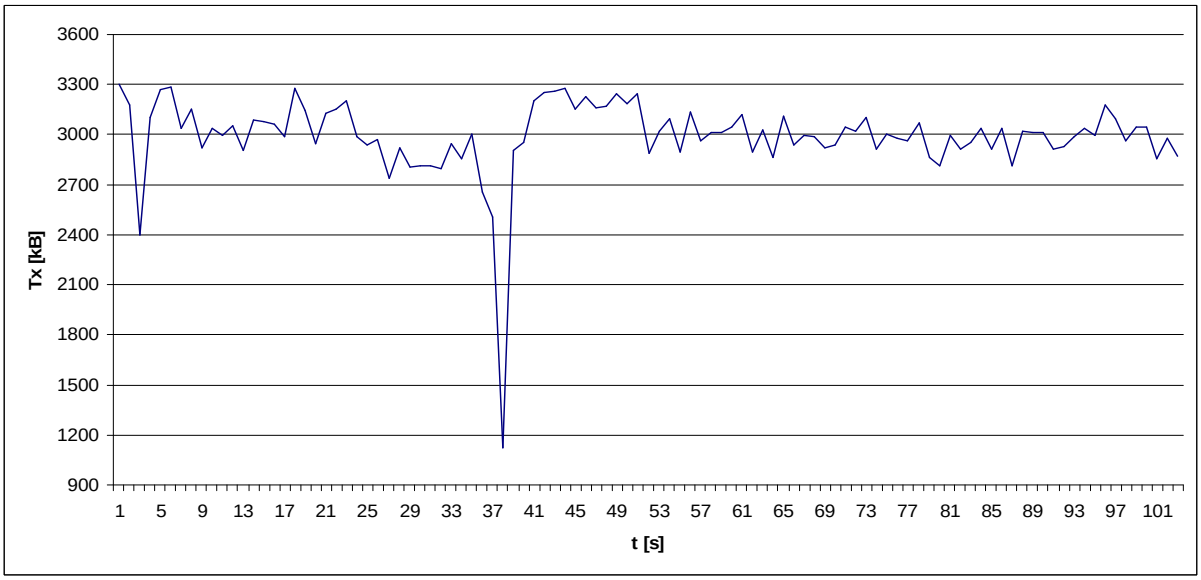

*Obrázek 23: 802.11n test propustnosti AP-klient ve vzdálenosti 5m*

Jak je vidět z grafu, odezva na větší vzdálenosti se uvnitř místnosti oproti propustnosti chová přibližně stejně jako u testu na vzdálenosti 2 metry. Až na špičkové hodnoty, které jsou způsobeny rušením, je křivka téměř stejná.




*Obrázek 24: 802.11n test odezvy ve vzdálenosti 5 m*

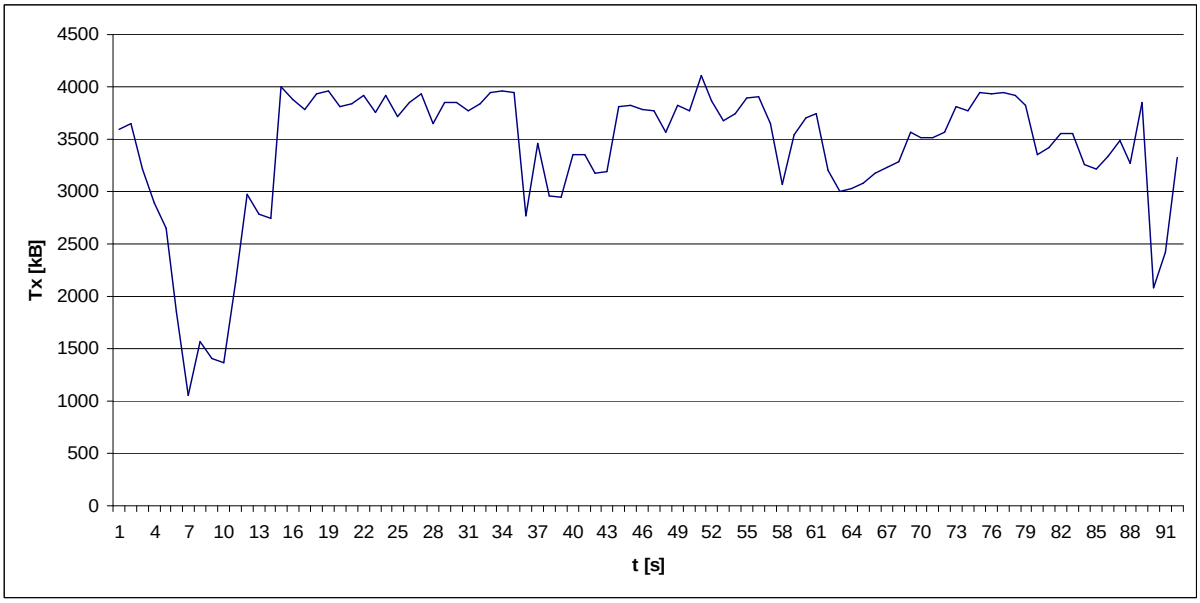
Test propustnosti ze strany klientského zařízení DWA-643 vykazuje hodnoty přibližně 3 MB/s. Kromě na první pohled viditelné špičkové hodnoty se chování velikosti propustnosti ukazuje být na větší vzdálenosti více stabilní, než tomu bylo na vzdálenosti 2 m od přístupového bodu. Způsobeno to bude pravděpodobně tím, že při větší vzdálenosti se signál šíří lépe a nevyužívá při svém šíření tolik odrazů jako u velmi malých vzdáleností.




*Obrázek 25: 802.11n test propustnosti klient-AP ve vzdálenosti 5 m*

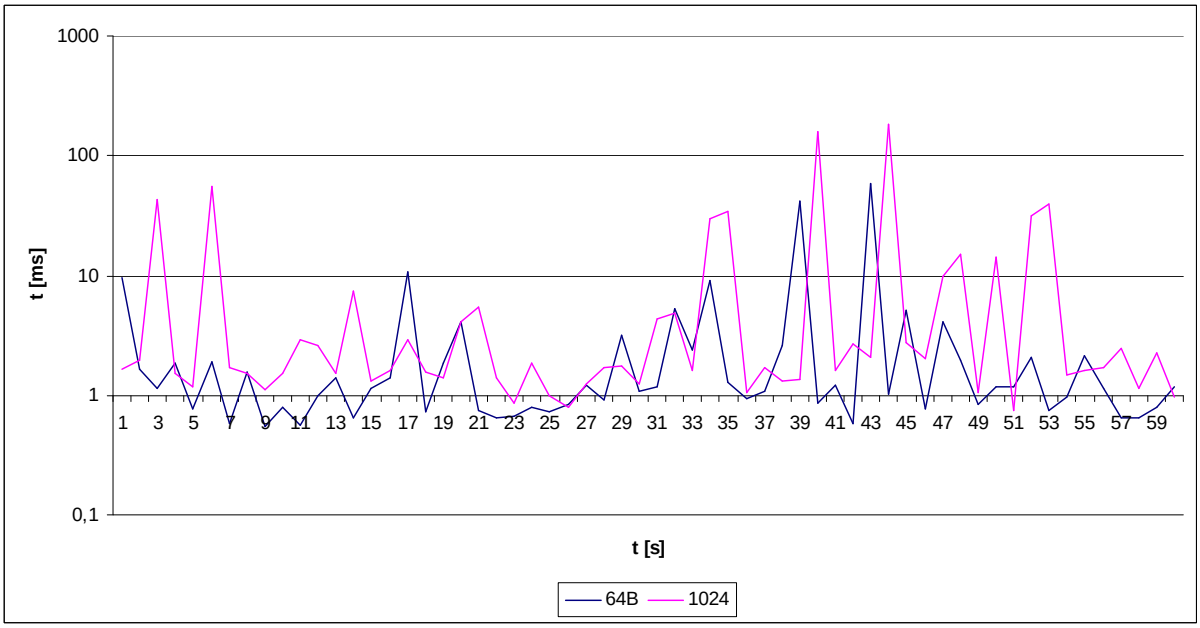
### 7.1.3 Test skrz cihlovou zeď

V tomto testu jsem zvolil jako překážku cihlovou zeď. V testu propustnosti ze strany přístupového bodu AP je signál, jak je vidět z grafu, překážkou značně oslaben. Propustnost se drží v hodnotách od 3 MB/s do 4 MB/s. Opět se objevují špičkové hodnoty a to převážně na začátku při sestavování spojení. Budou způsobeny pravděpodobně tím, že překážka představuje pro šíření signálu značný problém. Síla signálu se snížila na -52 dBm.



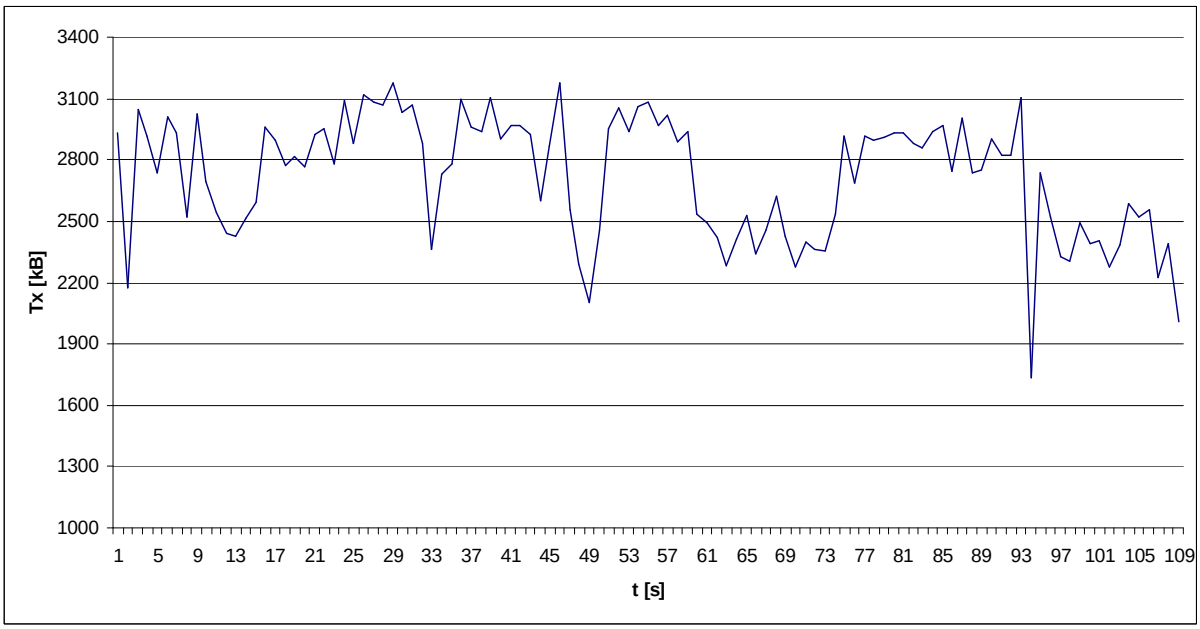

*Obrázek 26: 802.11n test propustnosti AP-klient skrz cihlovou překážku*

Graf odezvy prezentuje značně velké výchylky. Některé hodnoty dokonce přesahují hodnotu 100 ms. Signál má s překážkou větší problémy a při testu odezvy, kdy musí pro každou hodnotu sestavovat spojení je velikost odezvy v závislosti na čase měření dosti chaotická.




*Obrázek 27: 802.11n test odezvy skrz cihlovou překážku*

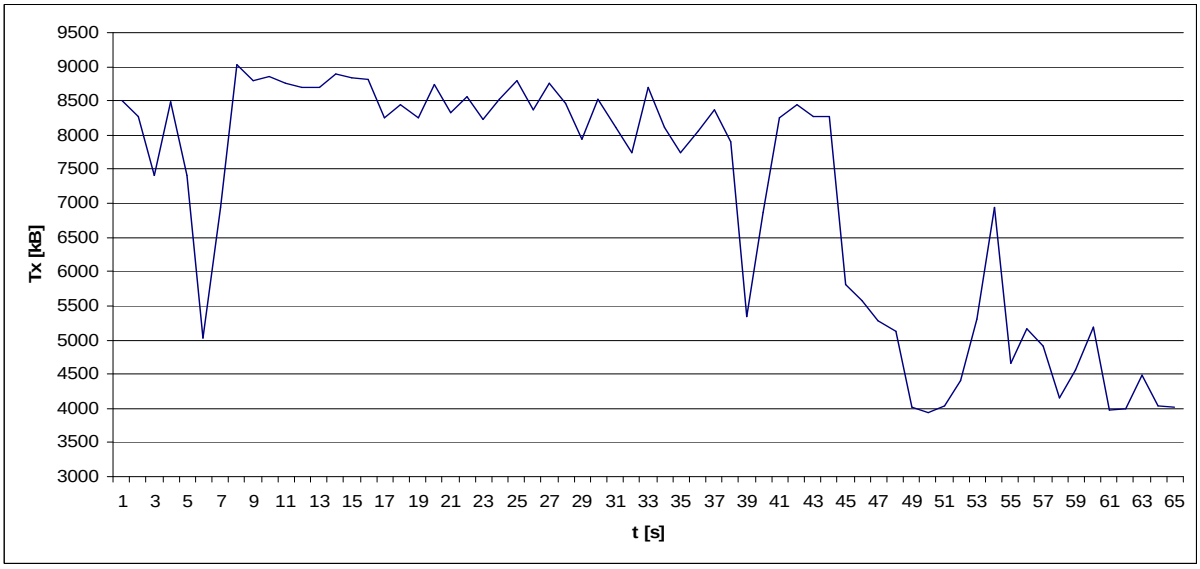
Na grafu testu propustnosti ze strany klientského zařízení DWA-643 jsou jasně vidět problémy s plynulostí průběhu přenosové rychlosti. Rychlost kolísá mezi hodnotami 2 a 3 MB/s. Po celou dobu měření se však spojení ani jednou nerozpadlo.




*Obrázek 28: 802.11n test propustnosti klient-AP skrz cihlovou překážku*

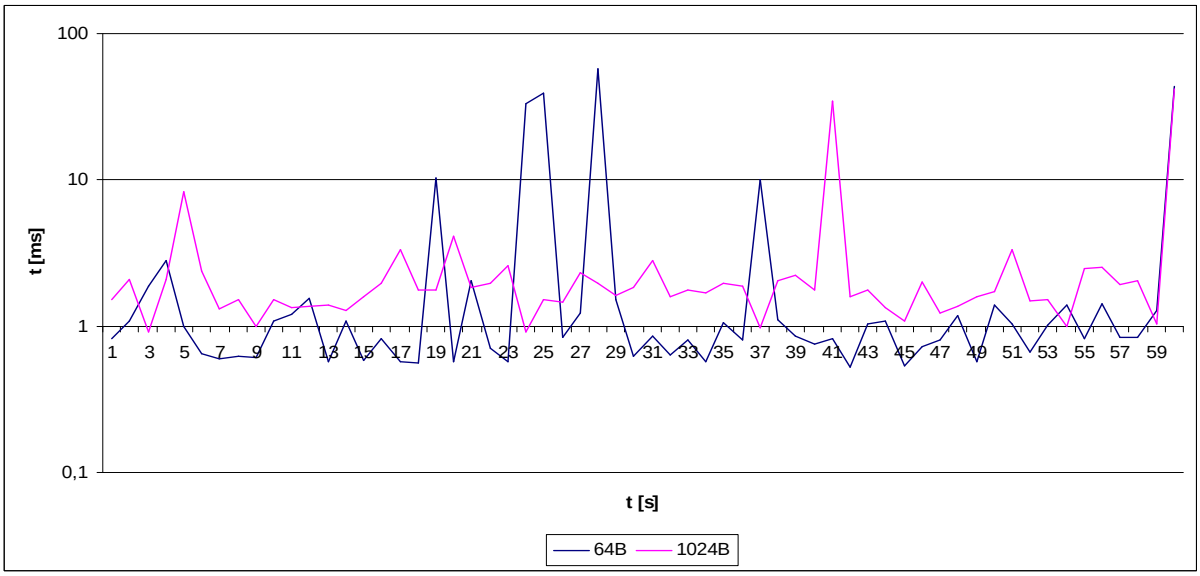
### 7.1.4 Test skrz betonový strop

V tomto měření jsem jako překážku pro rádiový signál použil betonový strop. V první části měření jsem proměřil chování datové propustnosti ve směru od AP ke klientskému zařízení v závislosti na čase měření. Velikost datové propustnosti se ze začátku přibližuje hodnotě 9 MB/s ovšem z grafu jsou vidět značné výchylky způsobené překážkou. Pokles je vidět i na hodnotě síly signálu, která byla změřena pomocí programu NetStrumbler -58 dBm.



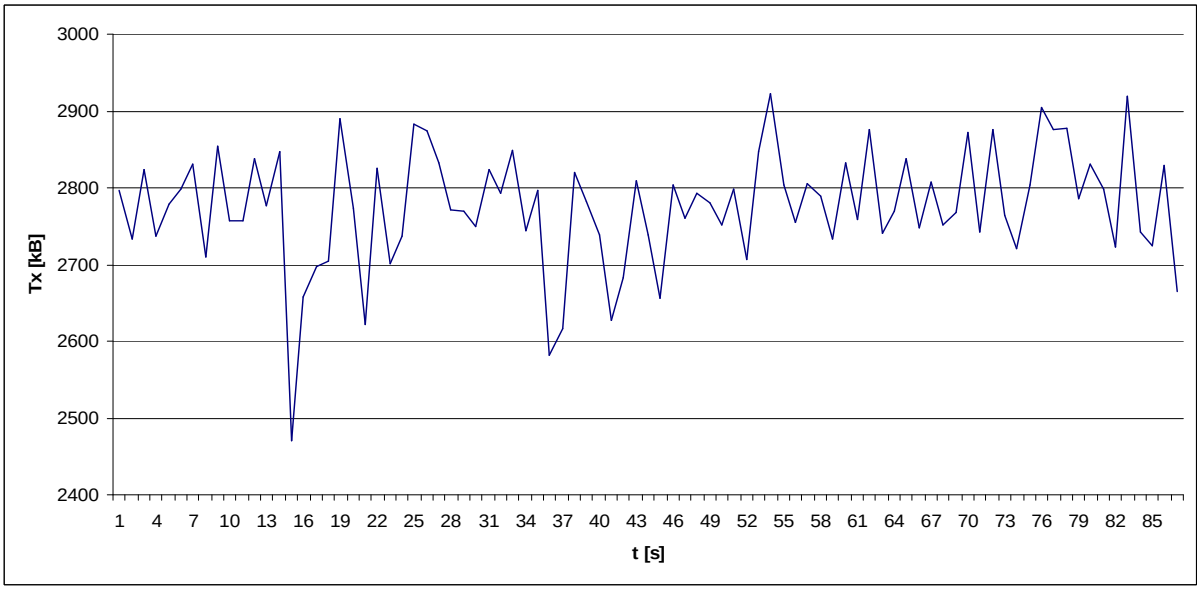

*Obrázek 29: 802.11n test propustnosti AP-klient skrz betonovou překážku*

Při měření velikosti odezvy na klientské zařízení přes betonovou překážku jsem zjistil veliké rozdíly mezi hodnotami. U 64 bajtového dotazu se hodnota až na vyjímky špiček pohybovala kolem jedné milisekundy. U kilobajtového dotazu jsou patrné větší rozdíly. Hodnota odezvy se pohybuje mezi jednou a deseti milisekundami. Některé špičkové hodnoty dosahují hodnoty až 100 ms.




*Obrázek 30: 802.11n test odezvy skrz betonovou překážku*

Z výsledné křivky z testu downloadu opačným směrem jsou vidět rozdíly v hodnotách. Průměrná hodnota se pohybuje mezi hodnotami 2700 kB/s a 2800 kB/s. V porovnání s testem downloadu s cihlovou překážkou se signál chová lépe, betonová překážka pro něj tvoří menší problém. V tuto chvíli se značně uplatňuje technologie „spatial multiplexing“ a „beamforming“, kde si signál snaží najít více cest za předpokladu, že u cíle budou jednotlivé složky signálu fázově posunuty, aby nedošlo k chybám. Křivka průběhu downloadu je výrazně stabilnější než v případě s cihlovou překážkou.




*Obrázek 31: 802.11n test propustnosti klient-AP skrz betonovou překážku*

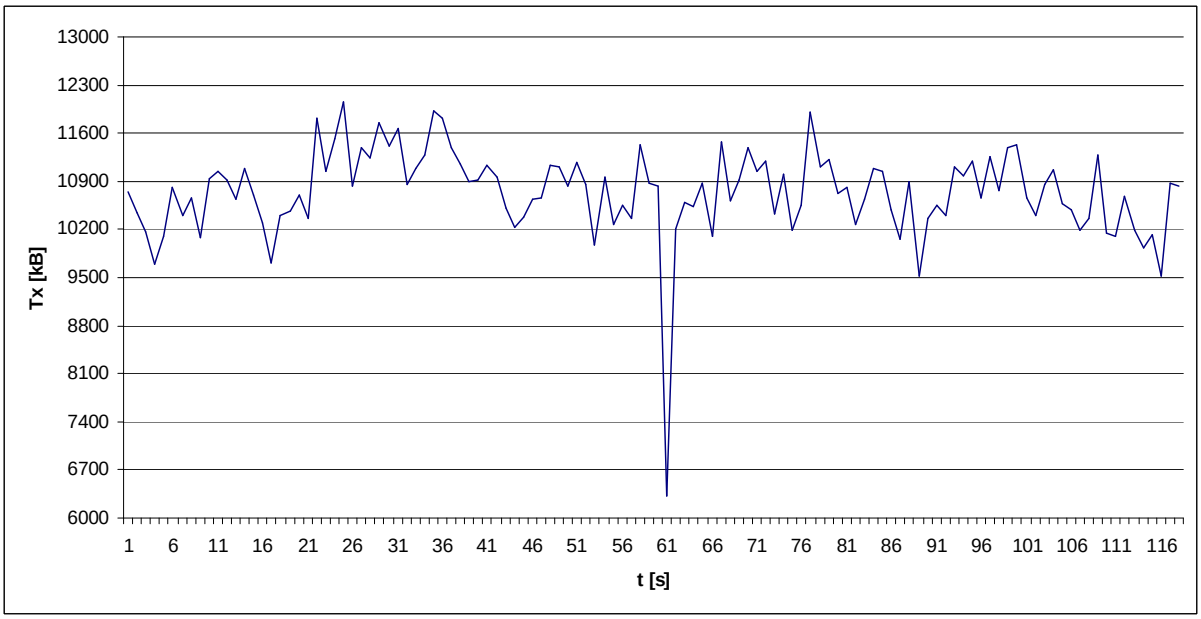
## 7.2 Mód 802.11n, 802.11g mixed - klient D-Link DWA-643

V tomto testu jsem přístupový bod D-link DIR-655 nastavil do módu “802.11n, 802.11g mixed”, ve kterém by AP měla schvalovat požadavky na asociace od všech zařízení žádajících připojení, které podporují standard 802.11n nebo 802.11g. Oba standardy jsou dosti odlišné. Jak bylo popsáno v kapitole o zpětné kompatibilitě standard 802.11n je plně kompatibilní se staršími standardy rodiny 802.11 a to 802.11g a 802.11b. Zajišťují to techniky „mixed mode” neboli sdružený mód, který spočívá v tom, že vysílaný signál je možné dekódovat staršími i novým standardem 802.11n. Kromě této metody je zpětná kompatibilita zajištěna mechanismem „CTS-to-self“, který však pro standard představuje jistá omezení.

V tomto testu jsem jako klientské zařízení opět použil D-Link DWA-643 v módu 802.11n a zjišťoval, zda vlivy rušní okolních zařízení pracujících na standardu 802.11g budou mít zásadnější vliv na přenos.

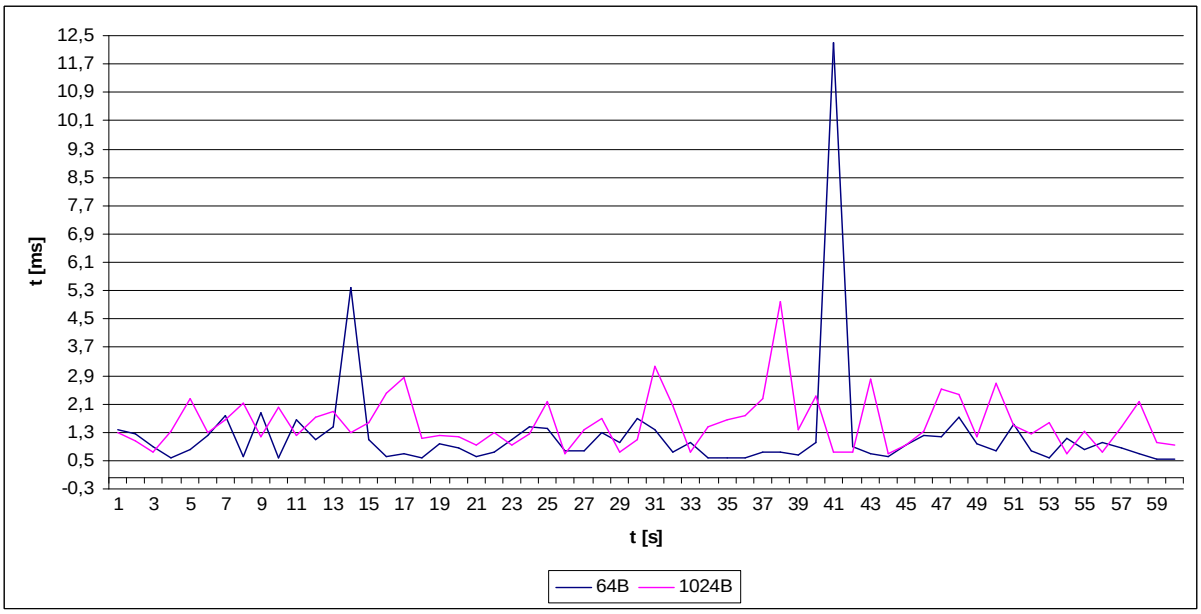
### 7.2.1 Test ve vzdálenosti 2 metry

Následující graf prezentuje chování sestaveného bezdrátového spojení mezi přístupovým bodem a klientským zařízením ve vzdálenosti 2 metry. Průběh downloadu je přibližně stejně stabilní jako v případě když byl přístupový bod v módu 802.11n only. Objevují se i špičkové hodnoty, které budou způsobeny rušením jiného rádiového zařízení pracujícím na stejné frekvenci. Síla signálu v tomto měření, změřená pomocí program NetStumbler, se pohybovala kolem hodnoty -36 dBm. To znamená, že SNR je 64 dB.




*Obrázek 32: 802.11n test propustnosti AP-klient ve vzdálenosti 2 m*

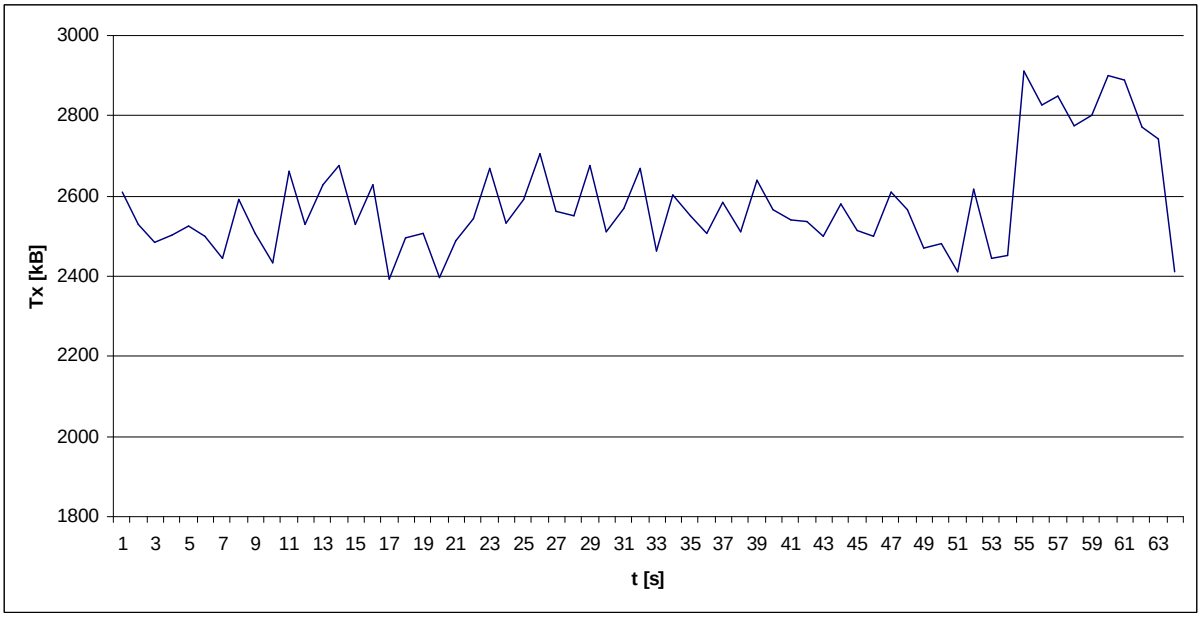
Test odezvy vykazuje téměř stejné hodnoty jako v prvním testu. 64 B požadavek má odezvu znatelně menší než 1024 B, avšak objevují se i špičkové hodnoty. Průměrná hodnota 1024 B požadavku se pohybuje kolem honoty 1,3 ms. I když u některých zařízení se při příliš malých vzdáleností objevuje značná chybovost v přenosu někdy i neasociovatelnost, v tomto případě test latence nevykazuje žádné abnormality, které by mohly mít negativní dopad na propustnost datového toku.




*Obrázek 33: 802.11n test odezvy ve vzdálenosti 2 m*

V testu propustnosti ve směru klient – AP se objevují změny oproti testu, kdy bylo AP v módu 802.11n. Křivka propustnosti se chová stabilněji, avšak průměrná hodnota se snížila na hodnotu 2600 kB/s. Způsobeno to může být tím, že klientské zařízení DWA-643 má

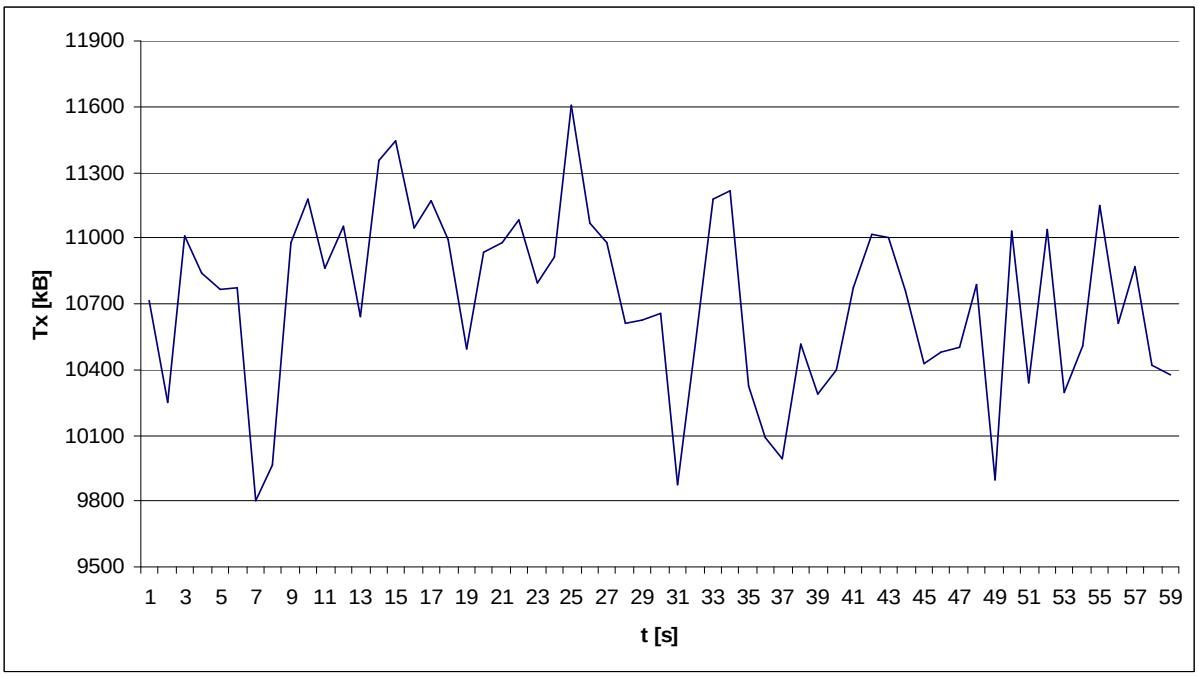
v módu 802.11n/g větší problém s překonáváním rušení od okolních zařízení a tudíž i s uploadem dat.




*Obrázek 34: 802.11n test propustnosti klient-AP ve vzdálenosti 2 m*

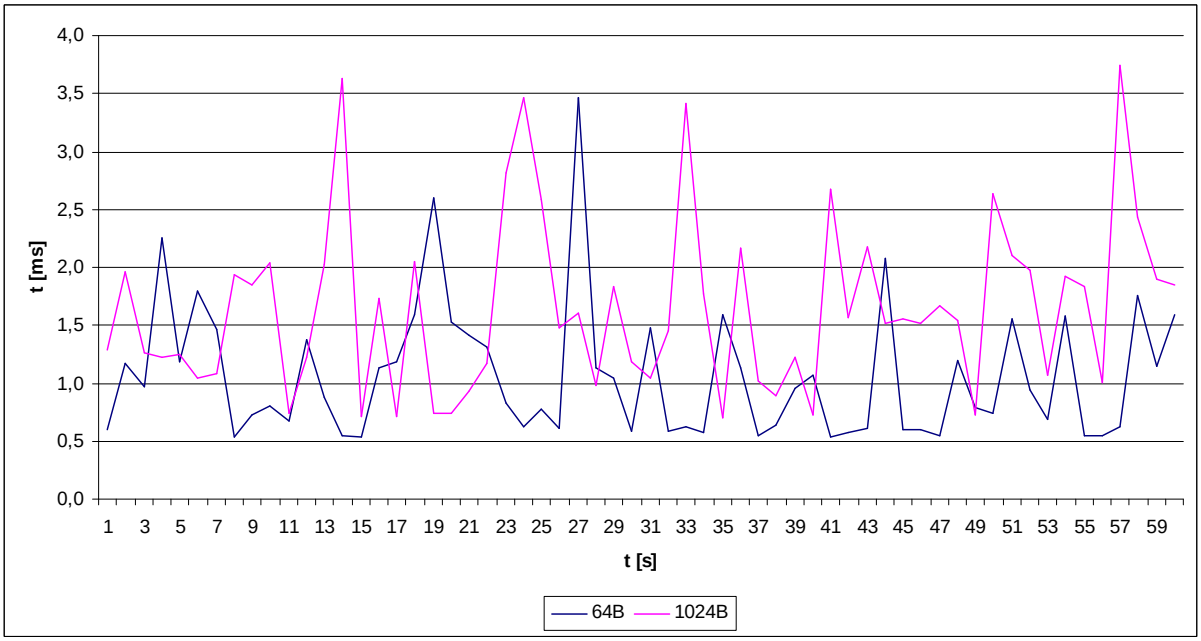
### 7.2.2 Test ve vzdálenosti 5 metrů

V tomto testu se průměrná hodnota oproti předchozímu testu zvýšila zhruba o několik desítek kB avšak propustnost je velice nestabilní, objevují se veliké rozdíly mezi sousedními hodnotami. Lze proto říci, že v homogenním prostředí se v uzavřené místnosti se zvyšující vzdáleností v módu 802.11n/g objevují větší problémy s přenosem. Síla signálu byla -46 dBm a odstup šumu SNR 54 dB.



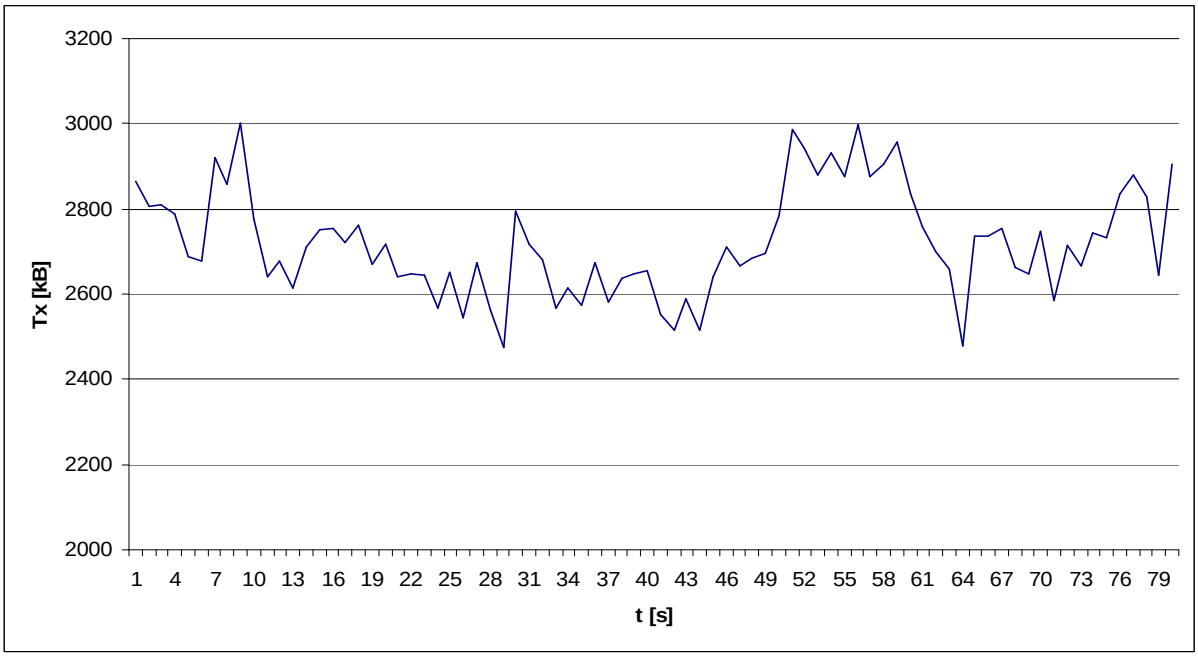

*Obrázek 35: 802.11n test propustnosti AP-klient ve vzdálenosti 5 m*

Test odezvy představuje v tomto měření velmi zajímavé hodnoty. Hodnoty odezvy požadavku o velikosti 64 B a 1024 B jsou velmi podobné, v některých místech téměř stejné. Rovněž špičkové hodnoty u obou požadavků se často podobají. Hodnoty jsou však o dost vyšší a více chaotické než v minulých případech. Proto je z tohoto měření zřejmé, že zvyšující se vzdálenost má velmi negativní dopad na propustnost. Veliký problém představuje takovéto chování odezvy pro přenosy citlivé na zpoždění např. hlasová nebo video komunikace.




*Obrázek 36: 802.11n test odezvy ve vzdálenosti 5 m*

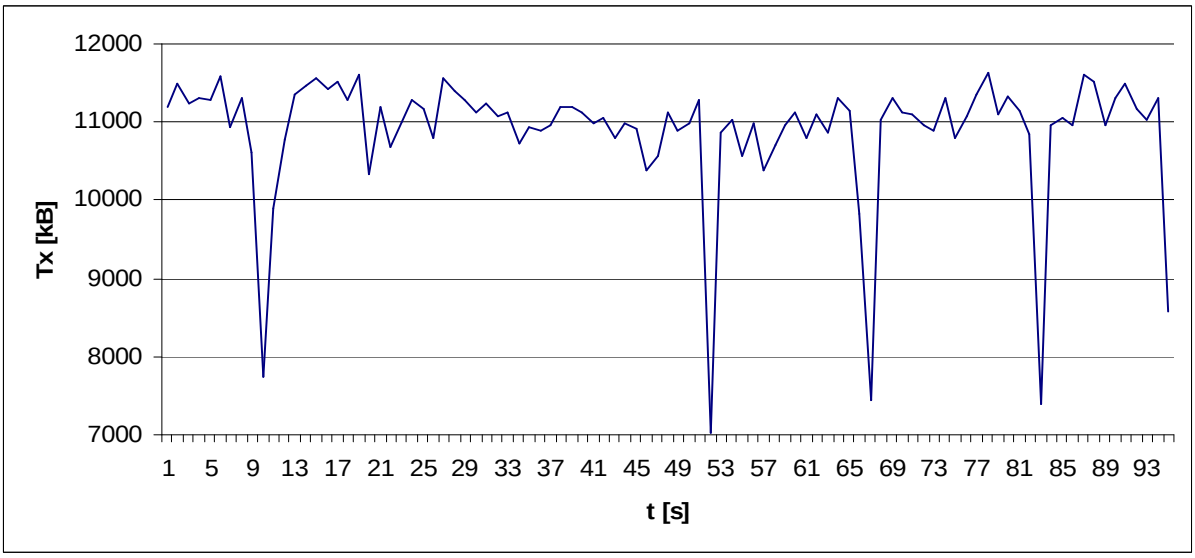
V testu downloadu v opačném směru vychází průměrná hodnota o málo vyšší, než tomu bylo u měření na vzdálenost 2 metry, avšak oproti tomuto měření se křivka chování propustnosti v závislosti na čase u kratší vzdálenosti chová méně chaoticky.




*Obrázek 37: 802.11n test propustnosti klient-AP ve vzdálenosti 5 m*

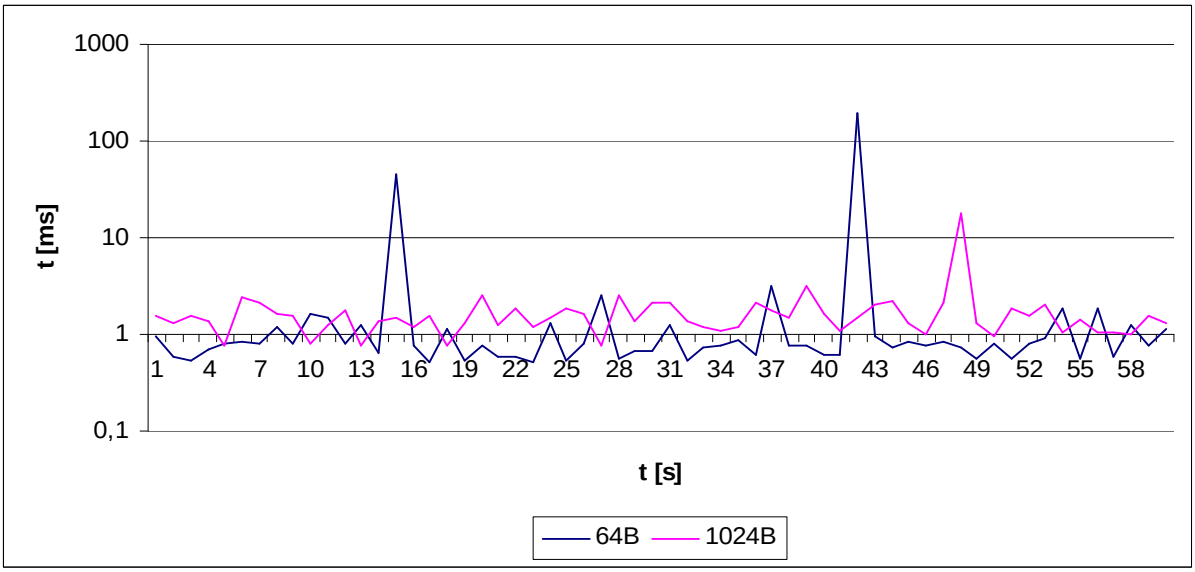
### 7.2.3 Test skrz cihlovou zeď

Následující test byl prováděn opět přes cihlovou překážku. Propustnost ve směru AP-klient se chová velice stabilně. Průměrná hodnota po aproximaci vychází přibližně 11 MB/s. Z grafu jsou však viditelné časté špičkové hodnoty, které jsou zcela jistě způsobeny působením cizích rádiových zařízení pracujících na stejné frekvenci. Důvodem však může být i problém s hledáním vhodné cesty signálu. Program NetStumbler ukazoval sílu signálu -46 dBm, což je stejná hodnota jako v předchozím měření.



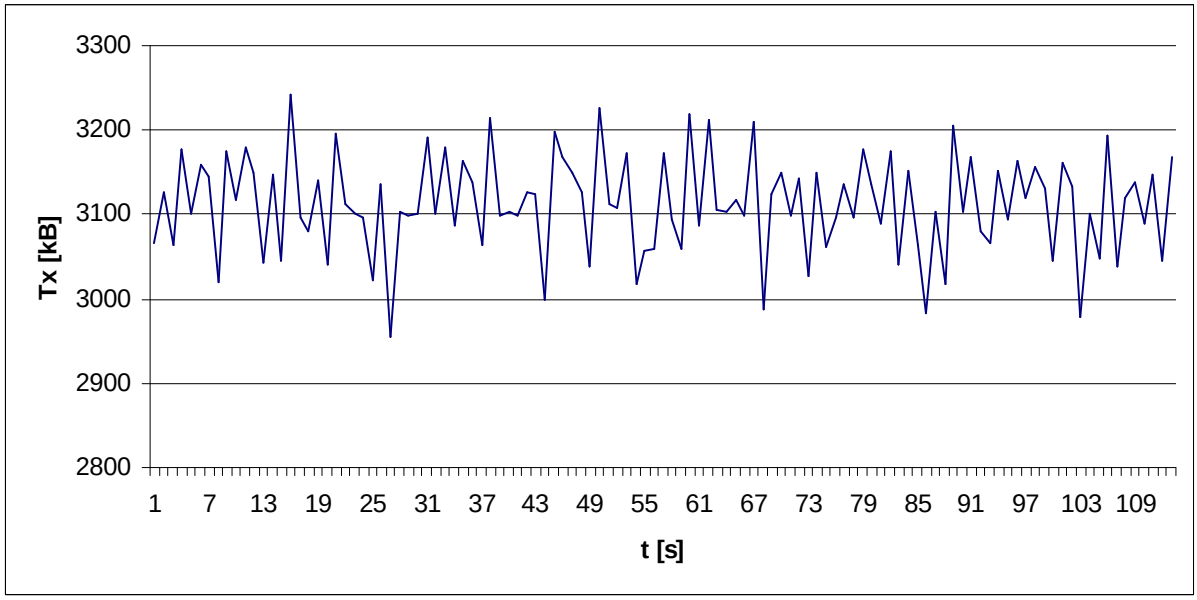

*Obrázek 38: 802.11n test propustnosti AP-klient skrz cihlovou překážku*

Odezva se v tomto měření chovala nestabilně. Dotaz o velikosti 64 B měl dobu odezvy většinou pod 1ms, objevují se taky hodnoty kolem 200 ms a 100 ms. 1024 B dotaz má rovněž nestabilní průběh, avšak špičkové hodnoty se v měření neprojevily. Velikost časové odezvy se pohybovala mezi kolem 2 ms. Velikost časové periody je ovlivněna překážkou.




*Obrázek 39: 802.11n test odezvy skrz cihlovou překážku*

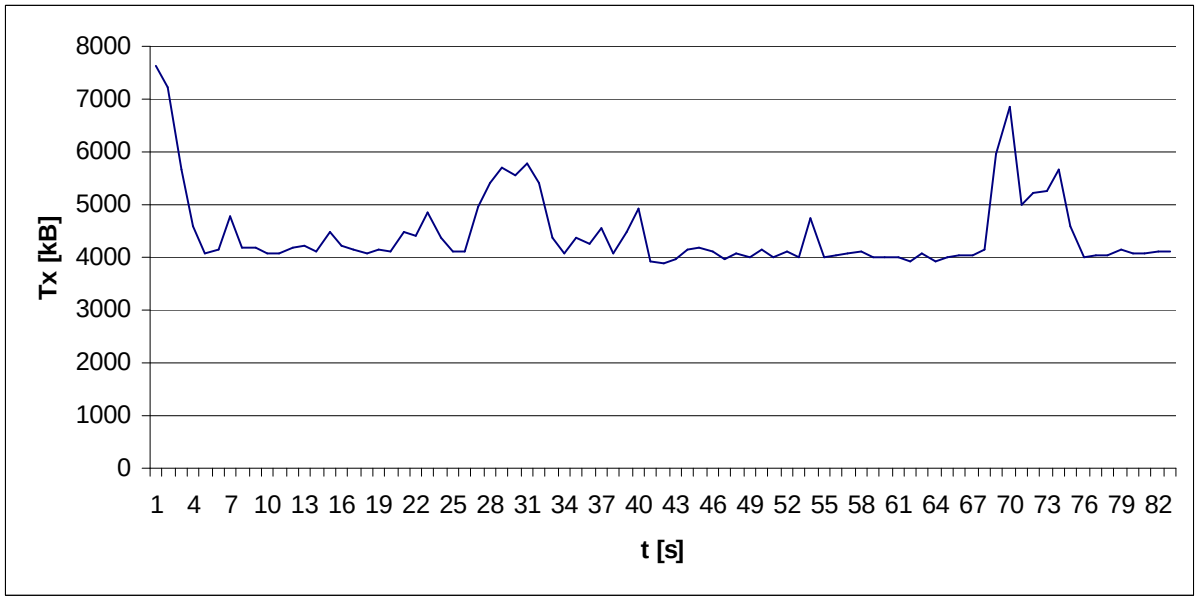
Download ve směru klient-AP vykazuje stabilnější hodnoty v průběhu měření, než tomu bylo v módu 802.11n, avšak průměrná rychlost stahování se mírně snížila a pohybuje se kolem hodnoty 3 MB/s.




*Obrázek 40: 802.11n test propustnosti klient-AP skrz cihlovou překážku*

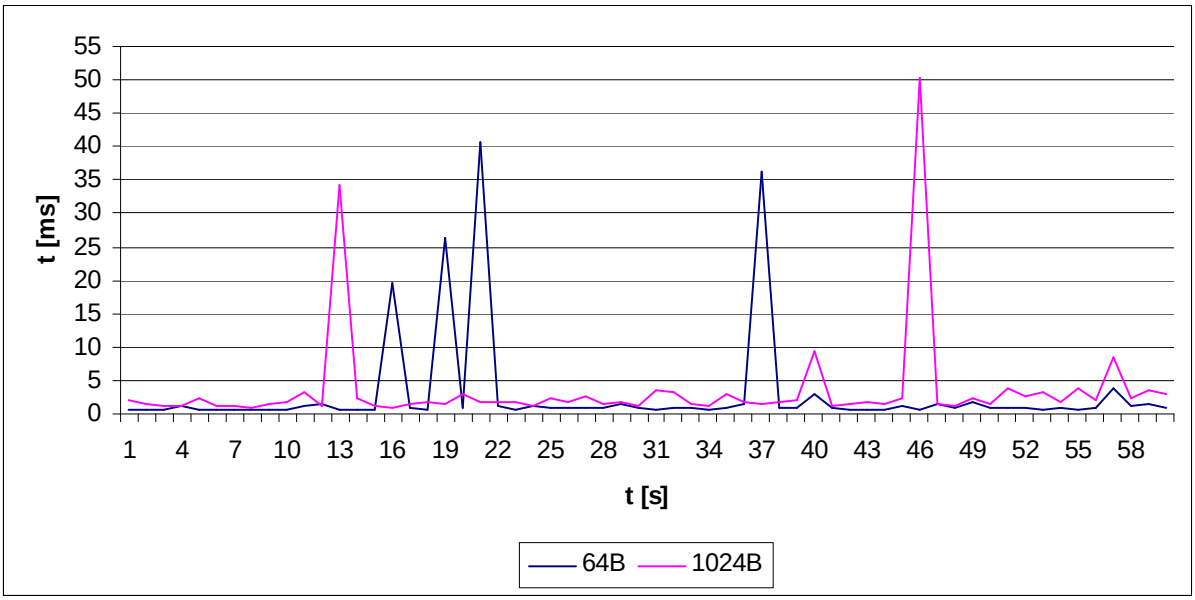
### 7.2.4 Test skrz betonový strop

V tomto testu jsem opět použil jako překážku betonový strop obytného domu. V testu byly hodnoty datové propustnosti výrazně nižší, než tomu bylo v předchozím případě. Velikost propustnosti ve směru AP-klient se pohybovala v průměru kolem hodnoty 4,5 MB/s, hodnota během celého měření neklesla pod hodnotu 4 MB/s. Hodnota signálu byla stabilně -57 dBm, což znamená výrazný pokles způsobený překážkou.



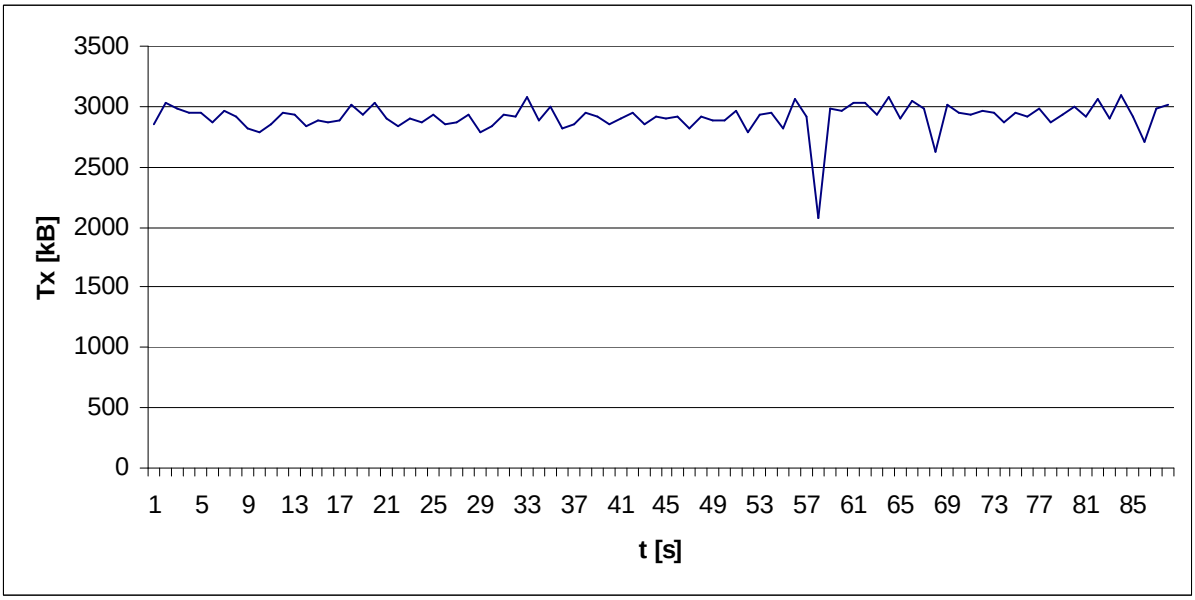

*Obrázek 41: 802.11n test propustnosti AP-klient skrz betonovou překážku*

V průběhu měření odezvy se objevovali skákavé hodnoty, u 64 B pingu v zásadě mezi 0,5 ms a 3 ms. Dotaz o velikosti 1024 B představoval pro spoj větší problém, hodnoty kolísaly od 1 ms do 5 ms. V obou měřeních se vyskytovali vysoké špičkové hodnoty jdoucí řádově až do desítek milisekund.




*Obrázek 42: 802.11n test odezvy skrz betonovou překážku*

V testu propustnosti ve směru klient-AP vycházeli hodnoty oproti testu v módu 802.11n only překvapivě vysoko a stabilně. Hodnota se celou dobu držela na hodnotě 3 MB/s. Důvodem bude pravděpodobně fakt, že v předešlém měření při nastavení přístupového bodu AP do módu 802.11only bylo v blízkosti aktivní rádiové zařízení které ovlivnilo linearitu průběhu přenosové rychlosti a standard 802.11n měl s takovouto překážkou větší problém a to i za využití standardem definovaných technik, jako jsou „spatial multiplexing“ a „beamforming“.



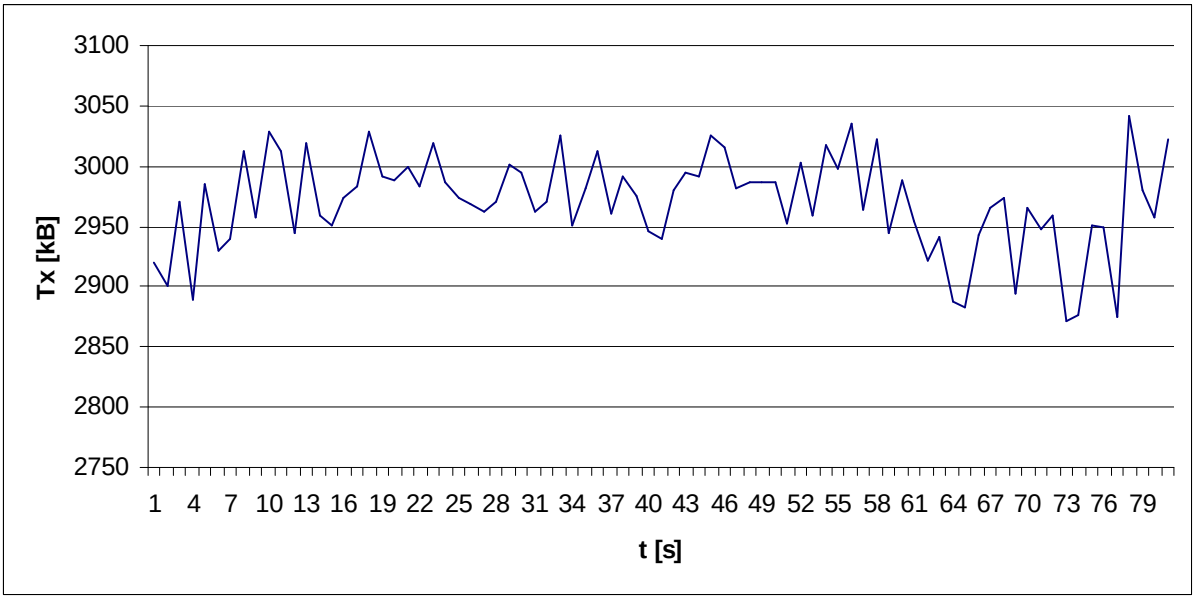

*Obrázek 43: 802.11n test propustnosti klient-AP skrz betonovou překážku*

## 7.3 Mód 802.11n, 802.11g mixed - klient Broadcom BCM4318bg

V následujících testech jsem jako klientské zařízení použil Broadcom BCM4318bg v podobě miniPCI karty integrované v notebooku Hewlett Packard Compaq nx6110. Ke kartě byly připojeny dvě všesměrové antény rovněž integrované v notebooku. Během měření byla rychlost přenosu nastavena na maximální použitelnou rychlost, tedy 54 Mbit/s. Jako přístupový bod byl použit D-Link DIR-655 nastavený v módu 802.11n/g mixed. Testy byly prováděny stejně jako v minulých případech na vzdálenost 2 m, 5 m, skrz cihlovou a betonovou překážku. Následující testy slouží pro porovnání standardů 802.11n a 802.11g z hlediska stability datového toku a schopnosti bránit se rušivým vlivům okolních radiových zařízení.

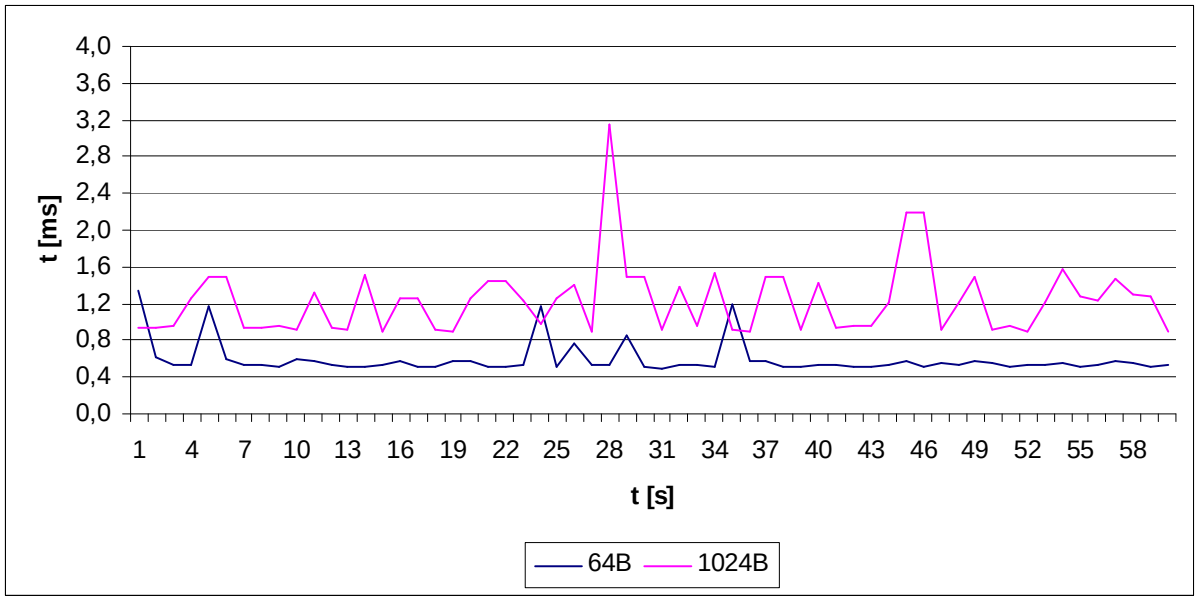
### 7.3.1 Test ve vzdálenosti 2 metrů

V prvním provedeném měření s klientským zařízením pracujícím na standardu 802.11g je patrný hlavní rozdíl mezi oběma testovanými standardy a to rozdíl v rychlosti. Ta se relativně stabilně drží u hodnoty 3 MB/s. Oproti klientskému zařízení DWA-643 se přenos chová více stabilně a sousední hodnoty se liší mnohem méně než u standardu 802.11n. Je patrný i úbytek špiček. Ty se objevují v grafu jen zřídka a mají mnohem menší velikost. Síla signálu byla změřena na -28 dBm, což je ve srovnání se standardem 802.11n na stejné vzdálenosti mnohem vyšší hodnota. Velikost šumu byla -98 dBm což znamená, že velikost odsupu signálu a šumu SNR byla 70 dB.



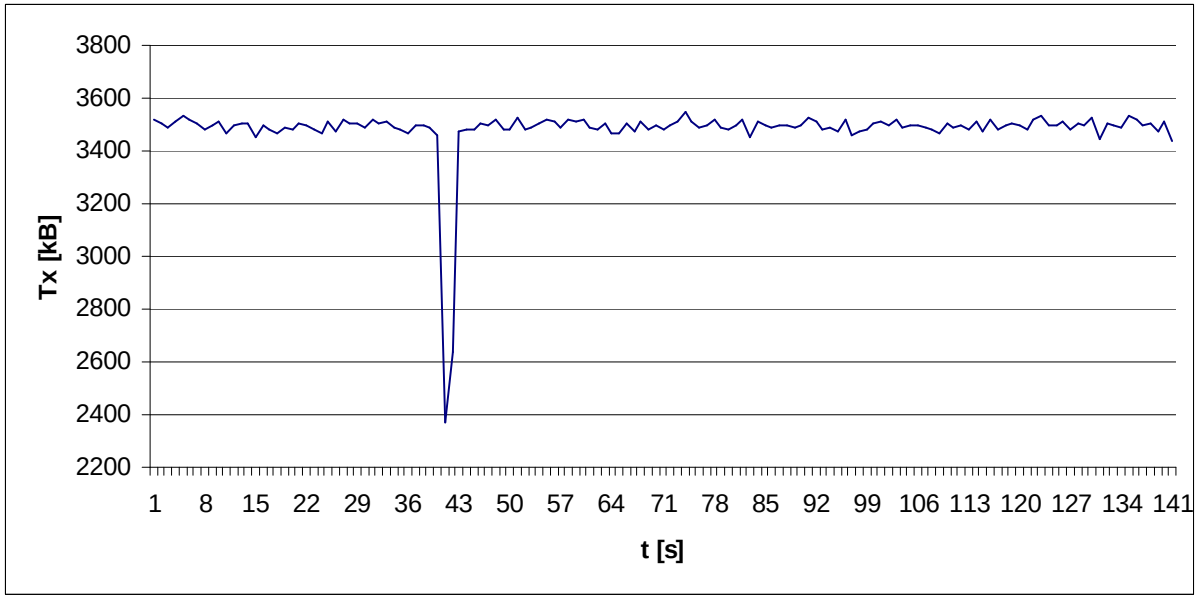

*Obrázek 44: 802.11g test propustnosti AP-klient ve vzdálenosti 2 m*

Test odezvy ve vzdálenosti dvou metrů dokazuje, že standard 802.11g má mnohem menší problémy s odrazy v uzavřené místnosti. Dotaz o velikosti 64 B se po celou dobu měření pohybuje kolem hodnoty 0,5 ms a i špičkové hodnoty jen zřídka přesáhnou hodnotu 1ms. Větší, 1024 B dotaz rovněž představuje pro standard menší problém. Téměř všechny hodnoty se drží u hranice 1,2 ms. Z grafu je také zřejmé, že občasné špičky jsou způsobeny velmi malou vzdáleností mezi zařízeními a odrazy.




*Obrázek 45: 802.11g test odezvy ve vzdálenosti 2 m*

Velmi zajímavým jevem je průběh závislosti datové propustnosti na čase ve směru klient-AP. Ve srovnání se standardem 802.11n je datová průměrná propustnost přibližně o 700 kB/s vyšší. Na první pohled je také patrné, že velikost rychlosti přenosu je téměř „konstantní" a to 3,5 MB/s (28 Mbit/s). Špičková hodnota je následkem působení jiného Wi-Fi zařízení nebo softwarový problém na straně přijímače či vysílače. Rozdíly v průběhu testů budou způsobeny pravděpodobně tím, že klientské zařízení Broadcom má na nižší vzdálenosti lepší schopnosti s koordinováním signálu a dokáže se lépe vypořádat s odrazy v místnosti. Tento test dokazuje, že na menší vzdálenosti je jednoznačně spolehlivějším standardem standard 802.11g o maximální datové propustnosti 54 Mbit/s. Důležité je také uvědomit si, že jistou roli může hrát v tomto měření i fakt, že vysílací část klientského zařízení je na nízké vzdálenosti stabilnější.

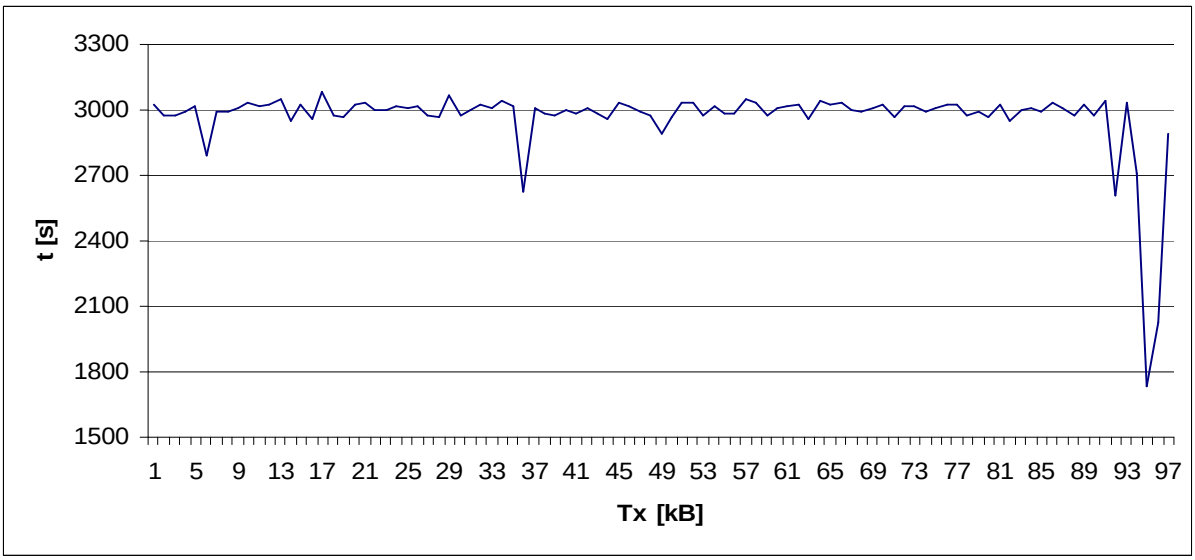



*Obrázek 46: 802.11g test propustnosti klient-AP ve vzdálenosti 2 m*

### 7.3.2 Test ve vzdálenosti 5 metrů

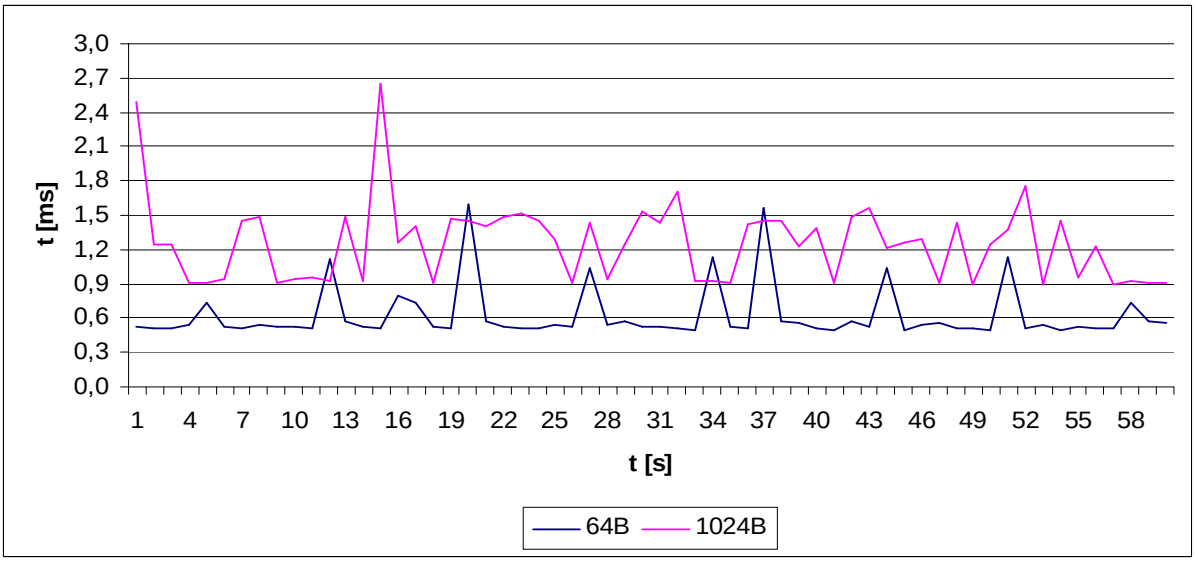
U testu na vzdálenosti pěti metrů se oproti testu na vzdálenosti 2 m objevují menší problémy s přenosem dat. Průměrná hodnota velikosti přenosu stoupla na 3 MB/s. Křivka se chová velmi plynně a špičkové hodnoty se objevují jen zřídka. Velikost signálu se paradoxně snížila na hodnotu -41 dBm a velikost šumu zvýšila na -96 dBm.

Různé výsledné hodnoty z měření standardu 802.11g na různých vzdálenostech budou způsobeny použitím zařízení od různých výrobců a různou citlivostí rádiových přijímacích a vysílacích částí obou zařízení, která se v závislosti na vzdálenosti mění.



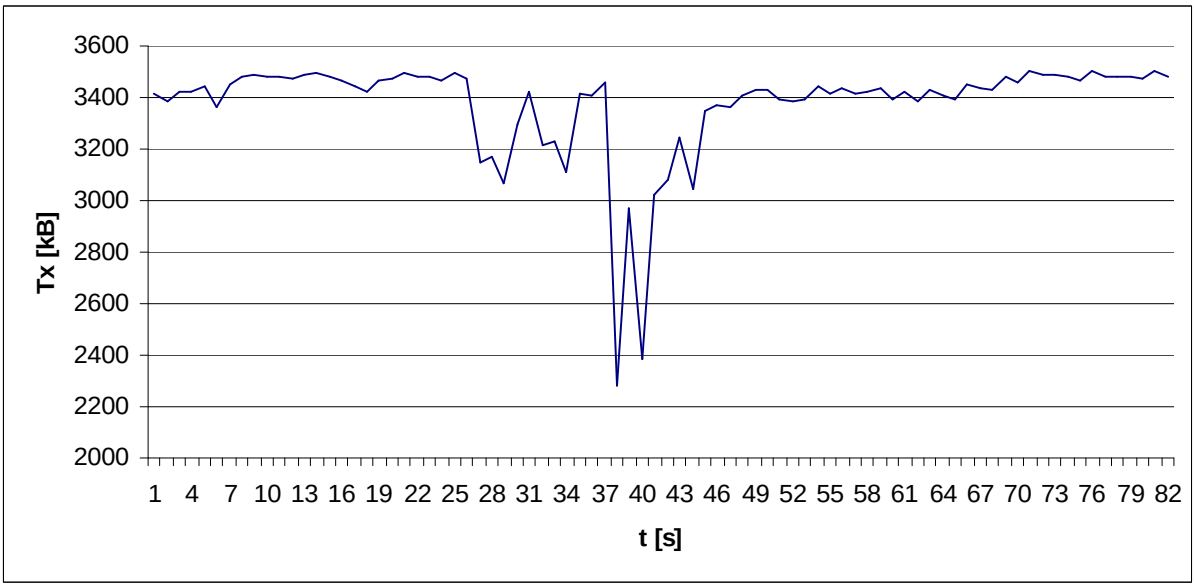

*Obrázek 47: 802.11g test propustnosti AP-klient ve vzdálenosti 5 m*

Rovněž z následujícího grafu testu odezvy jsou viditelné větší problémy s komunikací. U 64 B dotazu se objevují větší rozdíly mezi hodnotami a větší množství špiček než u testu na vzdálenosti 2 m. Průběh testu s 1024 B dotazem se chová přibližně stejně jako v předchozím případě. Oproti testu u standardu 802.11n jsou hodnoty velikosti latence nižší a stabilnější.




*Obrázek 48: 802.11g test odezvy ve vzdálenosti 5 m*

V testu propustnosti standardu 802.11g ve směru klient-AP jsou patrné větší problémy oproti testu ve vzdálenosti dvou metrů. Průměrná hodnota rychlosti přenosu se snížila na 3,4 MB/s. Rychlost je v závislosti na čase méně stabilní a z grafu je vidět i špičkové snížení rychlosti. Příčinou může být rušení cizích radiových zdrojů. Odrazy by v tomto případě měly mít z hlediska negativního ovlivnění signálu menší váhu.



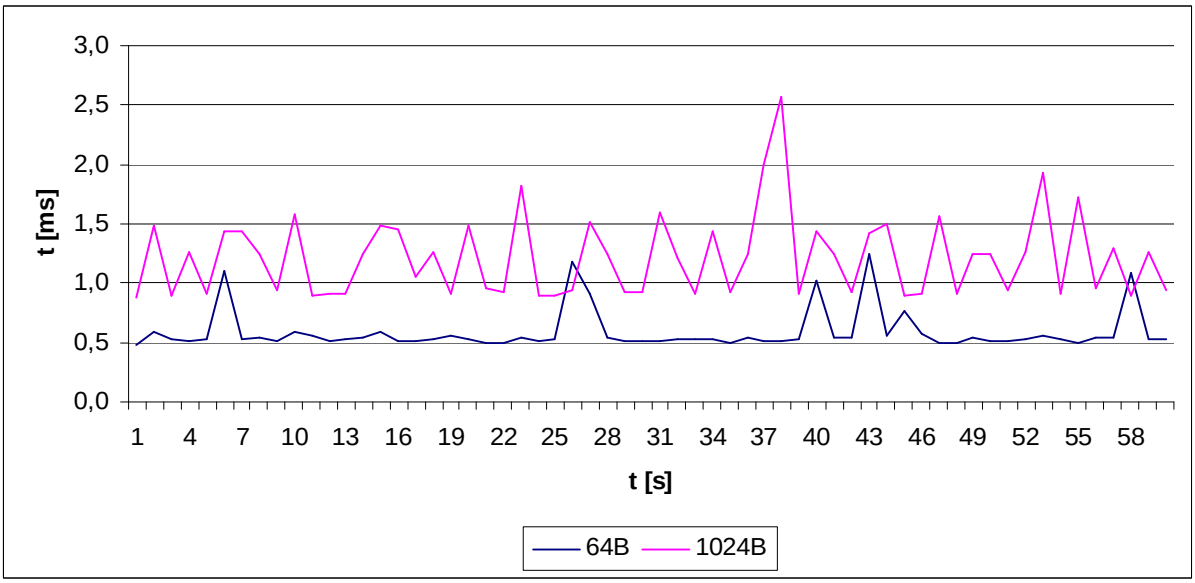

*Obrázek 49: 802.11g test propustnosti klient-AP ve vzdálenosti 5 m*

### 7.3.3 Test skrz cihlovou zeď

Test standardu 802.11g skrz cihlovou překážku přinesl v porovnání se standardem 802.11n velmi zajímavé výsledky. Následující graf vykresluje chování rychlosti přenosu dat ve směru AP-klient. Rychlost je po celou dobu měření téměř konstantní a to přibližně 3 MB/s.V grafu jsou vidět pouze dvě a to minimální výchylky. Starší standard 802.11g se i v tomto měření oproti standardu 802.11n chová stabilněji. Velikost signálu změřena příkazem „iwlist wlan0 scan“ byla po celou dobu testu -51 dBm.

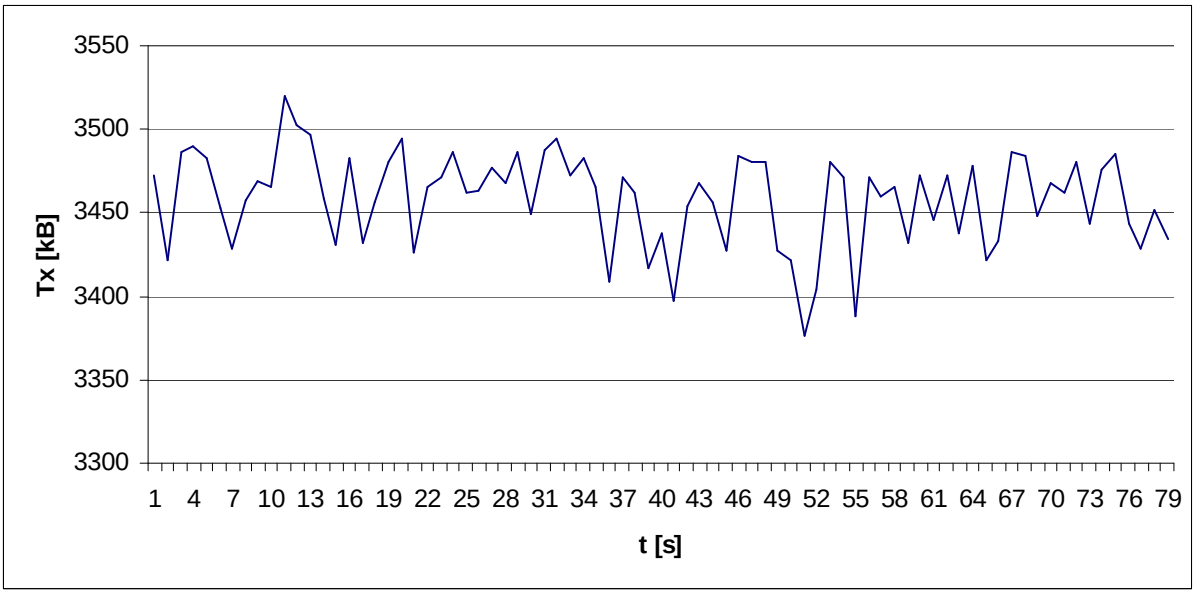

*Obrázek 50: 802.11g test propustnosti AP-klient skrz cihlovou překážku*

Výsledný graf testu odezvy skrz cihlovou zeď ukazuje, že pro standard 802.11g není cihlová překážka velkým problémem. 64 B ping minimálně kolísá kolem hodnoty 0,5 ms. 1024 B dotaz je už překážkou více ovlivněn, ovšem velikost odezvy jen zřídka překračuje hodnotu 1,5 ms. Oproti standardu 802.11n, který v testu odezvy několikrát nabýval i hodnot větších než 100 ms, standard 802.11g z hlediska spolehlivost a stability jednoznačně vede.




*Obrázek 51: 802.11g test odezvy skrz cihlovou překážku*

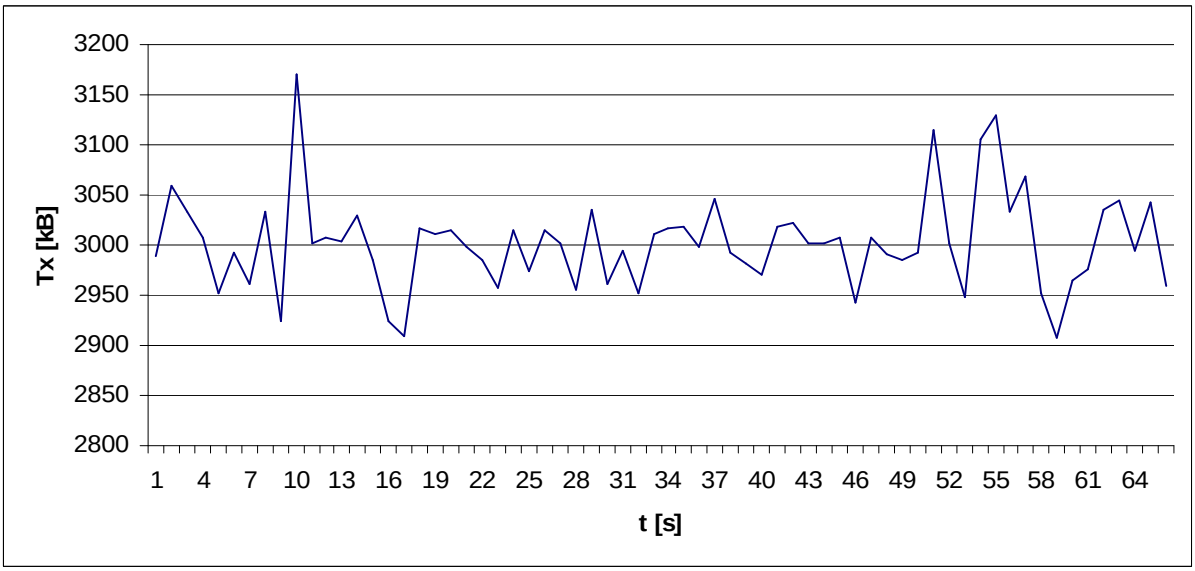
V testu propustnosti skrz cihlovou překážku se objevují větší výchylky než v testu v uzavřené místnosti. Průměrná hodnota rychlosti přenosu se pohybuje kolem hodnoty 3,4 MB/s. Ve srovnání s testem standardu 802.11n je průměrná hodnota vyšší zhruba o 600 kB/s a rovněž i jednotlivé hodnoty kolísají méně. Cihlová překážka představuje pro standard 802.11g z hlediska stability propustnosti znatelně menší problém. Důvodem je pravděpodobně výrazně „agresivnější" chování bezdrátového zařízení Broadcom BCM4318bg a použití duálních antén s větším ziskem.




*Obrázek 52: 802.11g test propustnosti klient-AP skrz cihlovou překážku*

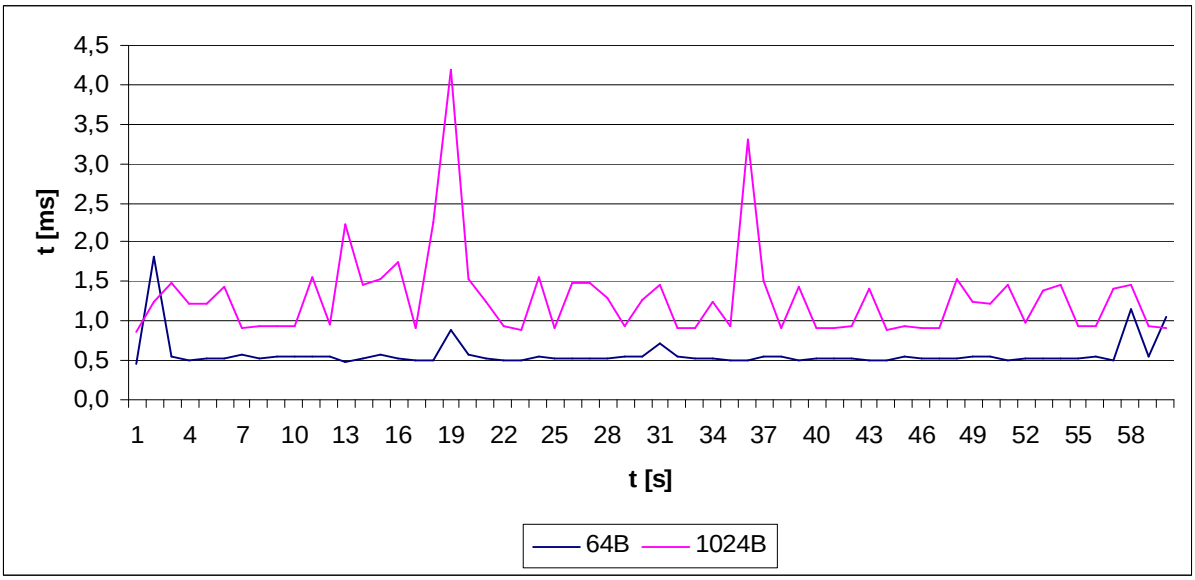
### 7.3.4 Test skrz betonový strop

U následujícího testu jsem testoval chování datové propustnosti za použití betonové překážky. Graf propustnosti vykazuje velmi kolísavé hodnoty a přenos je výrazně méně stabilní než v předchozím případě. Průměrná hodnota je přibližně 3 MB/s. Použití betonové překážky znatelně ovlivnilo průběh stahování, což bude způsobeno oslabením vysílací části přístupového bodu překážkou. Velikost signálu se v tomto měření pohybovala kolem hodnoty -63 dBm.



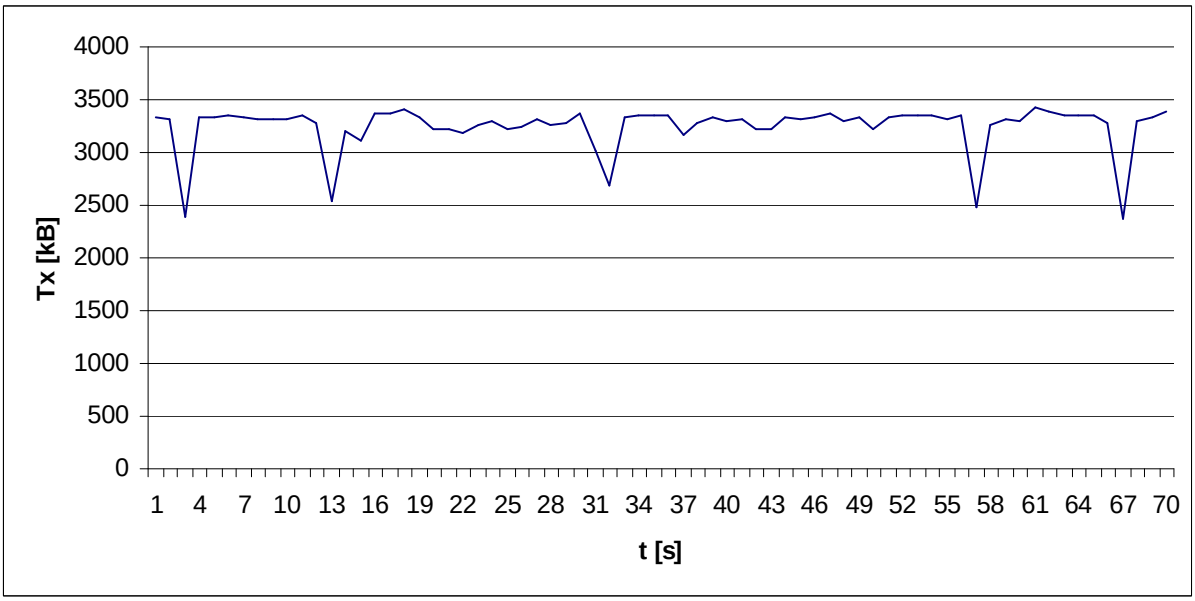

*Obrázek 53: 802.11g test propustnosti AP-klient skrz betonovou překážku*

Graf chování latence v závislosti na čase měření se velmi podobá grafu v měření přes cihlovou zeď. V testu odezvy se velikost časové prodlevy u dotazu o velikosti 64 B chovala velmi stabilně a mírně překračovala hodnotu 0,5 ms. 1024 B dotaz pouze ve špičkových hodnotách překračoval hodnotu 1,5 ms.




*Obrázek 54: 802.11g test odezvy skrz betonovou překážku*

Následující závislost popisuje chování rychlosti přenosu ve směru od klientského zařízení k přístupovému bodu. Paradoxně se křivka podobá testu propustnosti skrz cihlovou zeď ve směru AP-klient. Důvodem může být to, že pro klientské zařízení je betonová překážka větším problémem ve směru upload a menším ve směru download. Naopak cihlová zeď představuje pro radiovou část klientského zařízení větší překážku ve směru download a menší ve směru upload. Velkou roli hraje v těchto testech různá citlivost bezdrátových zařízení v různých podmínkách.




*Obrázek 55: 802.11g test propustnosti klient-AP skrz betonovou překážku*

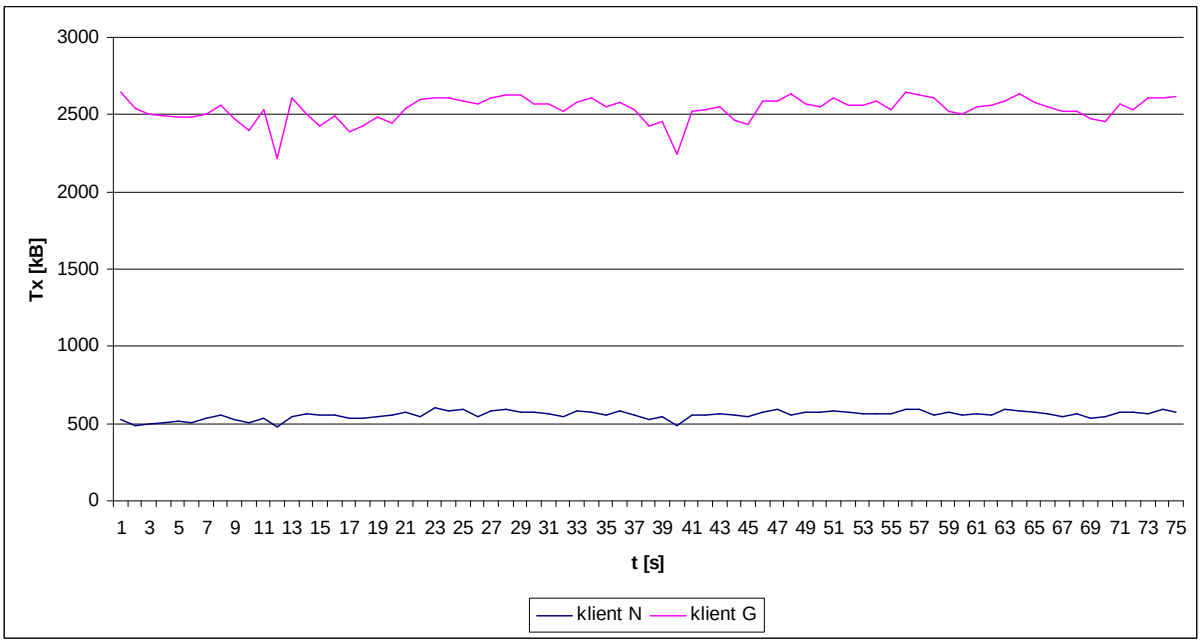
## 7.4 Mód 802.11n, 802.11g mixed - klient Broadcom a D-Link

V následujících testech jsem jako klientské zařízení do bezdrátové sítě zapojil obě zařízení D-Link DWA-643 i Broadcom BCM4318bg, přičemž první jmenované pracovalo v módu 802.11n a druhé na standardu 802.11g. Přístupový bod byl nastaven do módu „802.11n, 802.11g mixed“, aby byl schopen pracovat s oběma zařízeními. Testy byly prováděny ve třech vzdálenostech a s jednou překážkou tj. vzdálenost 2 m, 5 m, otevřený prostor cca 20 m a skrz betonovou překážku. Tyto testy mají pomoci čtenáři představit si vlivy komunikace zařízení od různých výrobců pracujících na různých standardech v reálném prostředí a ozřejmit si chování metod zpětné kompatibility definované v novém standardu 802.11n.

### 7.4.1 Test ve vzdálenosti 2 metrů

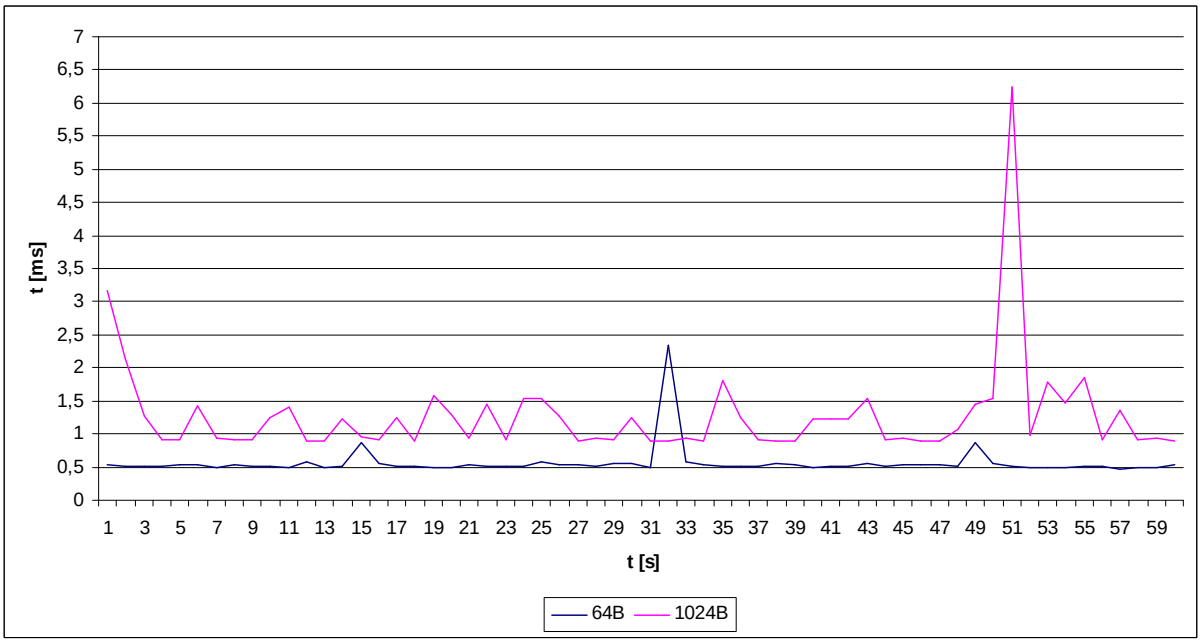
Následující graf vykresluje chování datové propustnosti v závislosti na čase měření obou zařízení na vzdálenosti dva metry. Starší standard 802.11g se chová stejně jako v testu samotného zařízení Broadcom a naopak propustnost zařízení DWA-643 pracujícím na standardu 802.11n je téměř mizivá. Důvodem je velké zarušení způsobené zařízením Braodcom BCM4318bg a především výrazně výkonnějšími anténami integrovanými v přenosném počítači. Na kratších vzdálenostech jak jsme si již ověřili v předešlých testech standard 802.11g lépe komunikuje a není ovlivněn tolika odrazy v místnosti. Průměrná

rychlost stahování je 2,5 MB/s u zařízení Broadcom a přibližně 0,5 MB/s u D-Link. Důležité jsou v tomto měření i síly signálu, které byly u obou zařízení -39 dBm.



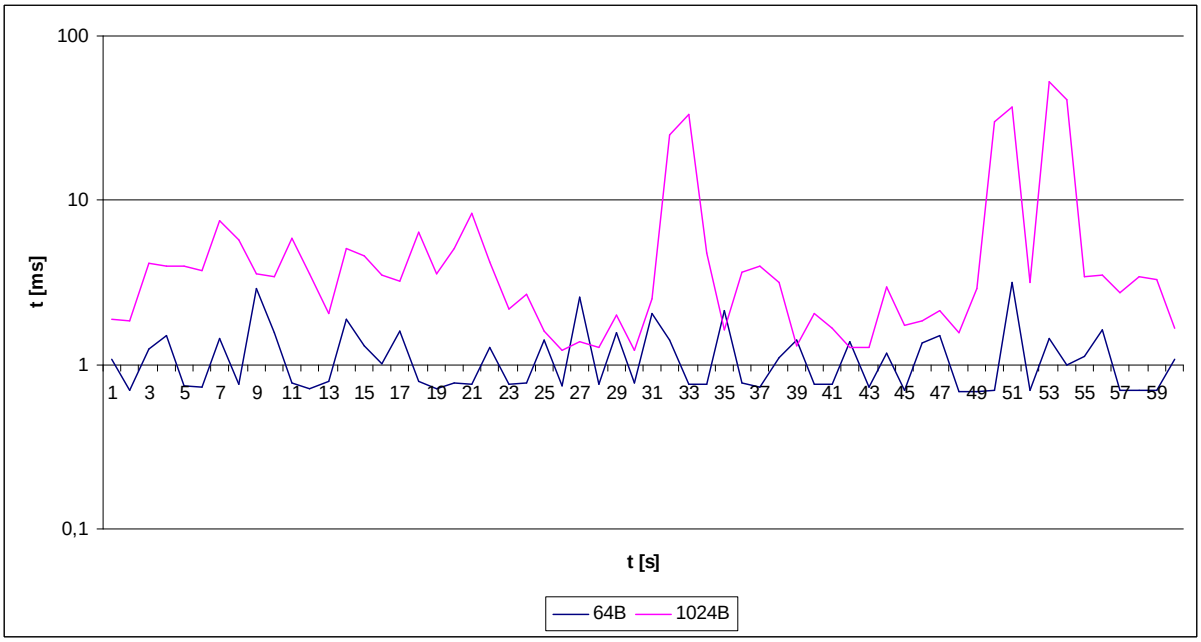

*Obrázek 56: Test propustnosti obou klientských zařízení AP-klient ve vzdálenosti 2 m*

Následující graf popisuje chování hodnoty velikosti odezvy klientského zařízení Broadcom. Křivka se chová velmi podobně jako u testu standardu 802.11g. Dotaz o velikosti 64 B se po dobu měření stabilně pohyboval kolem hodnoty 0,5 ms s minimálním počtem špičkových hodnot a větší, 1024 B se držel pod hranicí 1,5 ms.



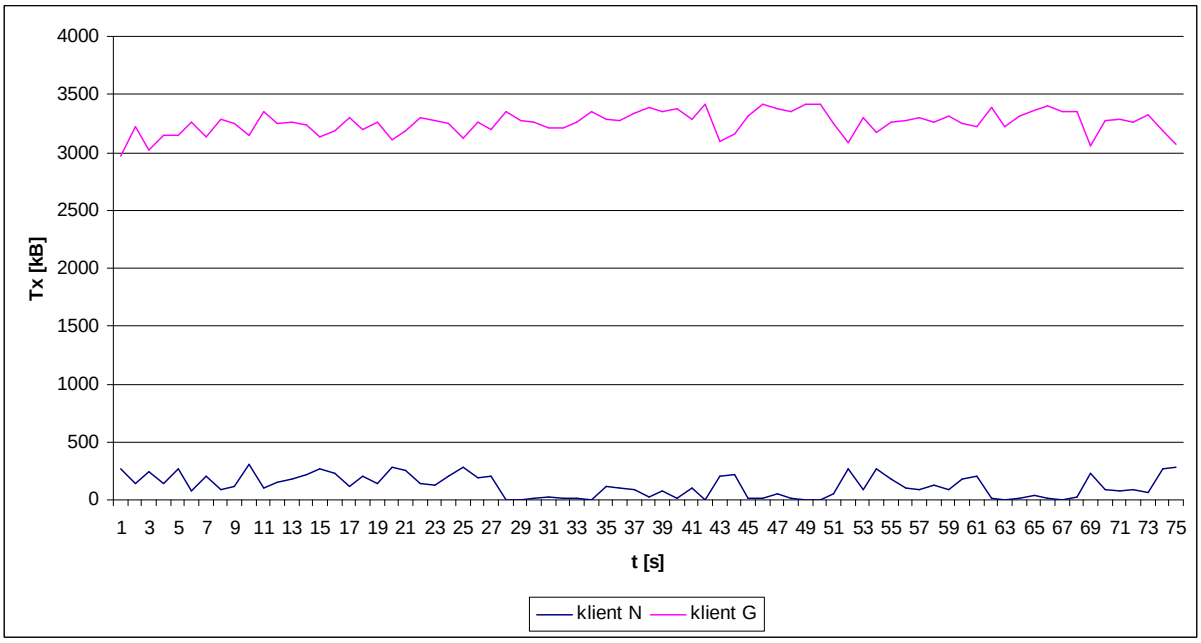

*Obrázek 57: 802.11g test odezvy ve vzdálenosti 2 m*

U testu odezvy klientského zařízení D-Link jsou na první pohled vidět veliké výchylky mezi sousedními hodnotami a proto bylo nutné graf vykreslit v logaritmickém měřítku. Velikost latence dotazu 64 B kolísala v intervalu 0,7-3 ms a dotaz 1024 B se často blížil hranici 10 ms a ve špičkách až hodnotě 100 ms.




*Obrázek 58: 802.11n test odezvy ve vzdálenosti 2 m*

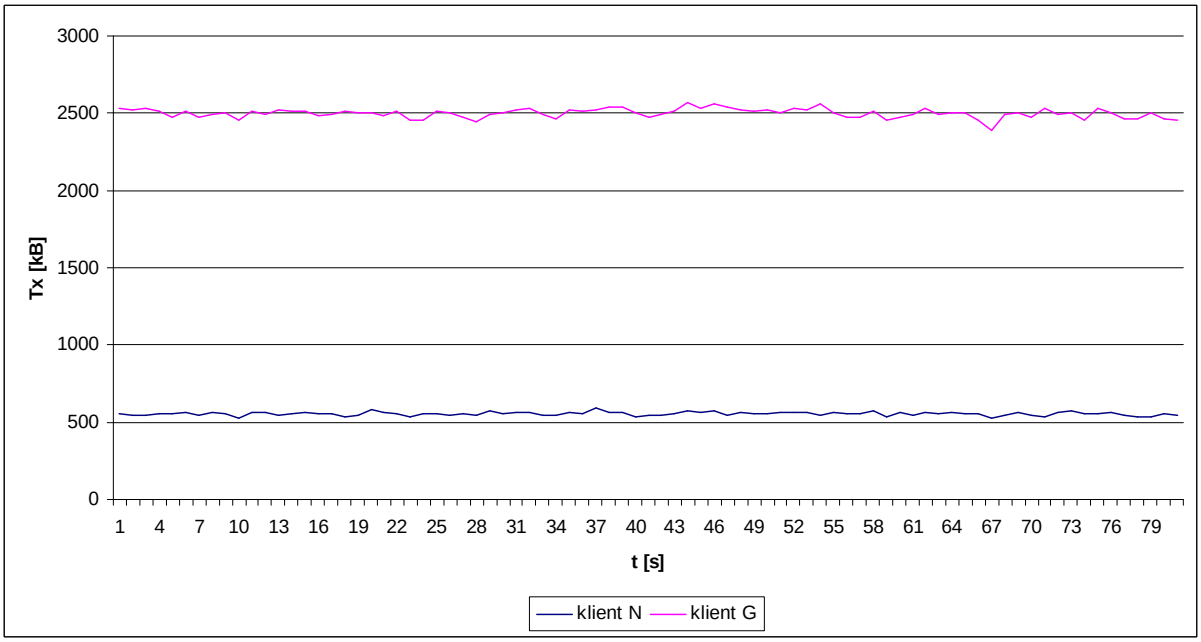
Grafické znázornění velikosti propustnosti ve směru klient-AP vypovídá opět o silném rušení zařízení Broadcom. Klientská stanice D-Link je silně znevýhodněna odrazy v místnosti a vlivy rušení, v některých úsecích měření došlo dokonce ke ztrátě komunikace mezi tímto zařízením a přístupovým bodem.




*Obrázek 59: Test propustnosti obou klientských zařízení klient-AP ve vzdálenosti 2 m*

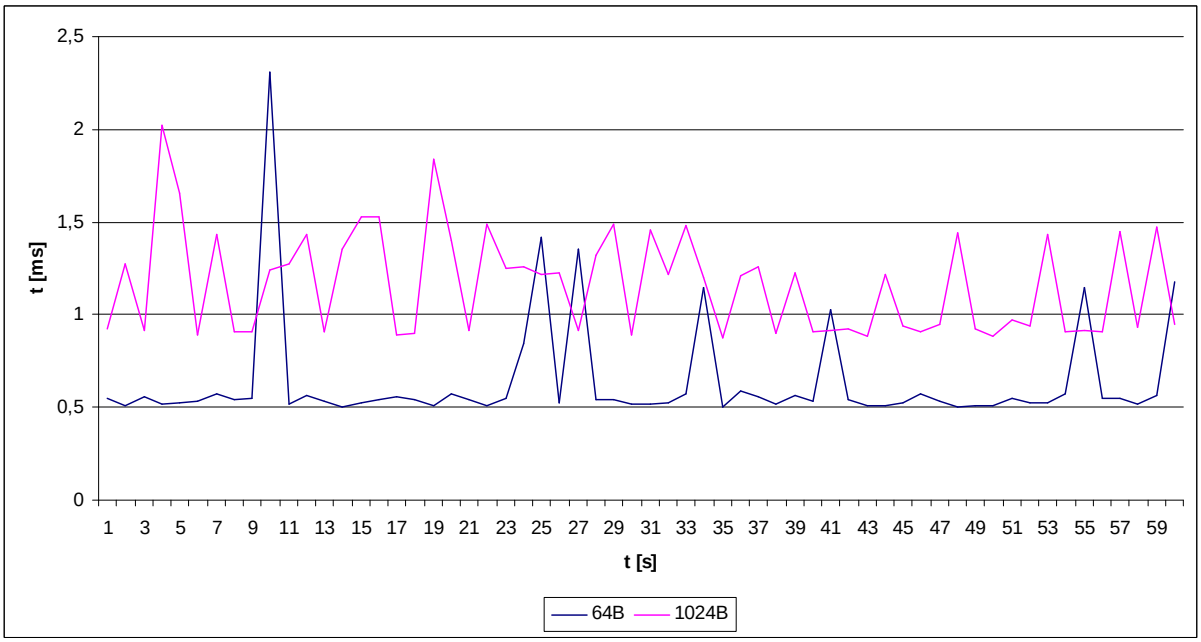
### 7.4.2 Test ve vzdálenosti 5 metrů

Výsledky testu propustnosti a odezvy pro vzdálenost 5m jsou téměř identické jako v předešlém testu. V prvním grafu jsou vidět minimální změny, závislosti propustnosti na čase obou standardů jsou stabilnější, ale průměrná hodnota se od testu ve vzdálenosti dvou metrů neliší. Standard 802.11n opět podléhá rušivým vlivům zařízení Broadcom a rychlost stahování je v porovnání s teoretickými předpoklady zanedbatelná. Síla signálu změřená na obou zařízeních je opět jako v minulém případě -39 dBm.



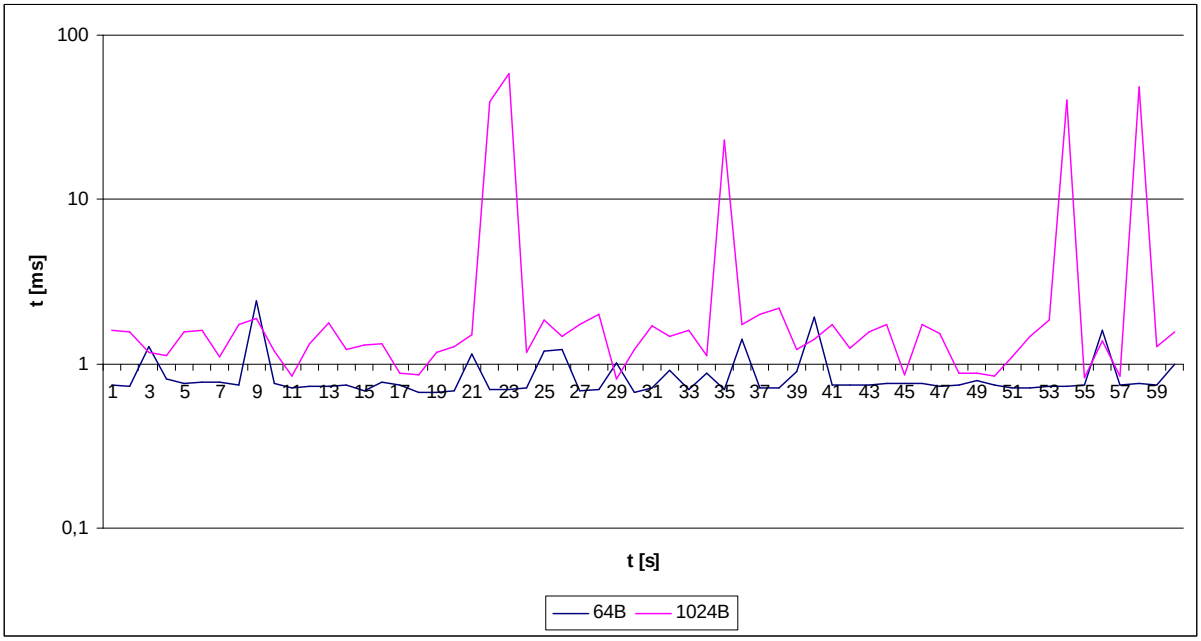

*Obrázek 60: Test propustnosti obou klientských zařízení AP-klient ve vzdálenosti 5 m*

Test odezvy na zařízení Broadcom se chová velmi podobně jako v předešlém případě.



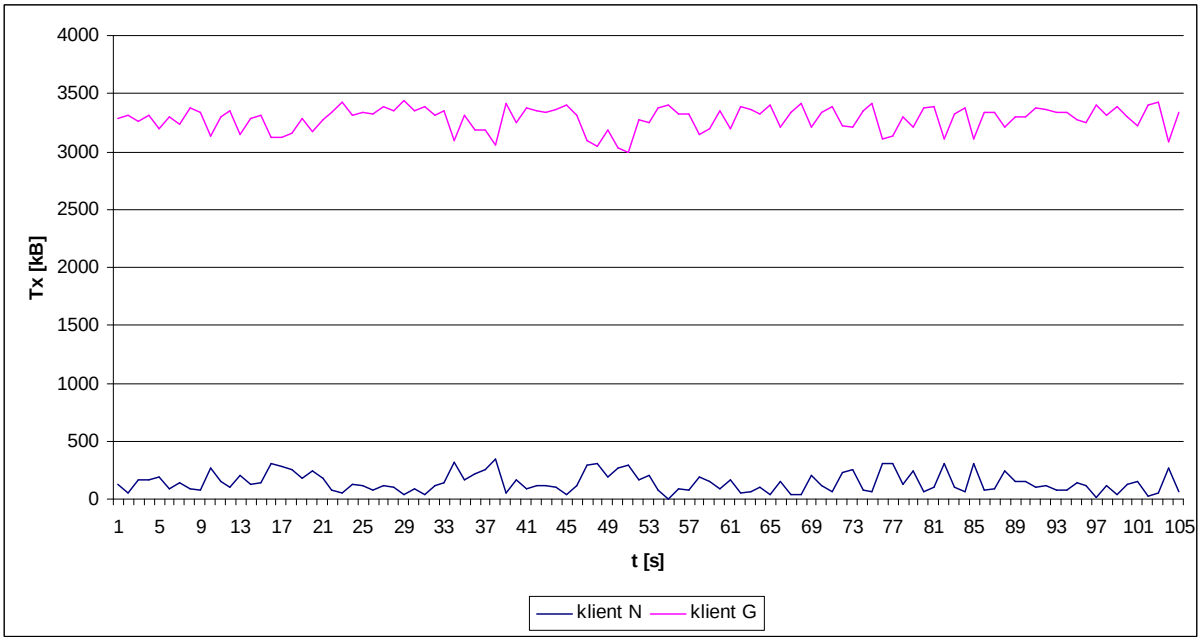

*Obrázek 61: 802.11g test odezvy ve vzdálenosti 5 m*

Graf odezvy na zařízení DWA-643 bylo nutno opět vykreslit v logaritmickém měřítku, protože se objevují i velmi vysoké hodnoty. Dotaz o velikosti 64 B se drží pod hodnotou 1 ms ale dotaz 1024 B nabývá podstatně vyšších hodnot blížících se ve špičkách hodnotě 100 ms.




*Obrázek 62: 802.11n test odezvy ve vzdálenosti 5 m*

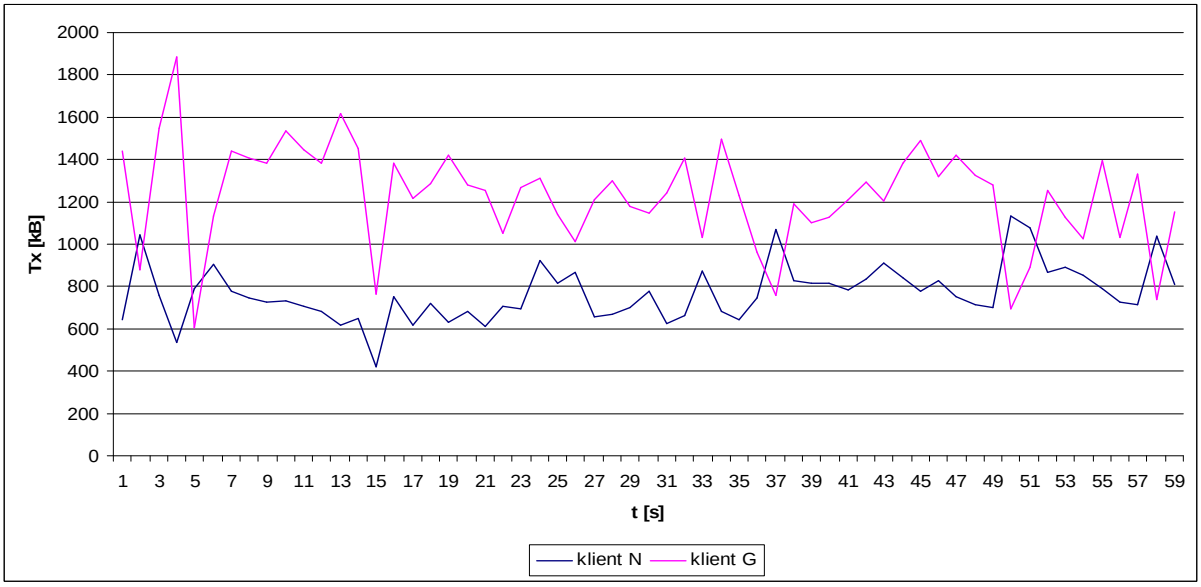
Vyjádření propusti nevykazuje žádné znatelné rozdíly oproti měření na kratší vzdálenost. Rychlost přenosu standardem 802.11n je opět velmi nízká, pro kvalitní a spolehlivou komunikaci nepoužitelná. Na druhou stranu standard 802.11g přenášel data relativně vysokou rychlostí bez známek rušivých vlivů nebo odrazů.




*Obrázek 63: Test propustnosti obou klientských zařízení klient-AP ve vzdálenosti 5 m*

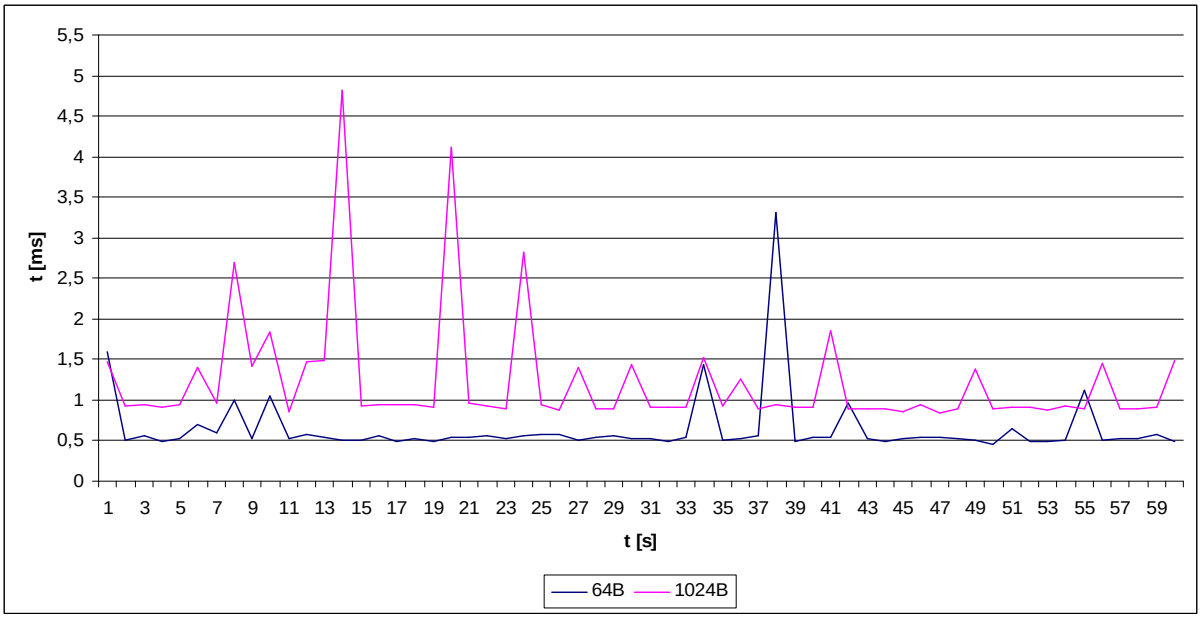
### 7.4.3 Test skrz betonový strop

V následujícím měření byla mezi obě klientská zařízení a přístupový bod postavena překážka. V grafu propustnosti se přenos choval v obou případech hodně chaoticky. Průměrná rychlost přenosu zařízením Broadcom se v tomto případě snížila 1,2 MB/s a rychlost zařízením D-Link zvýšila na přibližně 800 kB/s, což je oproti teoretickým předpokladům stále velmi nízká hodnota. Síla signálu byla nyní u zařízení Broadcom -60 dBm a u zařízení D-Link -53 dBm. Problémy standardu 802.11g jsou způsobeny pravděpodobně absencí technologií MIMO, spatial multiplexing a beamforming.



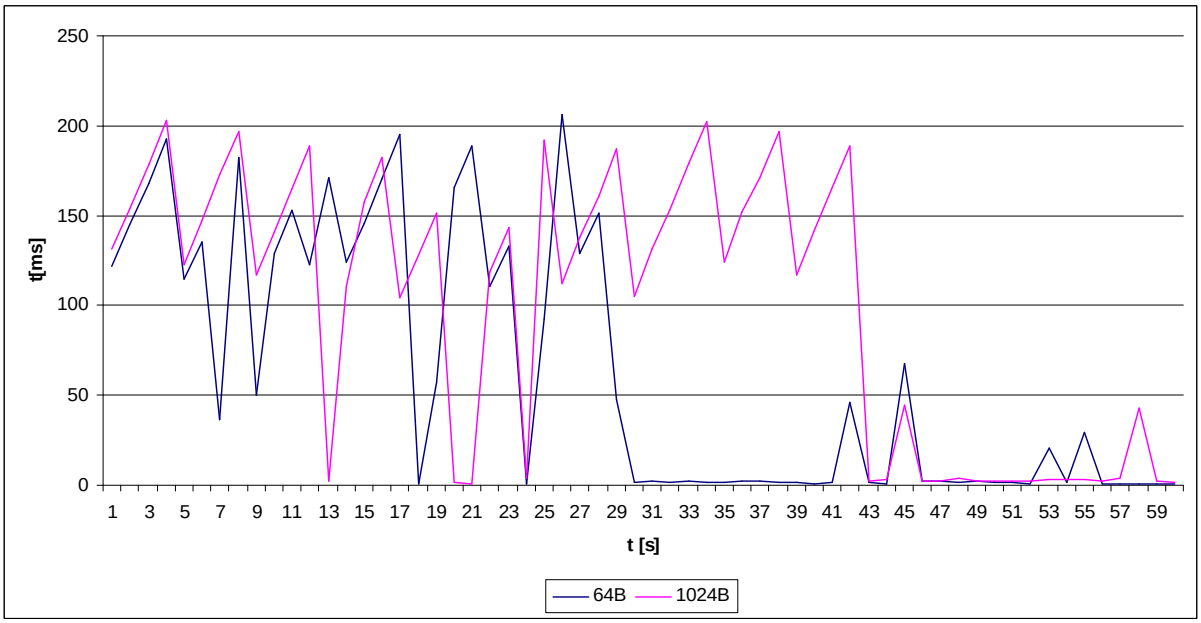

*Obrázek 64: Test propustnosti obou klientských zařízení AP-klient skrz betonovou překážku*

Průběh odezvy zařízení Broadcom během měření se u 64 B dotazu choval stabilně s minimálními výkyvy. U 1024 B dotazu jsou viditelné větší rozdíly mezi hodnotami.



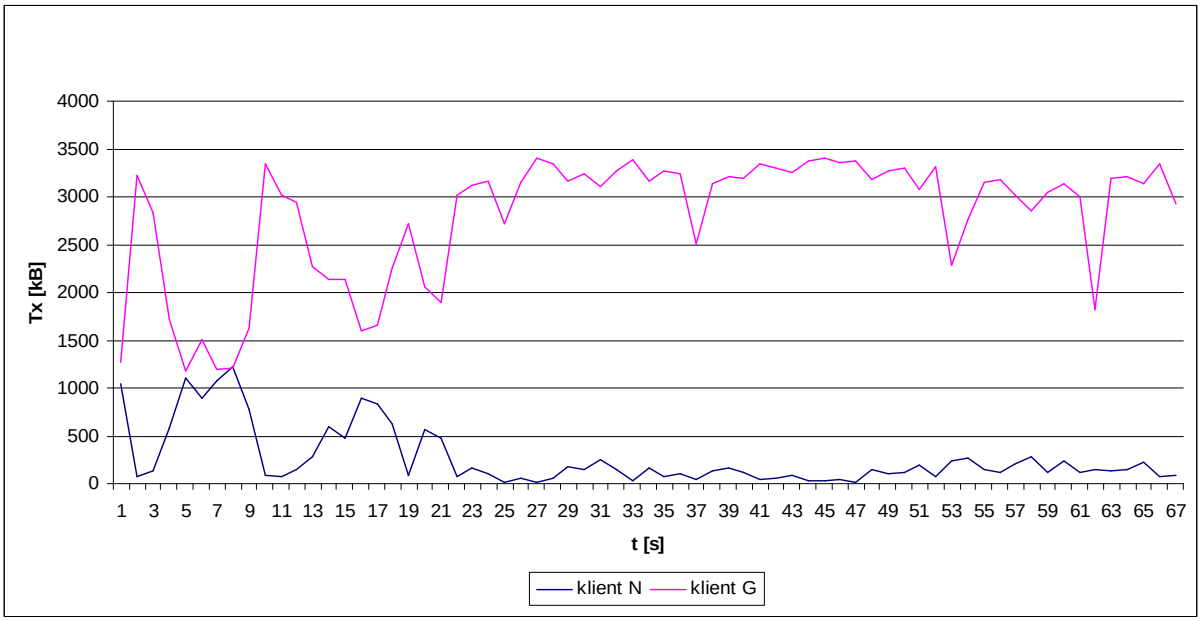

*Obrázek 65: 802.11g test odezvy skrz betonovou překážku*

V následujícím grafu odezvy zařízení D-Link se objevují velmi vysoké rozdíly mezi hodnotami. Obě velikosti dotazů mají veliké zpoždění, což je způsobeno překážkou a rušením druhého klientského zařízení. Pro přenosy citlivé na velikost latence, jako je protokol VoIP, videokonference nebo hraní počítačových her je standard 802.11n v tomto měření nepoužitelný.




*Obrázek 66: 802.11n test odezvy skrz betonovou překážku*

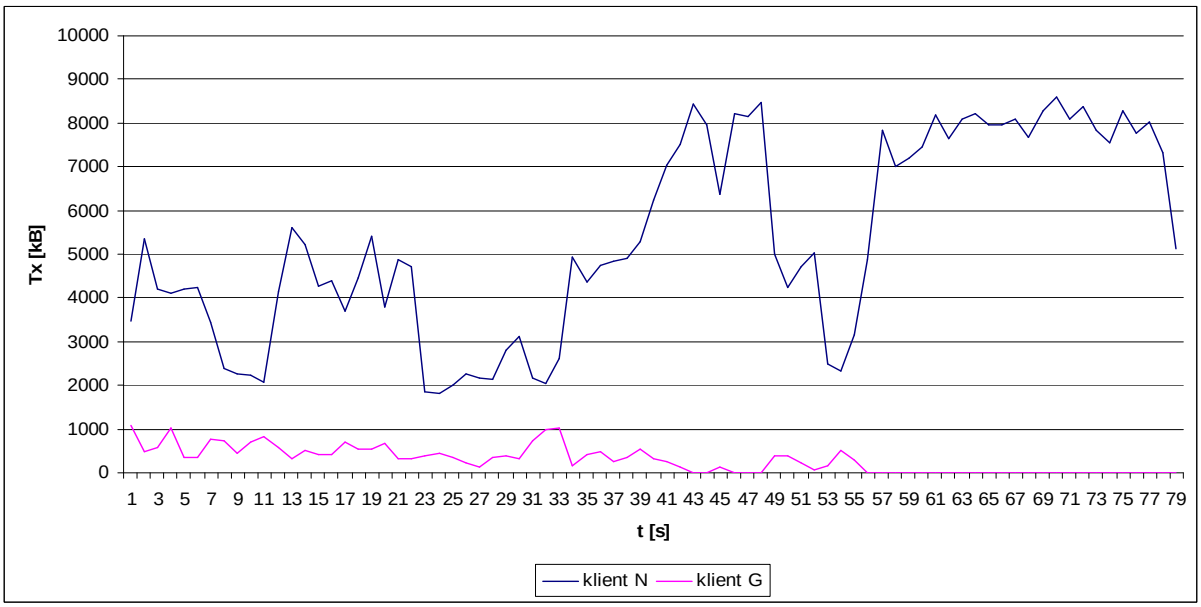
V testu propustnosti ve směru klient-AP se obě křivky chovají, jako kdyby se vzájemně doplňovaly. Na začátku měření mají oba standardy problémy se stabilitou přenosu, ale po krátké chvíli se rychlost ustálí a mezi rychlostmi obou zařízení jsou opět znatelné rozdíly. Standard 802.11g se ukazuje jako jednoznačně výkonnější, což je však způsobeno různě výkonnými a citlivými radiovými částmi klientských zařízení.




*Obrázek 67: Test propustnosti obou klientských zařízení klient-AP skrz betonovou překážku*

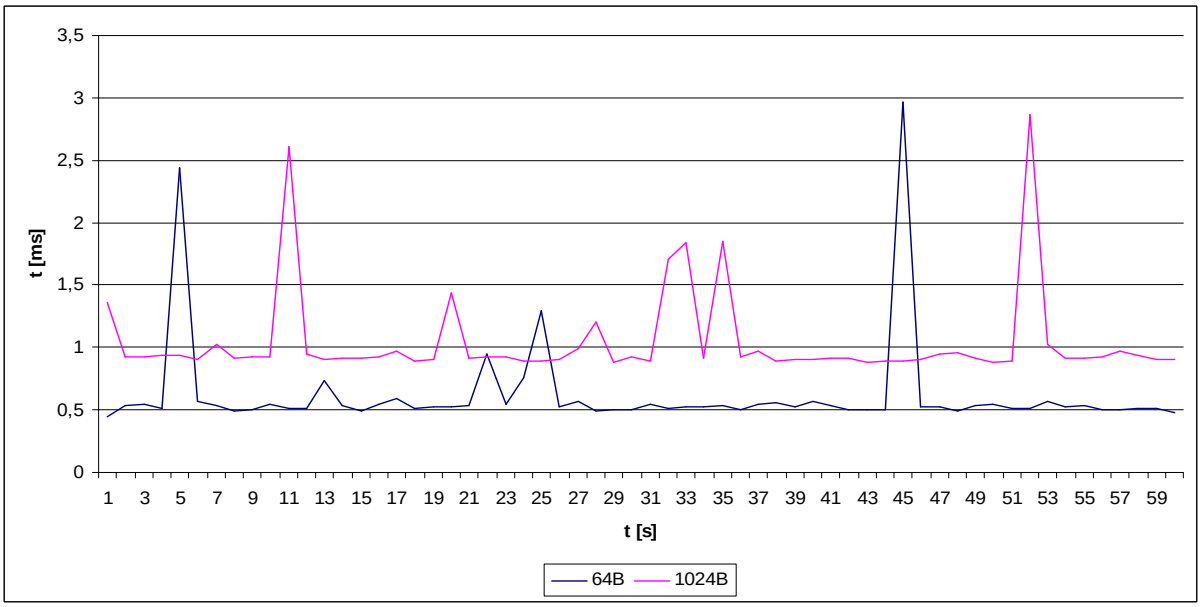
### 7.4.4 Test na otevřeném prostoru

V tomto testu jsem jako prostředí pro testování propustnosti obou zařízení zvolil otevřený prostor bez jakýchkoliv překážek a možností odrazů měřených zařízení. Větší váhu však budou mít negativní vlivy okolních zařízení pracujících na stejných frekvencích. Na prvním měření se standard 802.11n konečně ukazuje, co se týče rychlosti přenosu, jako výkonnější i když jsou v grafu vidět veliké výchylky. Zařízení disponující standardem 802.11g se tentokrát chová velmi omezeně, protože jeho průměrná rychlost přenosu je pouze 750 kB/s. Signál zařízení Broadcom byl v tomto měření -65 dBm a zařízení D-Link -57 dBm.



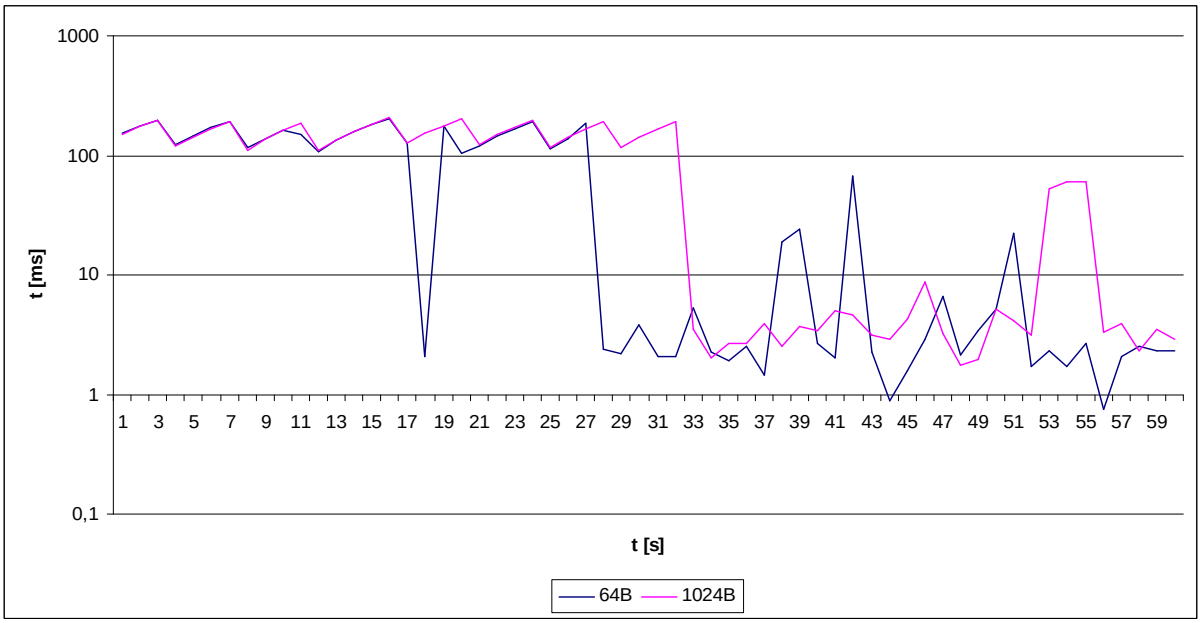

*Obrázek 68: Test propustnosti obou klientských zařízení AP-klient na otevřeném prostoru*

Graf níže vykresluje chování odezvy zařízení Broadcom v závislosti na čase. Kromě špičkových hodnot se velikost latence drží hodně nízko. Je to dáno tím, že signál má k přístupovému volnou cestu bez překážek.



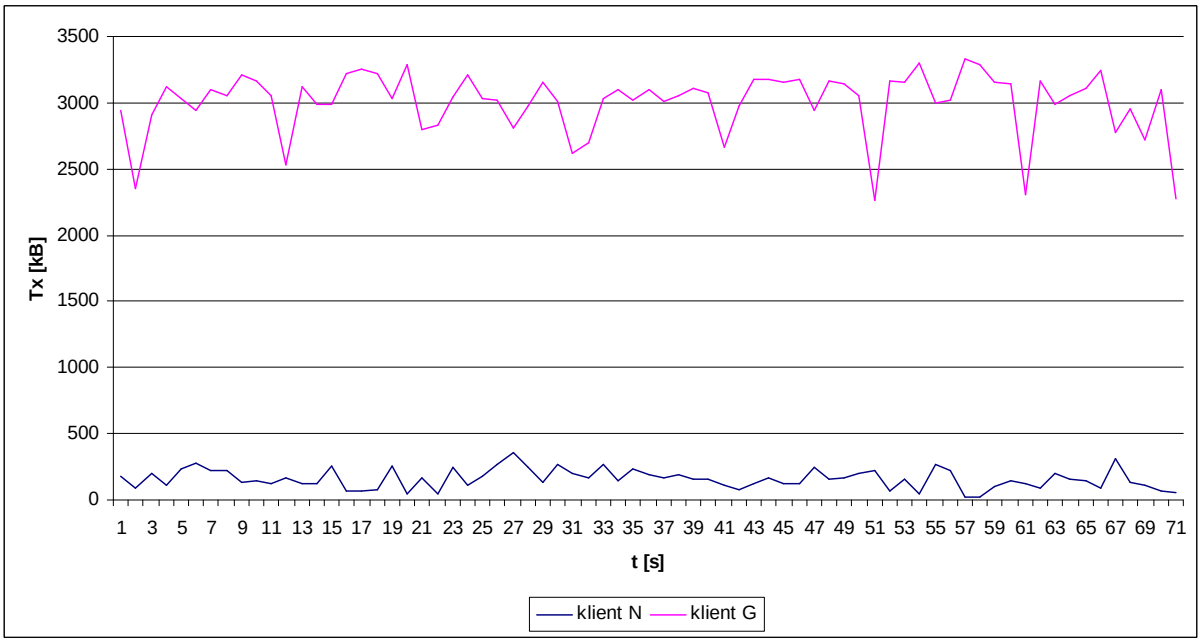

*Obrázek 69: 802.11g test odezvy na otevřeném prostoru*

Charakteristiku doby odezvy v závislosti na čase měření u zařízení D-Link lze považovat jako zcestnou jelikož z grafu je patrné, že signál byl ovlivněn rušením zařízení v okolí, které pracuje na stejné frekvenci. Časové periody odezvy nabývají velmi vysokých hodnot, tudíž graf musel být vykreslen v logaritmickém měřítku. V druhé polovině měření se velikosti period pro obě velikosti dotazů chovají chaoticky.




*Obrázek 70: 802.11n test odezvy na otevřeném prostoru*

Poslední graf popisující chování propustnosti dat ve směru od klientských zařízení k přístupovému bodu vypovídá o tom, že klientské zařízení Broadcom disponuje mnohem silnější a vysílací rádiovou částí a anténami se silnějším ziskem. Rychlost uploadování zařízení D-Link je velmi malá a pro požadovaný provoz nepoužitelná. Rychlost přenosu zařízení Broadcom je, vezmeme-li v potaz větší vzdálenost, velmi stabilní a dostatečná.




*Obrázek 71: Test propustnosti obou klientských zařízení klient-AP na otevřeném prostoru*

# 8 Standard 802.11e v praxi

Následující kapitola praktické části bakalářské práce je zaměřena na měření standardu 802.11e, přesněji jeho profilu standardu WMM. Hlavní myšlenkou testů je ověřit dopad standardu 802.11e (WMM) na datovou propustnost bezdrátové sítě. Testy jsou prováděny na datovém toku z pohledu klientských zařízení ve směru download. U všech testů byl pro generování datového provozu použit vytvořený soubor o velikosti 80 GB, který byl oběma klientskými stanicemi přenášen pomocí protokolu http. Testy jsou prováděny pro jednotlivé priority definované standardem WMM tzn. Voice (VO), Video (VI), Best Effort (BE), Background (BK). K nastavení priorit, definici rozsahů portů a adres IP slouží ve webovém rozhraní přístupového bodu D-Link subsekce WISH (Wireless Inteligent Stream Handling).

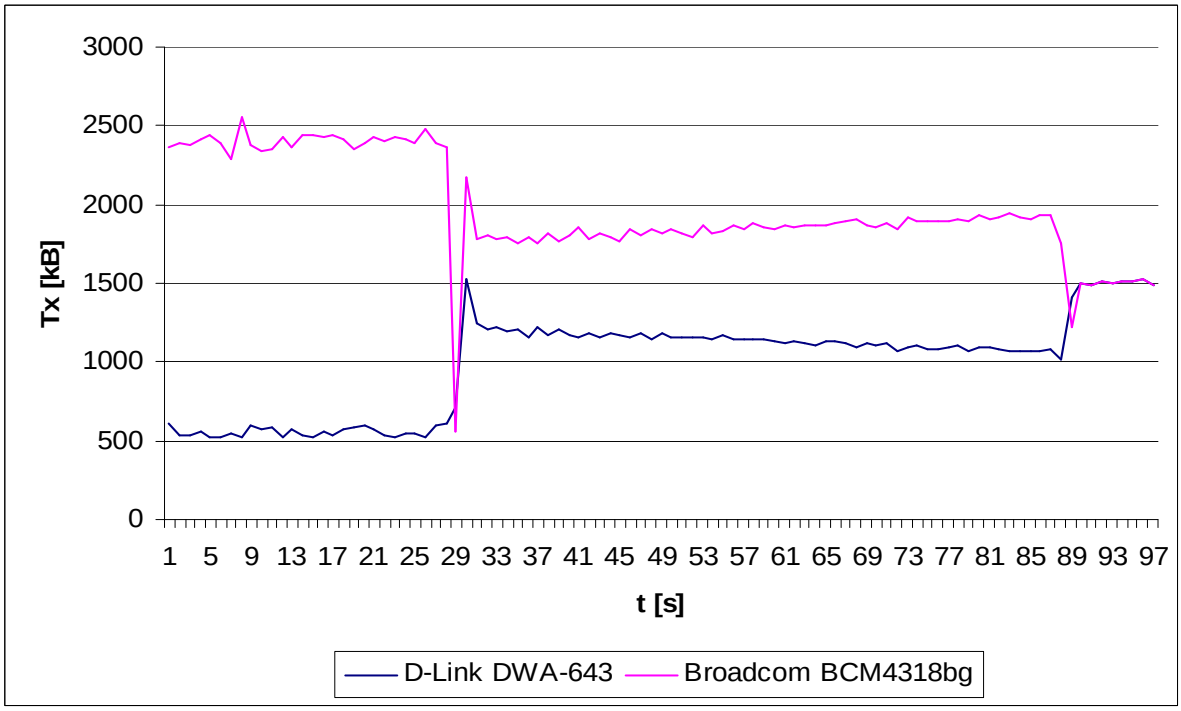

*Obrázek 72: Rozhraní WISH (Wireless Inteligent Stream Handling)*

K měření byly použity stejné komponenty jako při předešlých měření. Přístupový bod D-Link byl stejně jako klientská zařízení Broadcom a D-Link nastaven, aby pracoval pod standardem 802.11g tedy s maximální přístupovou rychlostí 54 Mbit/s. Pro obě klientská zařízení byla kompatibilita se standardem 802.11e (WMM) ověřena. Testy byly prováděny na stejné vzdálenosti cca 3 m. Při testech byl vytvořen testovací hovor pomocí programu

Ventrilo s nastaveným kodekem Speex (16 KHz, 16 bit, 9 Qlty) 4344 B/sec a streaming videa pomocí programu VLC po protokolu udp s datovým tokem přibližně 700 kB/s.

## 8.1 Test nastavení WISH-DISABLED

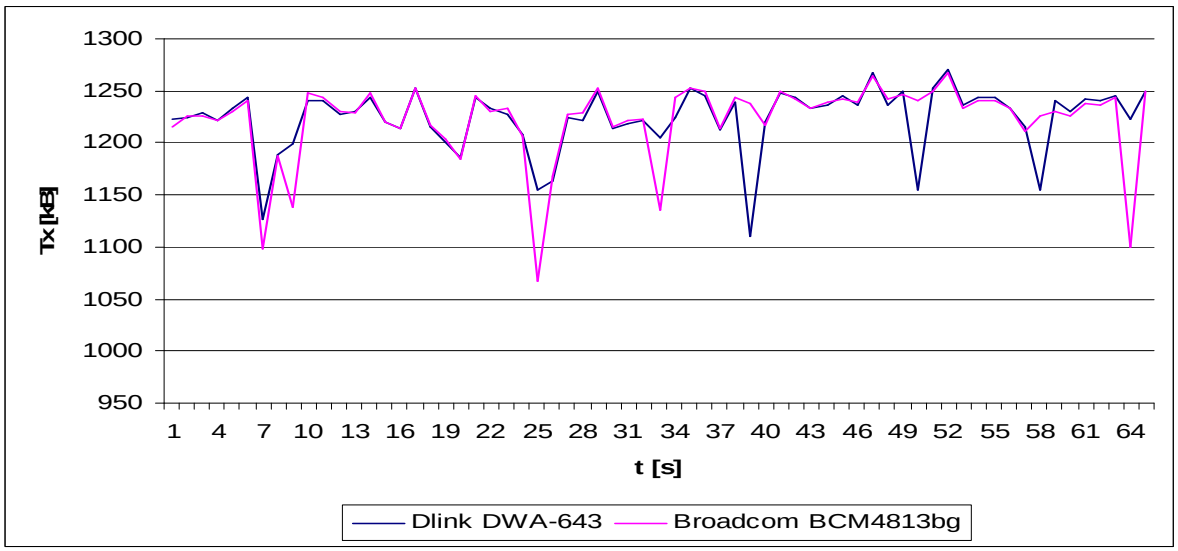
Tento test představuje chování a průběh přenosu z pohledu klientských zařízení ve směru download při vypnutém nastavení WISH. V tomto módu nemá přístupový bod nastavené žádné pravidla pro řízení a priorizaci datového toku.
Následující graf prezentuje chování propustnosti na obou klientských zařízeních při nastavení WISH-DISABLED. Při downloadu dat se ze začátku objevují velké rozdíly v rychlostech, ale ke konci měření je u obou zařízení přenosová rychlost téměř stejná. Během testu byl z klientského notebooku Acer se zařízením D-Link DWA-643 prováděn testovací hovor pomocí programu Ventrilo, avšak při subjektivním posouzení nedošlo k výpadkům hovoru.




*Obrázek 73: Test propustnosti při nastavení WISH-DISABLED*

## 8.2 Test nastavení WISH-AUTOMATIC

V tomto měření bylo v nastavení přístupového bodu zaškrtnuto automatické řízení přidělování priorit. Teoretický předpoklad je, že přístupový bod se sám pokusí svými, od výroby definovanými pravidly o priorizaci datového toku. V tomto módu zařízení deprioritizuje velké datové přenosy, zatímco interaktivním přenosům jako hraní počítačových her, video komunikace nebo komunikace pomocí protokolu VoIP ponechá dostatečný prostor a vyšší prioritu. Z grafu je vidět, že ačkoliv je přenos výrazně chaotický, velikosti rychlostí obou zařízení se po většinu doby měření téměř shodují. Přenos byl prováděn na obě zařízení pomocí protokolu http. Testovací hovor nevykazoval žádné omezení či výpadky.



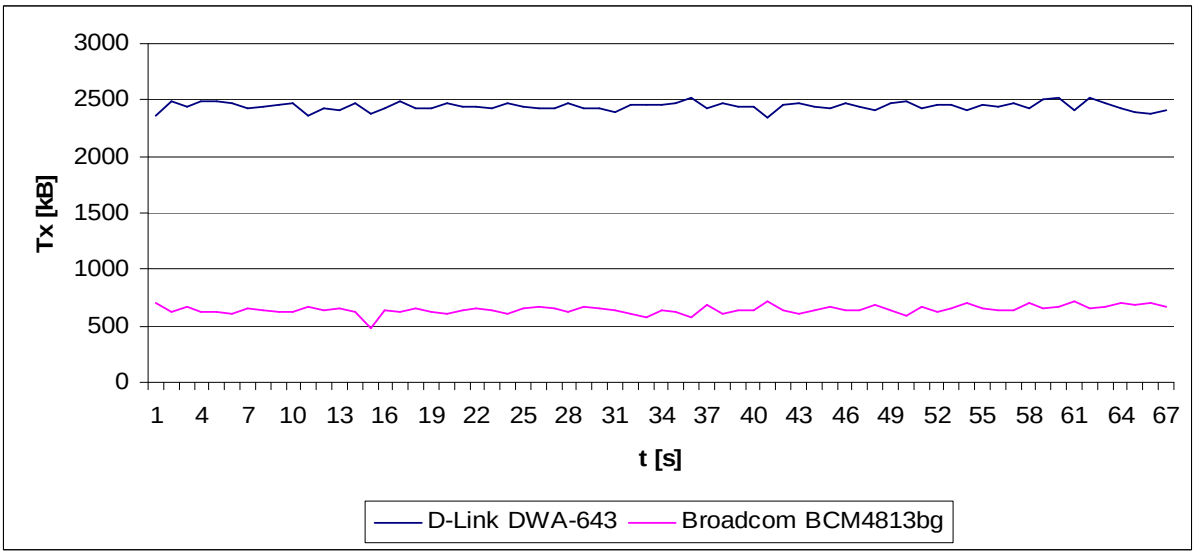

*Obrázek 74: Test propustnosti při nastavení WISH-AUTOMATIC*

## 8.3 Test nastavení WISH-MANUAL

### 8.3.1 Test 1

V tomto testu byla již manuálně nastavena prioritizace pro dané datové toky. Pro notebook Acer s klientským zařízením D-Link DWA-643 byl nastaven rozsah portů tedy 1-80 a priorita Voice (VO). Pro druhý počítač byl nastaven rozsah zahrnující všechny porty, tedy 1-65535, avšak priorita byla nastavena na nejnižší možnou tedy Background (BK). Do tabulky definice pravidel prioritizace sítě byl ještě přidáno pravidlo nastavující program Ventrilo na prvním PC, tedy komunikaci na portu 3784 rovněž na maximální prioritu Voice (VO). Na obou počítačích byl současně spuštěný download souboru o velikosti 80 GB po protokolu http. Na prvním zmiňovaném počítači byl navázán testovací hovor. Během měření nedošlo k žádnému výpadku. Hovor se nezdál být ani ničím rušen či ovlivněn datovým tokem jiného zařízení v bezdrátové síti.

Grafické znázornění představuje průběhy rychlosti stahování obou klientů.

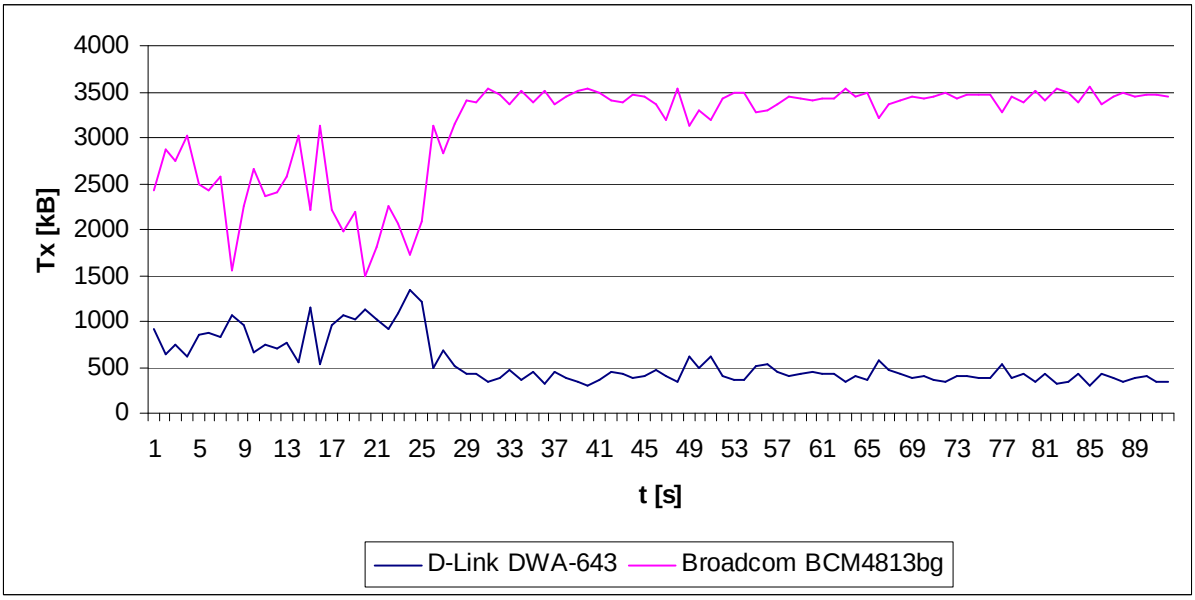



*Obrázek 75: Nastavení priorit VO/BK*

### 8.3.2 Test 2

Další test spočívá opět v nastavení tabulky priorit WISH. Tentokrát však klientský počítač Acer dostává pro porty 1-80 přiřazenou prioritu Background (BK). Další pravidlo nastavuje pro tento počítač prioritu pro port 3784 rovněž na Background (BK). Druhý klientský počítač HP dostává na celém rozsahu portů, tedy 1-65535, maximální možnou prioritu Voice (VO). Během hovoru uskutečněného na počítači Acer se jen zřídka objevovaly mírné chyby v přenosu, hovor byl nastavením nízkých priorit minimálně poznamenaný.
Z grafu níže jsou na začátku měření vidět výchylky v rychlosti, po chvíli se však rychlost přenosu stabilizuje a do konce měření už nemění.

V další části tohoto měření byla priorita komunikace po portu 3784 přenastavena na hodnotu Voice (VO). Hovor již dále nevykazoval žádné chyby či výpadky při přenosu.

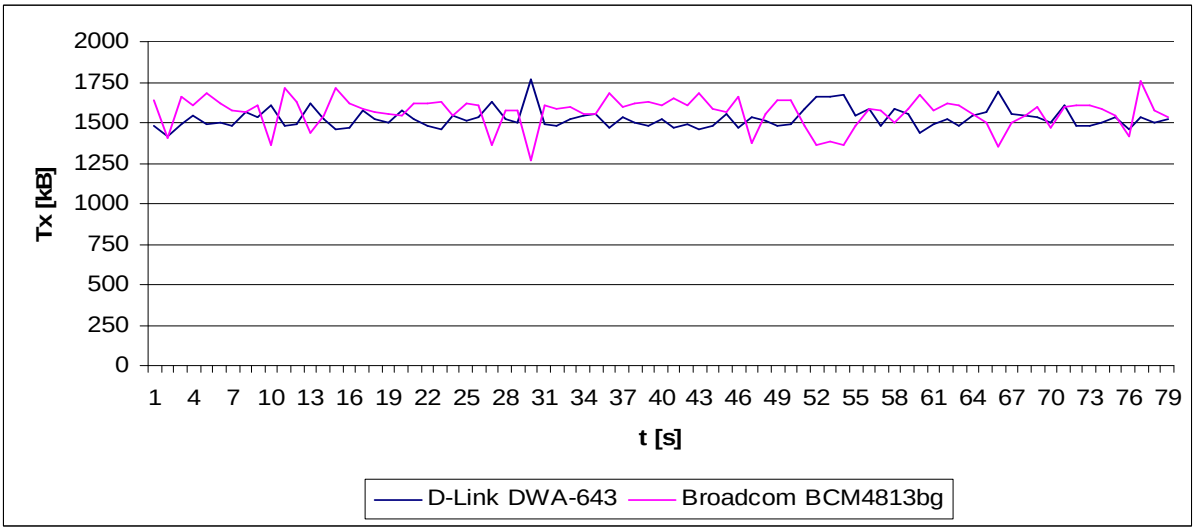



*Obrázek 76: Nastavení priorit BK/VO*

### 8.3.3 Test 3

V tomto testu byla v tabulce priorit použita další priorita definovaná standardem 802.11e. Pro klientský počítač Acer s bezdrátovým zařízení D-Link DWA-643 byla pro porty v rozsahu 1-80 nastavena priorita Voice (VO) stejně jako dalším pravidlem pro port 3784. Na počítači HP se zařízením Broadcom BCM4813bg byla pro celý rozsah portů 1-65535 nastavena druhá nejnižší priorita Best Effort (BE). Po spouštění downloadu na obě zařízení a po započetí hovoru nebyly mezi oběma datovými toky vidět žádné velké rozdíly. Hovor probíhal po celou dobu stahování bez komplikací a výpadků.

Grafické znázornění však představuje odchylku od teoretických předpokladů. Při použití dvou různých priorit u obou počítačů by měly být viditelné rozdíly v přenosových rychlostech.

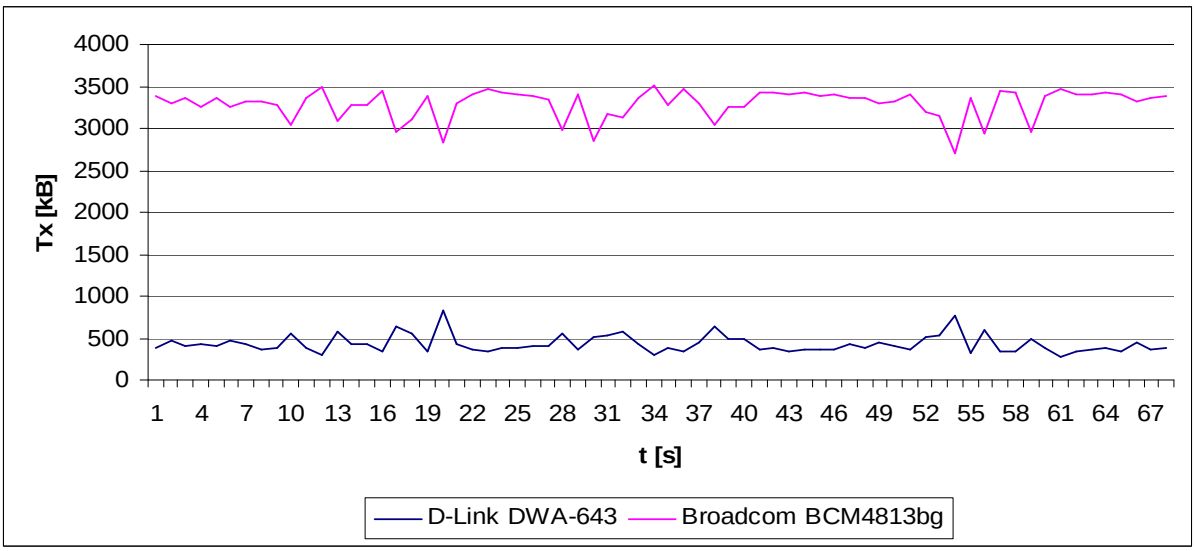



*Obrázek 77: Nastavení priorit VO/BE*

### 8.3.4 Test 4

V tomto testu byly priority pro klientské zařízení prohozeny. Počítač Acer měl pro stahování souboru pomocí protokolu http, tedy pro port 80 nastavenou prioritu Best Effort (BE) stejně jako pro rozmezí portů 3783-3784 pro hlasovou komunikaci pomocí programu Ventrilo. Na druhém klientském počítači byla nastavena priorita Voice (VO) pro všechny porty 1-65535.

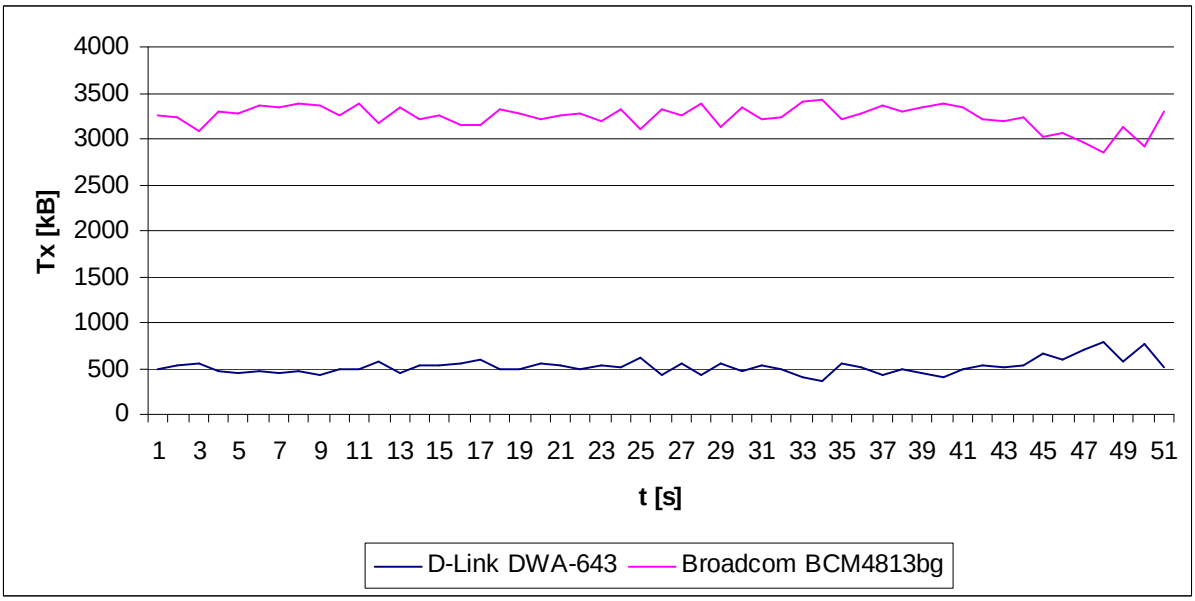
Průběh stahování dat obou zařízení se shoduje s teoretickými předpoklady. Priorizovaný datový tok je několikanásobně vyšší než datový tok s nižší prioritou. Velké rozdíly oproti výsledkům v předcházejícím měření, kdy byly priority obou zařízení prohozené, avšak průměrná přenosová rychlost byla téměř stejná, by se dali zdůvodnit silnějšími anténami připojenými k zařízení Broadcom BCM4813bg a pravděpodobně i „agresivnějším" chováním bezdrátové části. Testovací hovor vykazoval během měření občasnou chybovost přenosu, avšak hlas byl stále srozumitelný. V druhé části byla priorita pro rozsah portů 3783-3784 přenastavena na prioritu Video (VI), poté se chybovost již neopakovala.




*Obrázek 78: Nastavení priorit BE/VO*

### 8.3.5 Test 5

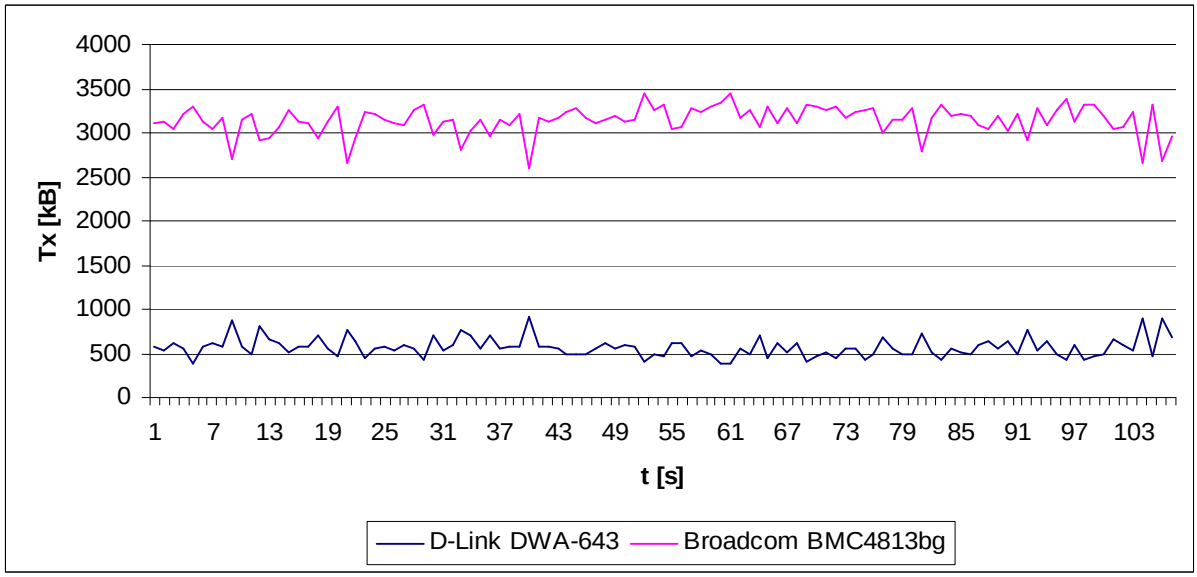
V tomto testu byly použity dvě nejvyšší priority a to tedy Voice (VO) a Video (VI). Klientskému počítači Acer byla pro rozsahy portů 1-80 a 3783-3784 přiřazena priorita Voice (VO) a druhém počítači HP Compaq priorita Video (VI) pro celý rozsah portů. Následující graf dokazuje, že priority Video a Voice nemají mezi sebou takový rozdíl. Počítač HP má po celou dobu stahování více jak šestkrát vyšší rychlost než počítač Acer. Důvodem těchto bude již zmíněná vyšší výkonnost bezdrátového zařízení Broadcom a neschopnost bezdrátového přístupového bodu priorizovat spolu s datovým tokem i bezdrátový přístup slabšího zařízení D-Link DWA-643. Uskutečněný hovor vykazoval minimální problémy. Zřídka se vyskytla chyba nebo přeskočení hlasu.




*Obrázek 79: Nastavení priorit VO/VI*

### 8.3.6 Test 6

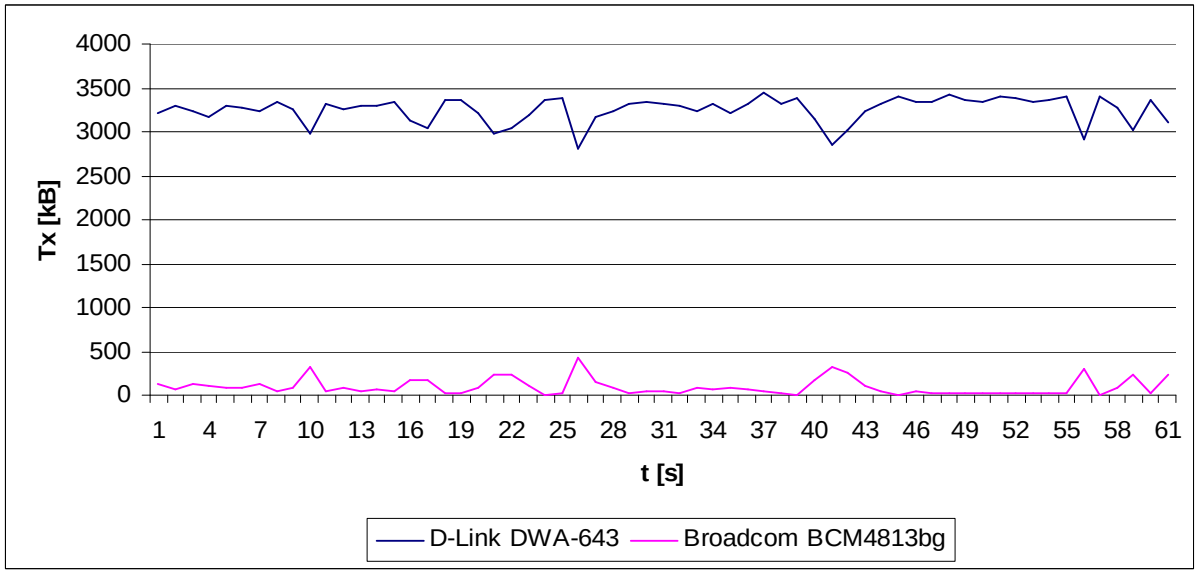
V tomto testu byly priority obou zařízení v tabulce přístupového bodu prohozeny. Klientský počítač Acer se zařízením D-Link DWA-643 měl přidělenou prioritu Video (VI) pro oba rozsahy portů 1-80 a 3873-3874 a počítač HP s bezdrátovým chipem Broadcom BCM4813bg pro celý rozsah portů 1-65535 prioritu Voice (VO). Výsledná závislost však ukazuje, že nastavení nemá na datovou propustnost příliš velký dopad, graf je velice podobný grafu z předešlého měření. Testovací hovor opět vykazoval občasné chyby a problémy při přenosu. Po většinu doby trvání měření byl hovor kvalitní a komunikace bez chyb. Po přenastavení priority pro rozsah portů 3783-3784 na Voice (VO) byl hovor zcela stabilní a bez problémů.




*Obrázek 80: Nastavení priorit VI/VO*

### 8.3.7 Test 7

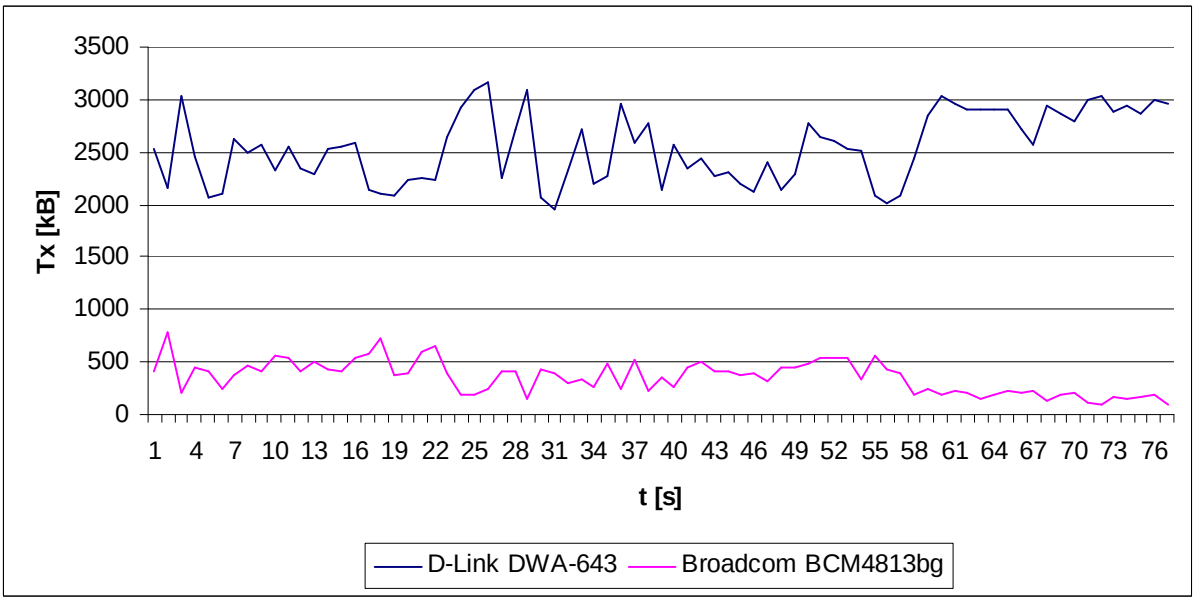
V následujících testech bylo místo testovacího hovoru použito streaming videa pomocí programu VLC. Video bylo formátu „avi“ v kvalitě HDTV. Streaming byl vysílán počítačem připojeným na bezdrátový přístupový bod pomocí protokolu UDP na portu 1234 a přijímáno klientským počítačem Acer se zařízením D-Link DWA-643. Oba dva počítače měly během měření aktivní stahování 80GB souboru po protokolu http a portu 80 pro vytížení sítě. U prvního testu bylo nastavení prioritizace sítě následující – počítač Acer měl pro rozsah portů 1-80 nastavenou prioritu Video (VI) a pro rozsah 1233-1234 prioritu Voice (VO), druhý počítač měl pro celý rozsah portů 1-65535 nastavenou prioritu Background (BK). Přenos videa byl po celou dobu měření bez jediného zamrznutí obrazu. Následující graf prezentuje závislost rychlosti přenosu dat na čase měření. Hodnoty velikosti rychlosti přenosu klientského počítače HP s bezdrátovým zařízením Broadcom se často blíží nule.




*Obrázek 81: Nastavení priorit VI(VO)/BK*

### 8.3.8 Test 8

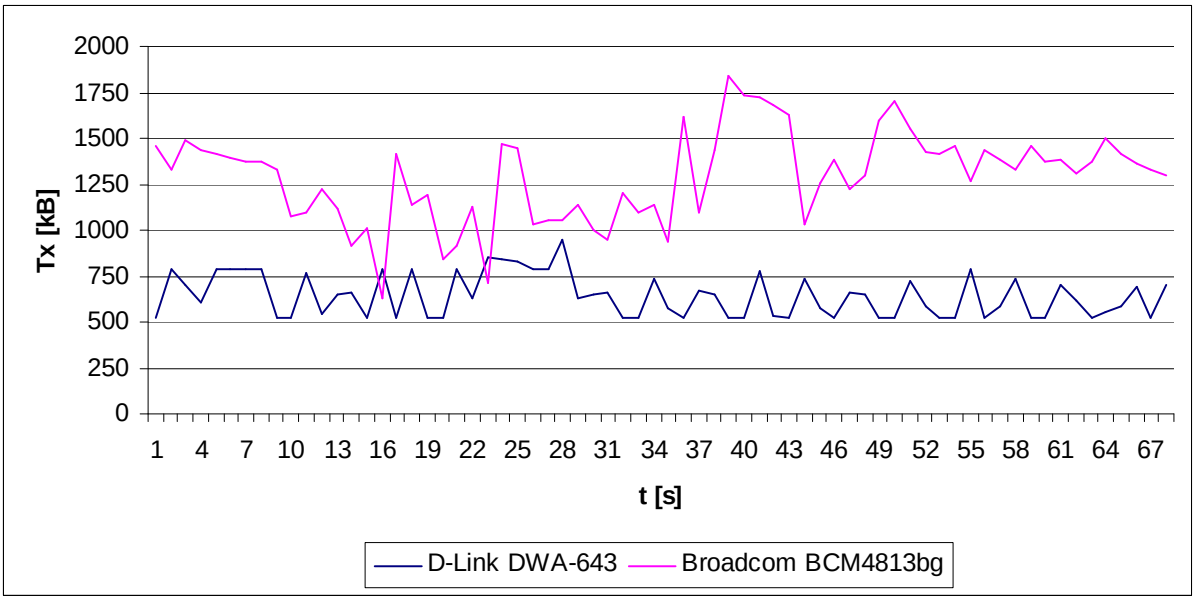
V tomto testu byla priorita klientského počítače pro port přenosu videa 1234 ponechána na úrovni Voice (VO) a pro přenos souboru port 80 na prioritě Video (VI), ovšem priorita druhého počítače HP byla z nejnižší možné posunuta na vyšší příčku, a sice na úroveň Video (VI). V následujícím grafu je vidět zvýšení rychlosti počítače HP a mírné snížení přenosové rychlosti downloadu počítače Acer. Streaming video souboru opět probíhal bez chyb a výpadků.




*Obrázek 82: Nastavení priorit VI(VO)/VI*

### 8.3.9 Test 9

U tohoto testu byla priorita Voice (VO) nastavena druhému klientskému počítači pro rozsah portů 1-65535. Počítači Acer byla pro rozsah portů pro přenos souboru 1-80 přiřazena priorita Background (BK) a pro rozsah portu 3783-3784 pro přenos videa protokolem UDP priorita Best Effort (BE). V grafické závislosti se objevuje výrazné snížení přenosové rychlosti. Během streamování videa docházelo k častým přeskokům a výpadkům. Toto nastavení se pro sledování streamovaného videa ukázalo být zcela nevyhovující.




*Obrázek 83: Nastavení priorit BK(BE)/VO*

# ZÁVĚR

Celá rodina standardů 802.11 už od svého vzniku v roce 1999 neustále nabírá na popularitě. Svou funkcí a vlastnostmi ohromila nespočetné množství uživatelů a i přes své nedostatky jsou zařízení podporující tento standard neustále častěji instalované do míst, kde není možné instalovat sít metalickou. Postupem času, se poptávka po bezdrátových zařízeních zvětšila. To bylo způsobeno především většími nároky na mobilitu. Právě především potřeba mobility je jedním z nejzásadnějších faktorů, který se podílí na vzniku nových úprav a standardů. Všechny standardy rodiny standardů 802.11 svým vznikem vytvořili revoluci v mobilitě a možnostech bezdrátového připojení.

Kromě svých pozitivních vlastností, mají na druhou stranu i vlastnosti, které nemusí být pro kvalitní bezdrátový přenos přínosem. Jsou to zejména nedostatky v zabezpečení, schopnosti odolávat vlivům rušení a podpoře kvality služeb. V současné době jsou proto tyto standardy pomalu nahrazovány novějšími, jejichž metody se na tyto nedostatky a chyby speciálně zaměřují. Jedním z těchto standardů je 802.11n. Disponuje technologií MIMO, která spočívá v použití více antén. Tím se snaží o dosáhnutí vysokých přenosových rychlostí a přenosů, které budou odolávat vlivům rušení a špatným podmínkám prostředí. Byl navržen tak, aby splňoval nejnáročnější požadavky na síť. Maximální teoretická hodnota přenosové rychlosti je až 600MB/s. Výhodou je také fakt, že standard je schopný provádět zpětnou kompatibilitu se staršími standardy rodiny 802.11, pro případ že některé zařízení v sítí standard 802.11n nepodporuje.

S druhým zmíněným standardem 802.11e přicházejí důležité změny. Standard 802.11e do světa bezdrátových sítí přináší velké úpravy a vylepšení. Především pomocí technik hybridní koordinační funkce EDCA a HCCA se mnohonásobně zvyšuje kvalita správy kvality služeb QoS. Tím tento standard výrazně napomáhá k dosáhnutí schopností metalické sítě.
Sepisováním této práce jsem získal poznatky z oboru bezdrátových sítí a hlouběji jsem pronikl do principů a funkcí známých norem. V práci se mi podařilo porovnat standardy, které se v současnosti skrývají pod pojmem bezdrátové technologie a shrnut problematiku jednotlivých standardů uvedených institutem IEEE (*Institute of Electrical and Electronics Engineers*) za spolupráce organizace Wi-Fi Alliance.

Vypracování praktické části ozřejmuje chování standardů 802.11n a 802.11e v praxi. Ve srovnání s teoretickými předpoklady, standard 802.11n nepředstavuje výrazné zlepšení v problematice rušení. V testech se standard představil jako dosti nespolehlivý a velmi náchylný k negativním vlivům rušení. V případě použití prvků podporující pouze standard 802.11n se maximální přenosová rychlost přibližovala rychlosti sítě Fast Ethernet. Teoretické hodnotě 300Mbit/s se však ani jednou během měření nepřiblížila. U měření velikosti odezvy jsem rovněž nezaznamenal výrazné zlepšení. Naopak v grafech se objevují značné výkyvy lišící se v řádech. U testů zpětné kompatibility, při použití zařízení 802.11n a 802.11g současně je standard 802.11n pro kvalitní přenos nepoužitelný. Maximální hodnoty přenosové rychlosti nesplňovali ani ty nejmenší požadavky. Testy standardu 802.11g dokázali, že starší standard je spolehlivější, stabilnější a je výhodný pro použití jak v otevřených, tak v uzavřených prostorách.

Testy standardu WMM většinou souhlasili s teoretickými předpoklady. Objevují se však i odchylky, které budou pravděpodobně během dalších úprav specifikací opraveny.

## SEZNAM POUŽITÉ LITERATURY:


[1] Gast, Matthew. *802.11 Wireless Networks: The Definitive Guide*. 2nd ed. O'Reilly Media, Inc., 2005. 688 s. ISBN 0-596-10052-3.

[2] Ganz, Aura; Ganz, Zvi; Wongthavarawat, Kitti; *Multimedia Wireless Networks: Technologies, Standards and QoS*. Prentice Hall PTR, 2003. 352 s. ISBN 0-13-046099-0.

[3] Prasad, Anand; Prasad, Neeli; *802.11 WLANs and IP Networking: Security, QoS, and Mobility*, Artech House, 2005. 621 s. ISBN 1-58053-789-8.

[4] ZANDL, Patrick. *Bezdrátové sítě Wi-Fi : Praktický průvodce.* Vydání první. Brno : Computer Press, 2003. 176 s. ISBN 80-7226-632-2.

[5] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi.* Vydání první. Brno : Computer Press, 2004. 171 s. ISBN 80-251-0346-3.

[6] Torrieri, Don; *Principles of Spread-Spectrum communication systems*, Springer Science & Business Media, Inc., 2005. ISBN 0-387-22783-0.

[7] Fazel, Khaled; Kaiser, Stefan; *Multi-Carrier and Spread Spektrum Systems*, John Eley & Sons Ltd, The Atrium, Southern Gate, Chichester, 2003. 382 s. ISBN 0-470-84899-5.

[8] ANSI/IEEE Std 802.11, 1999 Edition [online]. [cit 2008-10-18]. Dostupný z WWW: http://standards.getieee.org/getieee802/download/802/download/802.11-1999.pdf

[9] 802.11n: The Next Generation of Wireless Performance, 2007 Edition [online]. [cit 2008-11-15]. Dostupný z WWW: http://www.cisco.com/en/US/prod/collateral/ wireless/ps5678/ps6973/ps8382/prod_white_paper0900aecd806b8ce7.pdf

[10] 802.11n Wireless Technology Overview, 2007 Edition [online]. [cit 2008-11-15]. Dostupný z WWW: http://www.cisco.com/en/US/prod/collateral/ wireless/ps5678/ ps6973/ps8382/prod_brochure0900aecd806b8a92.pdf

[11] 802.11n: Next-Generation Wireless LAN Technology, 2006 Edition [online]. [cit 2008-11-16]. Dostupný z WWW: http://www.broadcom.com/docs/WLAN/ 802_11n-WP100-R.pdf/

[12] Providing QoS in WLANs: How the IEEE 802.11e Standard QoS Enhancements Will Affect the Performance of WLANs, 2004 Edition [online]. [cit 2008-11-28]. Dostupný z WWW: http://download.intel.com/network/connectivity/resources/ doc_library/white_papers/30376201.pdf

[13] Jahanzeb, Faroog; Rauf, Bilal. *Implementation and Evaluation of IEEE 802.11e Wireless LAN in GloMoSim*. Švédsko, 2006. 112 s. , 0 Department of Computing Science Umeå University Sweden. Vedoucí oborové práce Thomas Nilsson.

[14] Wi-Fi CERTIFIED™ for WMM™ – Support for Multimedia Applications with Quality of Service in Wi-Fi Networks, 2004 Edition [online]. [cit 2008-12-10. Dostupný z WWW: http://www.wifi.org/files/wp_1_WMM% 20QoS%20In%20Wi-Fi_9-1-04.pdf

[15] Wi-Fi CERTIFIED™ for WMM™ – Support for Multimedia Applications with Quality of Service in Wi-Fi Networks, 2004 Edition [online]. [cit 2008-12-10. Dostupný z WWW: http://www.cpx.cz/dls/WMM.pdf