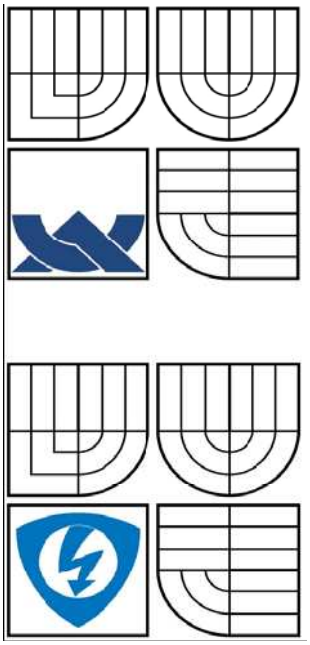


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION DEPARTMENT OF TELECOMMUNICATIONS

MODERNÍ BEZDRÁTOVÉ TECHNOLOGIE - 802.11n

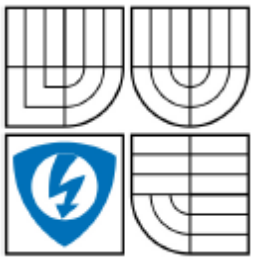
MODERN WIRELESS TECHNOLOGY – 802.11n

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
FRANTIŠEK BEDNÁŘ

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. MICHAL SKOŘEPA

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: František Bednář ***ID:*** 98666
Ročník: 3 ***Akademický rok:*** 2008/2009

NÁZEV TÉMATU:

Moderní bezdrátové technologie - 802.11n

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte problematiku bezdrátové sítové technologie IEEE 802.11n. Proveďte srovnání této technologie s ostatními standardy 802.11 a uveďte její přínosy. Dále se seznamte se simulačním prostředím OPNET Modeler. Proveďte implementaci existujících modelu 802.11n do prostředí OPNET Modeler. Vytvořte simulaci porovnávající technologie 802.11a/b/g/n z hlediska přenosu dat v reálném čase, především streamovaného videa ve vysokém rozlišení.

DOPORUČENÁ LITERATURA:

[1] Perahia, Eldad; Stacey, Robert. Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n, Cambridge University Press, 2008, 416 s., ISBN: 978-0521885843.

[2] H. Walke, Bernhard; Mangold, Stefan; Berlemann, Lars. IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence, Wiley, 2007, 402 s., ISBN: 978-0470014394.

Termín zadání: 9.2.2009 ***Termín odevzdání:*** 2.6.2009

Vedoucí práce: Ing. Michal Skořepa

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

Anotace:

Tato práce popisuje nový standard IEEE 802.11n pro bezdrátové sítě. Práce obsahuje dvě části teoretickou a praktickou. Teoretické znalosti, poznatky a hlavně porozumění dané problematiky bude využito u návrhu a simulace sítě.

Teoretická část pojednává o funkcích a metodách, které tento standard přebírá ze starších standardů 802.11a, 802.11g a také o nových a součástech, které mají výrazně zvýšit přenosovou rychlost a propustnost na MAC vrstvě. Rychlosti sítí vytvořené na základu 802.11n budou srovnatelné se sítěmi Ethernet. Hlavní součást, která výrazně zvyšuje rychlost na fyzické vrstvě je použití vícenásobných antén MIMO a použití kanálu o šířce 40MHz. Na MAC vrstvě bude přidána agregace rámců, která způsobí přibližně lineární závislost propustnosti na MAC vrstvě na datovém toku na fyzické vrstvě.

V praktické části se pak budeme věnovat simulaci streamového videa ve vysokém rozlišení v bezdrátových sítích jednotlivých standardů. Tato část obsahuje návrh a popis konfigurace jednotlivých komponent sítě. Vytvořením několika duplicitních scénářů, budeme moci srovnat výsledky simulací jednotlivých standardů

Klíčová slova:

IEEE 802.11n, vysoká propustnost, MIMO technologie, OFDM , WLAN, agregace rámců, 40 MHz kanál, blokové ACK

Abstract:

This work describes new standard 802.11n for wireless network. The work contains two parts: theoretical and practical. Theoretical knowledge and understanding our problems will be used in design and simulation wireless network.

Theoretical part will discuss about function and methods, which the standard picking over from older standard 802.11a, 802.11g a about new features, that should raise transmission data rate and throughput on MAC sublayer dramatically. Data rate of networks based on standard 802.11n will be comparable with Ethernet networks. Main features that increase data rate on PHY layer is method of multiple antennas calls MIMO and use 40 Mhz channel. On MAC layer will be add frame aggregation that cause linear dependent of throughput on MAC layer and data rate on PHY layer.

In practical part we will pay attention simulation of stream video high definition in wireless network. This part contain design and components configuration in network. We will be able to compare simulation results individual standards, by creation of several duplicate scenarios.

Keywords:

IEEE 802.11n, high throughput (HT), MIMO, OFDM, WLAN, frame aggregation, 40 MHz channel, block ACK

.

BEDNÁŘ, F. *Moderní bezdrátové technologie - 802.11n.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 56 s. Vedoucí bakalářské práce Ing. Michal Skořepa.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Moderní bezdrátové technologie - 802.11n“ 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 bakalářské 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

Chci poděkovat vedoucímu mé bakalářské práce Ing. Michalu Skořepovi za účinnou metodickou, pedagogickou a odbornou pomoc při zpracování mé kvalifikační práce.

V Brně dne . . . .
(podpis autora)

Seznam obrázků:

Seznam tabulek:

1. Úvod:

Protože se bezdrátové technologie stávají čím dál více oblíbenější a rozšiřovanější, jsou také jejich uživatelé náročnější. Nároky na rychlost sítí se zvětšují díky stále náročnějším aplikacím. V dnešní době se hodně populární stává vysílání ve vysoké kvalitě HDTV, nebo IPTV (Internet Protocol TeleVision). Služby HDTV můžou spotřebovat až 20 Mbit/s. Bezdrátová technologie 802.11n by mohla také způsobit průlom a rozšíření tzv. Wi-Fi telefonie. Proto je již od roku 2003 ve vývoji standard 802.11n, který by měl přinést rychlosti srovnatelné se sítěmi Ethernet. Hlavními rysy standardu 802.11n, bude zvýšení propustnosti na MAC vrstvě, které budou způsobeny různými modifikacemi a novými funkcemi, které budu popisovat v této práci. Důležitou technologii, kterou tento standard využívá, je technologie MIMO. Pomocí několikanásobných antén na přijímací a vysílací straně dosáhneme významného nárůstu rychlosti na fyzické vrstvě. Momentálně, byl v listopadu 2008, schválen Draft 7.0, který byl vytvořen vývojovou skupinou TGn Sync. Datum plného schválení standardu je stále odkládáno, ale mnoho zařízení už je nyní certifikováno a v prodeji. Z cen za které se tyto zařízení prodávají je vidět, že technologie 802.11n bude určena široké skupině uživatelů. Tento standard bude určen, jak pro menší domácí sítě např. ke sledování HDTV, tak i pro rozlehlejší firemní sítě. Vývojáři slibují, že propustnost tohoto standardu bude zvládat současné užívání náročných aplikací, jako HDTV, online gaming, streamových Hi-Fi zařízení atd. Standard je také vyvíjen s ohledem na kapesní přístroje, jako jsou PDA, mobilní telefony atd. Protože kapesních přístrojů s podporou Wi-Fi neustále přibývá a také přibývá veřejných Hot-Spotů, kde se člověk může bezplatně připojit, vývojáři aplikovali různé úsporné režimy, aby připojení pomocí Wi-Fi bylo co nejméně energeticky náročné.

2. Standardy 802.11

Standard 802.11n sice používá nové metody a technologie, ale jsou zde zaměstnány i metody převzaté, nebo pouze vylepšené ze starších standardů jako 802.11a nebo 802.11g. Proto se nejdříve seznámíme s těmito staršími standardy, jaké používají přenosové metody, modulace, kódování, zabezpečení atd.

2.1 Historie vývoje 802.11

V roce 1997 byl institutem IEEE vydán a schválen standard 802.11. Byl to standard pro bezdrátové sítě pracující v pásmu ISM. [3] Měl sloužit jako alternativní řešení při návrhu sítí uvnitř budov. Na počátcích vývoje tento standard dosahoval nízkých přenosových rychlostí, které se pohybovali okolo 2 Mbit/s. Postupem času docházelo k vylepšování stávajícího standardu a vydávání doplňků k tomuto standardu. První dva standardy byly vydány v roce 1999. Byl to standard 802.11b, který dosáhl navýšení rychlosti na 11 Mbit/s a standard 802.11a, který byl vytvořen pro používání v pásmu 5 GHz. Poprvé byla v tomto standardu použita modulace OFDM, pomocí které došlo k navýšení rychlosti na 54 Mbit/s. Při vývoji tohoto standardu se počítalo i s použitím ve venkovních prostorách. Protože pásmo 5 GHz, není ve všech státech volné, byl v roce 2003 vydán standard 802.11g, který pracuje v pásmu 2,4 GHz a dosahuje stejných přenosových rychlostí jako 802.11a. Do dnešní doby bylo vydáno ještě mnoho dalších doplňků ke standardu 802.11. Srovnání rychlostí jednotlivých doplňků standardu 802.11 je zobrazeno v tab. 2.1.

Tab. 2.1: Přehled standardu IEEE 802.11 a srovnání přenosových rychlostí a způsobů kódování

Přehled standardu IEEE 802.11				
Standard	Frekvence	Max. teoretická přenosová rychlost	Průměrná skutečná rychlost	Použité kódování
	GHz	Mbit/s	Mbit/s	
802.11	2,4	2	0,9	FHSS/DSSS/IrDA
802.11a	5	54	23	OFDM
802.11b	2,4	11	6	DSSS
802.11g	2,4	54	19	OFDM/DSSS
802.11n	2,4 nebo 5	až 540	-	MIMO-OFDM

2.2 Doplňky standardu 802.11

IEEE 802.11a

Vylepšení této verze spočívá v přechodu do pásma 5 GHz, aby nedocházelo k rušení s ostatními přístroji (mikrovlnné trouby, mobilní telefony, technologie Bluetooth),

které pracují v pásmu 2,4 GHz. Přenosová rychlost na fyzické vrstvě byla navýšena na 54 Mbit/s, hlavně také díky použití OFDM. Díky většímu vyzařovacímu výkonu se používá pro přenos na větší vzdálenosti.

IEEE 802.11b

Tento standard využívá stejně jako 802.11 pásmo 2,4 GHz, ale k přenosu na fyzické vrstvě už využívá pouze modulaci DSSS. Podle momentálního zarušení kanálu může měnit rychlost od 1 Mbit/s až na 11 Mbit/s.

IEEE 802.11d

Standard je používaný v zemích, kde nejsou povoleny jiné dodatky k IEEE 802.11 standardu. Definuje požadavky na fyzickou vrstvu k uspokojení regulačních domén nepokrytých existujícími standardy. Liší se v povolených frekvencích, vyzařovacích výkonech a propustnosti signálu [11].

IEEE 802.11e

Vylepšuje MAC podvrstvu zavedením podpory kvalitu služeb QoS. Tento standard je průlomem, používání aplikací citlivých na zpoždění v bezdrátových sítích. Zavádí novou koordinační funkci HCF, která používá k přístupu k médiu metody HCCA a EDCA. HCCA je přístupová metody pro přístup ke kanálům řízená HCF a EDCA je vylepšená DCF přístupová metoda ke kanálům.

IEEE 802.11h

Řeší problémy rušení od ostatních zařízení pracujících na frekvenci 5 GHz. Tento standard omezuje svůj vysílací výkon, nebo dokonce přeruší vysílaní na kanále, na kterém rozpoznal rušení. Rušení v tomto pásmu můžou způsobovat např. radary nebo některé satelitní systémy. Dynamickým výběrem kanálu dosahuje kvalitnějšího příjmu signálu.

IEEE 802.11n

Tento nejnovější standard ještě není plně schválen, aktuálně je schválený Draft 7.0. Hlavními vlastnostmi budou změny na MAC vrstvě, aby se přenosové rychlosti mohly vyrovnat sítím Ethernet. Bude využívat technologii MIMO, pro vysílání až na čtyřech prostorově oddělených kanálech. Bude používat stejně jako standardy 802.11g a 802.11a přenosovou metodu OFDM a na fyzické vrstvě by měla dosahovat rychlostí až kolem 540 Mbit/s. Užití najde především u aplikací potřebující velkou šířku pásma, kde se uplatňuje zajištění kvality používaných služeb QoS. To můžou být například služby IPTV nebo HDTV.

Skutečné dosahované rychlosti vrstvě bývají skoro poloviční oproti maximálním rychlostem, které udává výrobce. To je způsobeno mnoha faktory. Úbytek rychlosti na

fyzické vrstvě ovlivňují faktory jako místní zarušení, vliv počasí, překážky na signálové cestě a samozřejmě také vzdálenost mezi přijímačem a vysílačem.

Další ztráty vznikají na linkové vrstvě, která má určitou propustnost. Tato vrstva má určitou režii, která je oproti metalickým sítím výrazně vyšší a zabírá téměř 30-40% kapacity. Svou vlastní režii má také přenosový protokol TCP/IP. Také dochází ke zpoždění, které důsledkem toho, že WiFi sítě jsou poloduplexní, tzn.: že vysílač nemůže v jeden okamžik vysílat a přijímat data od klienta. Plný duplex by byl teoreticky možný, ale za cenu dvojnásobné šířky pásma.

2.3 Přenosové metody:

IrDA(Infrared Data Association):

Tento přenos využívá ke komunikaci infračerveného pásma. Nevýhodou je, že je nutná přímá viditelnost.

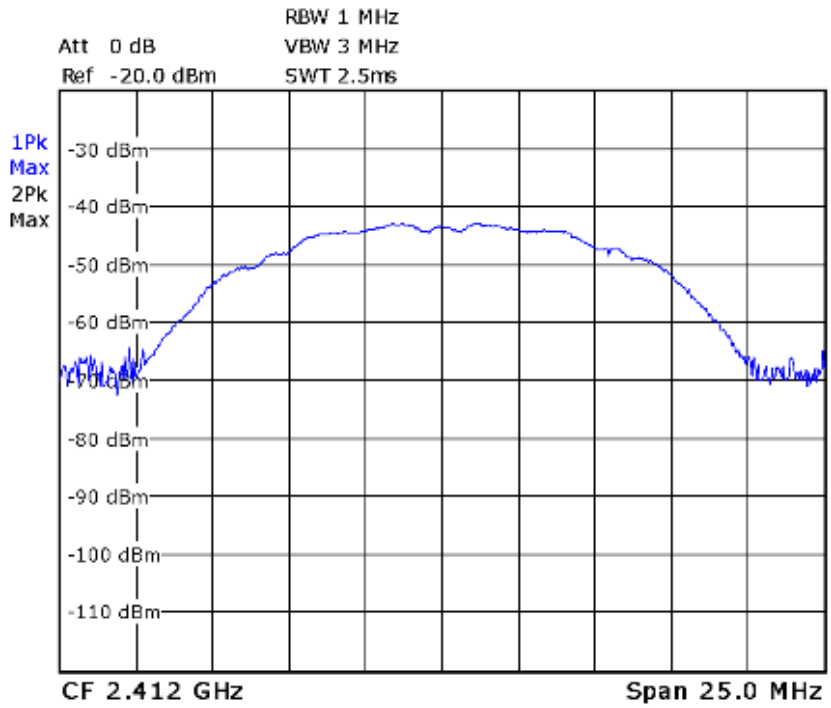
Pro zajištění vícebodového spoje se používá dvou metod:

- Rozptýlený (diffused) mód- síť je tvořena pouze bezdrátovými stanicemi a prostředím odrážející infračervené paprsky. Nevýhodou je vysoký vysílaný výkon a možné interference.
- Směrovaný (directed) mód – síť je tvořena pouze stanicemi vysílajícími signál soustředěný v úzkém paprsku a přijímači, které jsou schopny signál přijmout pouze v úzkém prostorovém úhlu. Ještě obsahují translanční bod, který zajišťuje šíření signálu do všech směrů, kde se můžou vyskytovat přijímací stanice.

Použité modulace: OOK (On-Off Keying), PMM (Pulse-position modulation), modulace nosné PSK, FSK.

DSSS (Direct Sequence Spread Spectrum)

Tato metoda je založena na rovnoměrném rozložení vysílaného signálu v celé šířce pásma kanálu, jak vidíme na obr. 2.1. Používá se k tomu matematické kódování. Každý vysílaný bit je nahrazen n-bitovou (chipovou) pseudonáhodnou sekvencí. Nejčastěji se používá Bakerovo kódování. Tím je do přenášené informace přidána redundance, která zajistí větší robustnost přenášeného signálu a tím tak zamezí vzniku chyb na přenosovém kanále. Použitím pseudonáhodného kódu pro rozprostření spektra se stane pro ostatní objekty v síti signál bez znalosti rozprostíracího kódu nečitelný. Je velmi důležité přijímač a vysílač správně zasynchronizovat, aby došlo k správnému derozprostírání. Hlavní výhodou této technologie rozprostřeného spektra je, že je odolná vůči úzkopásmovým rušením.



Obr. 2.1: Frekvenční spektrum DSSS signálu [3]

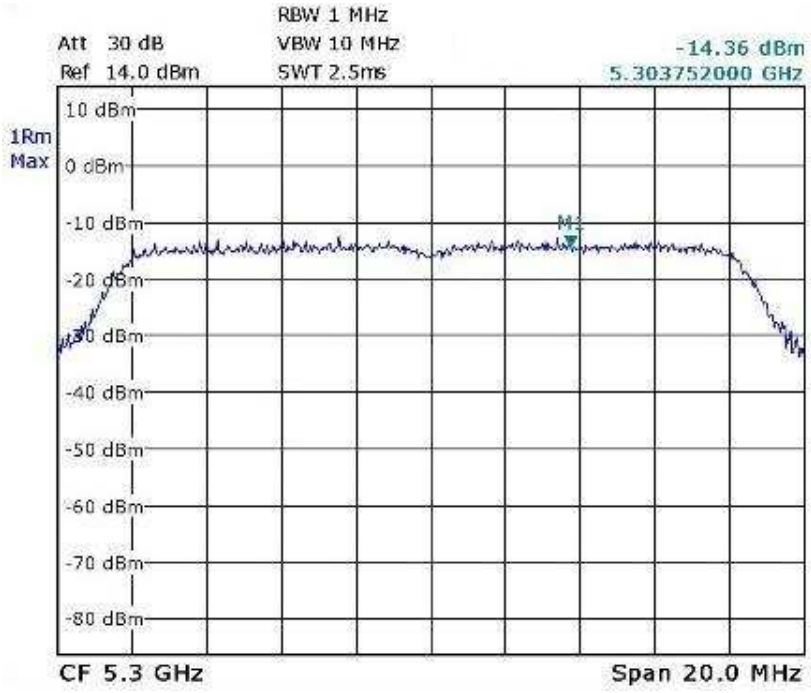
V ČR je v bezlicenčním pásmu vyhrazeno pro WiFi technologie 13 kanálů, které jsou umístěny v pásmu 2402 – 2482 MHz. Kanály se navzájem překrývají. Odstup jejich nosných je 5 MHz. Každý kanál má rozsah 22 MHz, a aby se sousední kanály neovlivňovaly, musí být jejich odstup 25 MHz. Z toho vyplívá, že v pásmu 2402 – 2482 se vejdou pouze tři nepřekrývající se kanály. Podle rychlosti je vybrána vhodná modulace. Pro rychlost 1 Mbit/s se používá BPSK, pro 2 Mbit/s se moduluje pomocí QPSK a při použití rychlostí 5,5 a 10 Mbit/s je využívána modulace CCK.

FHSS (Frequency hopping spread spectrum)

Celé pásmo o šířce 83,5 MHz je rozděleno na 79 kanálů o velikosti 1 MHz, zbytek pásma slouží jako ochrana proti interferencím ze sousedního pásma. Vysílač pak skáče v pseudonáhodném pořadí mezi jednotlivými kanály a na každém vysílá krátký datový tok. [10] Opět je nutná správná synchronizace, přijímač musí znát pseudonáhodnou posloupnost, pomocí které vysílač mění vysílací frekvenci. Tím, že vysílač rychle mění frekvenci nosné, se pak spektrum jeví, jakoby v daný moment obsahovalo mnoho frekvencí, i když je jasné, že vždy je v daný moment vysíláno pouze na jedné nosné. Vysílač by měl za 30 sekund vystřídat 75 kanálů a na každém vysílat maximálně po dobu 400 ms. [10] Výhodou tohoto systému je to, že na určitém území může pracovat více zařízení, která se nebudou ovlivňovat. V bezdrátových sítích už se téměř nevyužívá. Použití např. v systému Bluetooth.

OFMD (Orthogonal Frequency Division Multiplex)

Tuto metodu používají standardy 802.11a v pásmu 5 GHz a 802.11g v pásmu 2,4 GHz a také nový standard 802.11n, v kombinaci s technologií MIMO. Používá se pro vysokorychlostní přenos pomocí systému ortogonálního frekvenčního multiplexu. Ortogonalita jednotlivých subkanálů zajišťuje, že se navzájem neovlivňují. Metoda OFDM rozdělí kanál o šířce 20MHz do 52 subkanálů, ze kterých je 48 využito pro přenos dat a zbývající subkanály nesou pilotní sekvenci. Spektrum signálu vidíme na obr. 2.2.



Obr. 2.2: Frekvenční spektrum OFDM signálu [3]

Každý ze subkanálů je modulován pomocí vícestavové kvadraturní amplitudové modulace (QAM) nebo modulací s klíčováním fázovým posuvem (PSK) [3]. Vliv použité modulace na přenosovou rychlost vidíme v tab. 2.2. Soubor 52 subkanálů představuje jeden OFDM symbol, ke kterému se přidává ochranný interval GI, který zamezuje ovlivnění přijímaného signálu nežádoucími odraženými signály.

Tab. 2.2: Přehled používaných modulací a srovnání přenosových rychlostí

Přehled podporovaných rychlostí 802.11g v závislosti na použité modulaci	
16-QAM	54, 48, 36, 24 Mbit/s
QPSK	18,12 Mbit/s
BPSK	9, 6 Mbit/s
DSSS	11, 5.5, 2, 1 Mbit/s

2.4 Vrstvový model:

Obdobně jako u ostatních síťových zařízení a protokolů, vycházejí bezdrátové sítě založené na standardech 802.11 z referenčního modelu ISO/OSI. Standardy 802.11 jsou definovány na prvních dvou vrstvách tohoto modelu. Strukturu vrstvového modelu vidíme na tab. 2.3.

Tab. 2.3: Vrstvový model standardu 802.11

Spojová vrstva	LLC					
	IEEE 802.11 MAC					
Fyzická vrstva	IEEE 802.11 IR	IEEE 802.11 DSSS	IEEE 802.11 FHSS	IEEE 802.11a OFDM	IEEE 802.11b HR-DSSS	IEEE 802.11g OFDM

2.4.1 Fyzická vrstva:

Je to vrstva, která se nachází na dně vrstvového modelu. Jejím úkolem je připravit data k přenosu po bezdrátovém mediu a samozřejmě se také stara o samotný příjem a vysílání dat po bezdrátovém mediu. Zajišťuje zvolení správné modulace a kódovacího schématu na základě stavu přenosového kanálu.

Ve všech standardech 802.11 je fyzická vrstva rozdělena do dvou podvrstev:

- **PMD (Physical Medium Dependent)**
- **PLCP (Physical Layer Convergence Procedure)**

Podvrstva PMD:

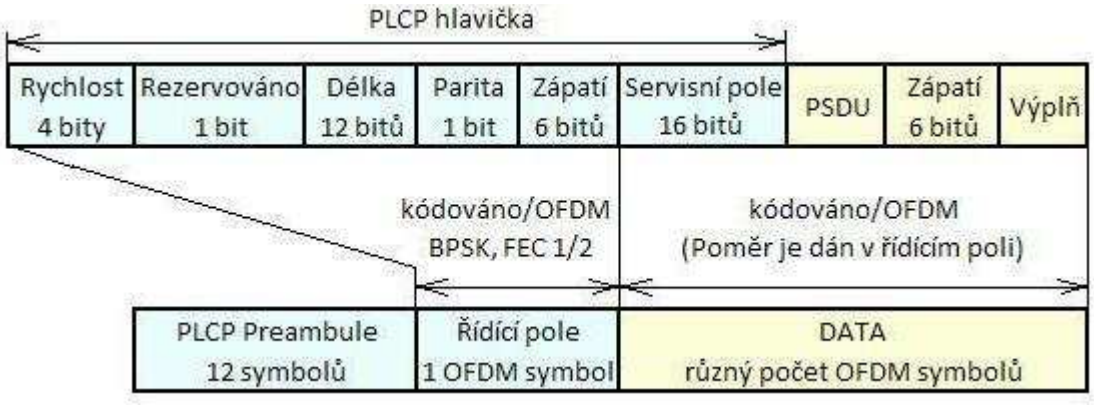
Podvrstva funkcí závislých na fyzickém médiu zajišťuje funkce spjaté se samotným radiovým přenosem. Má na starosti modulaci a demodulaci signálu. Určuje velikost vysílaného signálu a nastavuje vysílací frekvenci.

Podvrstva PLCP:

Na podvrstvě konvergenčních procedur fyzické vrstvy se k MAC rámcům přikládají informace o typu modulace a použité přenosové metodě. [3] Dále tato vrstva zajišťuje synchronizaci, identifikuje začátek rámce a zavádí prostředky pro zamezení výskytu chyb. Hlavní výhoda této vrstvy spočívá v tom, že přenášené rámce se tak stanou nezávislými na typu fyzické vrstvy.

Struktury podvrstev PLCP jednotlivých doplňků standardu se liší. Nebudu zde uvádět všechny, ale zmíním strukturu, kterou používá standard 802.11g, protože k ní má 802.11n nejblíže.

Přenos probíhá ve formě PPDU rámců. Tento rámec začíná polem preambule, pak následuje řídící pole a nakonec samotná data, jak vidíme na obr. 2.3 [3].



Obr. 2.3: Struktura rámce PPDU

Složení PPDU rámce:

- **PLCP preambule** – je tvořena dvanácti OFDM symboly. Z toho prvních deset je krátkých s trváním 0,8 µs. Zbylé dva symboly jsou dlouhé a trvají 4 µs [3].
- **PLCP hlavička** - první část o délce 24 bitů je součástí řídícího pole. Řídící pole trvá jeden OFDM symbol a je fixně kódován modulací BPSK s kódovým poměrem 1/2 (kódový poměr je poměr mezi užitečným počtem bitů a celkovým počtem, který zahrnuje i redundanci). Řídící pole obsahuje pole rychlost, které udává jakou rychlostí a jakou modulací bude přenášena datová část. Důležité je také pole délka, které udává délku přenášených dat v bajtech. Druhá část PLCP hlavičky je přenášena v poli data a je pojmenována servisní pole. Tato část má délku 16 bitů a je přenášena volitelnou datovou rychlosti a kódovým poměrem, podle toho co je uvedeno v poli rychlost. Prvních šest bitů je nastaveno na logickou nulu a slouží k synchronizaci při descramblování v přijímači. Zbylé bity jsou rezervovány pro pozdější použití.
- **DATA** – v této části jsou přenášena uživatelská data z vyšších vrstev, servisní informace, zápatí a výplň [3]. Datová část je přenášena přenosovou rychlostí a kódovacím poměrem uvedeným v poli rychlost.

2.4.2 Spojová vrstva:

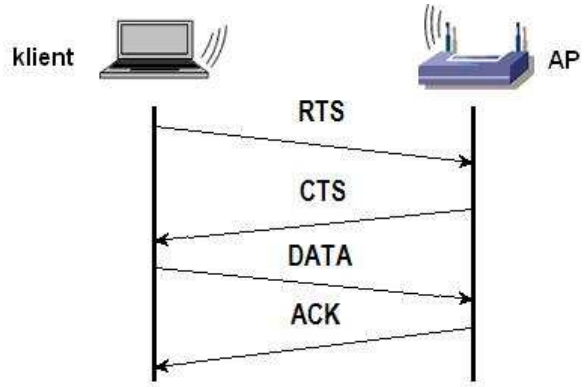
Podvrstva MAC:

Jak vyplývá z názvu, stará se o ovládání přístupu k médiu. Tvoří vlastně rozhraní mezi fyzickou vrstvou a hostitelskými zařízeními. Používá metodu mnohonásobného přístupu ke sdílenému médiu CSMA/CA. V odborných textech je tato metoda také označována jako DCF (Distributed Coordination Function). Je to základní metoda a je založena na principu detekce nosné a předcházení kolizím, na rozdíl od CSMA/CD která kolize detekuje. V bezdrátových sítích nelze použít CSMA/CD z toho důvodu, že tato metoda

potřebuje plně duplexní kanál a jak již víme komunikace u bezdrátových sítí je poloduplexní.

Vysílací stanice před samotným vysíláním poslouchá na společném mediu a zkoumá, jestli je volné nebo obsazené. Pokud je medium volné, vysílač vygeneruje náhodný časový interval a po jeho uplynutí může začít vysílat. Pokud je medium obsazeno, nebo nedošlo k úspěšnému přijetí dat u přijímače, po uplynutí náhodného intervalu zahájí vysílač exponenciální čekání a znovu se pokusí o přístup k médiu. Vygenerovaný interval se při neúspěšných pokusech zdvojnásobuje.

MAC vrstva také řeší problém skrytých uzlů za pomocí RTS/CTS. Tento problém vzniká tím, že stanice připojené k jednomu AP jsou od sebe vzdáleny tak, že na sebe nemusí „vidět“. Proto stanice nejdříve vyšle RTS zprávu, aby zjistila, jestli je volný kanál, pokud dostane od AP potvrzení ve formě zprávy CTS, může vysílat data. Pokud přijímací stanice data přijala, pošle zprávu ACK. Komunikace pomocí RTS/CTS je naznačena na obr. 2.4. Zprávy RTS/CTS dobře zajišťují předcházení kolizím, ale zvyšují režii.



Obr. 2.4: Navázání spojení mezi dvěma stanicemi

Další vlastnostmi MAC podvrstvy jsou:

- CRC neboli cyklický kontrolní součet
- Fragmentace paketů

Každý vysílaný paket je opatřen kontrolním součtem CRC a tím je zajištěno, že za jeho pomoci bude přijímací strana schopna zjistit případnou chybu paketu, která vznikne na přenosové cestě. Fragmentace paketů dělí dlouhé datové jednotky na menší části, které postupně vysílá. Následné opakování přenosu celého paketu by síť značně zdržovalo, ale pokud se bude opakovat vysílání pouze jeho části, proces se tak velmi urychlí. [10]

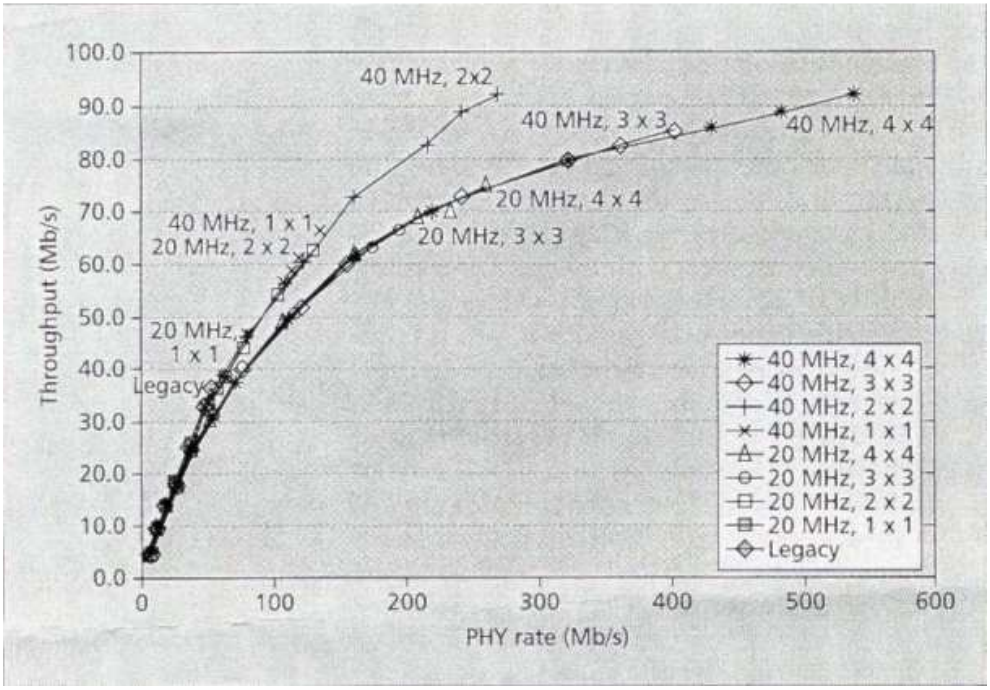
Podvrstva LLC

Vyšší ze dvou podvrstev spojové vrstvy, též známá jako standard IEEE 802.2. LLC podvrstva má na starosti MAC adresaci, řízení toku dat, vytváření rámců a kontrolu chyb.

3. 802.11n

3.1 Úvod:

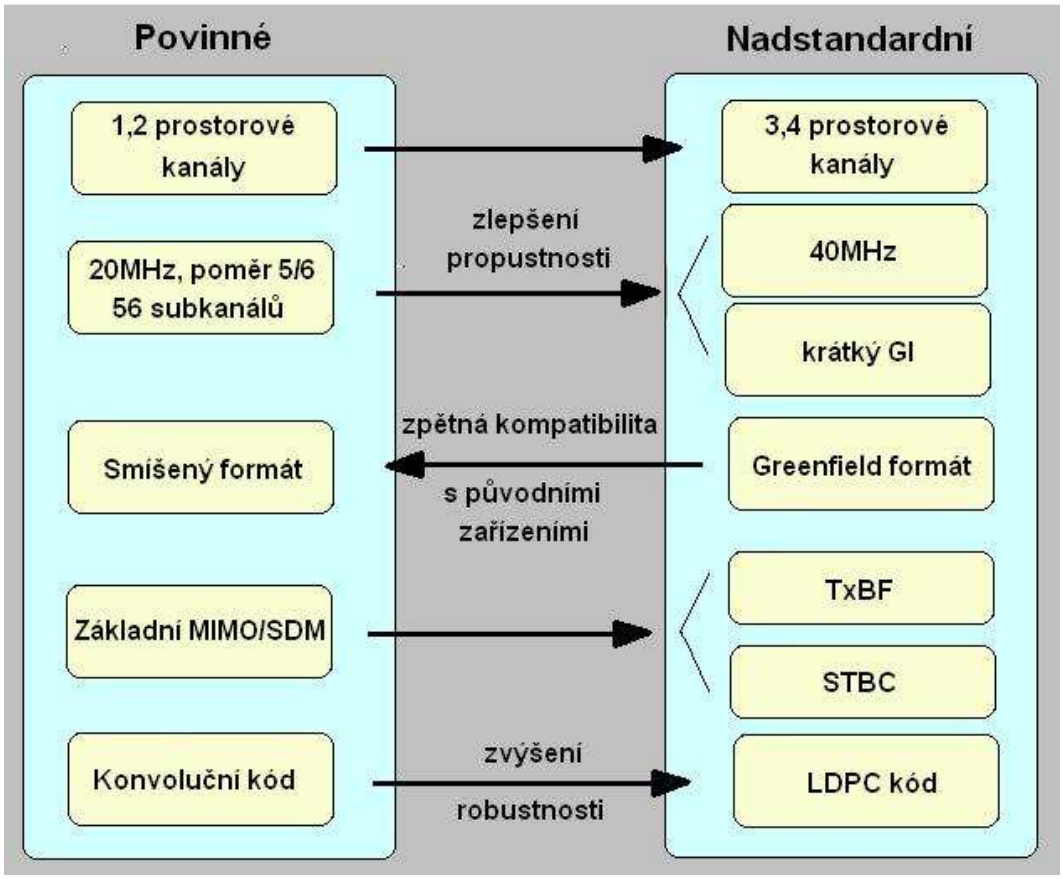
Hlavní požadavek, který řídil většinu vývoje 802.11n byl zvýšení propustnosti přinejmenším na 100 Mbit/s na MAC vrstvě. Vzhledem k tomu, že typická výkonnost starších standardů jako je 802.11a/g se pohybuje kolem 25 Mbit/s (na fyzické vrstvě kolem 54 Mb/s), požadavek jasně říkal, že je nutné minimálně čtyřnásobné zrychlení. Jelikož byl dán požadavek, aby bylo dosáhnuto určité přenosové rychlosti na MAC vrstvě nikoli na fyzické, jak tomu bylo u minulých standardů, byli vývojáři donuceni řešit složitý problém, jak výrazně vylepšit efektivitu přenosu na MAC vrstvě. Obr 3.1 demonstruje dosažitelnou propustnost, když bude navyšován datový tok na fyzické vrstvě s nemodifikovaným standardem 802.11e založeným na vrstvě MAC. Neschopnost dosáhnout propustnosti 100 Mbit/s vyžadovala podstatná zlepšení v efektivitě MAC vrstvy při vývoji 802.11n [6].



Obr. 3.1: Závislost propustnosti na MAC podvrstvě na celkovém datovém toku [7]

3.2 Fyzická vrstva:

Fyzická vrstva zaznamenala několik zásadních vylepšení oproti starším standardům. Nejzásadnější bude asi použití OFDM v kombinací s MIMO technologií. MIMO využívá prostorové multiplexování (SDM) a tvarování vysílaného paprsku (beamforming). Na obr 3.2 vidíme v levém sloupci nové nebo vylepšené povinné součásti fyzické vrstvy, které zajistí, že zařízení 802.11n budou zpětně kompatibilní se staršími standardy. V pravém sloupci jsou nadstandardní součásti, které zajistí výrazný narůst výkonu, ale za cenu nesoučinnosti s původními zařízemi.



Obr. 3.2: Povinné a nadstandardní součásti fyzické vrstvy u standardu 802.11n

3.2.1 MIMO OFDM

Standard používá k přenosu dat metodu OFMD, kterou používali standardy 802.11a a 802.11g. Avšak pro navýšení rychlosti na fyzické vrstvě ji kombinuje s technologií MIMO. MIMO technologie není žádnou novinkou na trhu, byla vynalezena již před 40 lety v Bellových laboratořích, ale podstatného využití se jí dostavilo až nyní. Technologii MIMO využívají některé produkty certifikované standardem 802.11g a

802.11a, můžeme slyšet, že se jim říká tzv. „pre-n technologie“. Avšak plně využita je MIMO technologie až v standardu 802.11n.

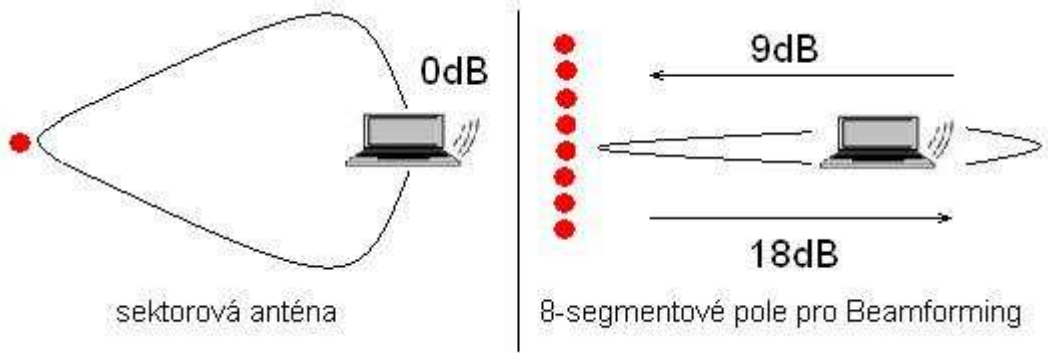
Zkratku MIMO můžeme do češtiny přeložit jako vícenásobný vstup a několikanásobný vstup a několikanásobný výstup. Základem této technologie je zjednodušeně vysílání na několika prostorově oddělených cestách, které však patří do jednoho společného přenosového kanálu. K tomu se využívají několikanásobné antény jak na straně přijímače, tak i na straně vysílače.

MIMO využívá následující součásti:

- Formování paprsku (Beamforming)
- Prostorové multiplexování (SDM)
- Diverzita antén

Formování paprsku:

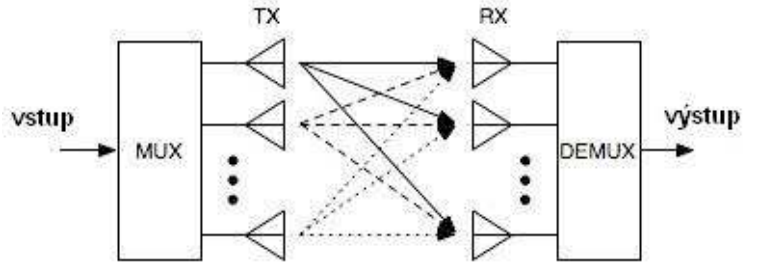
Tato metoda je založena na tom, že vysílač vyhledá nejlepší cestu pro přenos signálu k vysílači. Pro docílení této cesty je vysílač řízen pomocí algoritmu posunu fáze na zaměření rádiového výkonu na zamýšlený přijímač [12]. Při adaptivním formování paprsku systém vytváří tzv. „dopředné mapy“, pomocí kterých se signál dostane k přijímači nejvhodnější cestou. Tyto mapy jsou vytvářeny pomocí údajů, zjištěných z příchozích signálů od koncových zařízení. Systém zpracovává údaje jako je relativní síla signálu, fáze a úhel. Adaptivní tvarování paprsku je velmi náročné na procesní kapacitu, proto se uplatňuje až v dnešní době, kdy jsou výrobní technologie dokonalejší. Použitím tvarování paprsku dosáhneme lepšího poměru odstupu signálu od šumu. Na obr. 3.3 vidíme, jak se využití tvarování paprsku projeví na úrovni přijímaného signálu. V levé části obr. 3.3 je použitá všesměrová anténa, bez použití tvarování. Úroveň přijímaného signálu je 0 dB. Pokud použijeme speciální anténu, signál bude vysílán pouze v úzkém svazku směrem k bezdrátové stanici. Zlepšením vyzařovací charakteristiky je dosaženo lepší úrovně signálu.



Obr. 3.3: Princip adaptivního tvarování paprsku

Prostorové multiplexování:

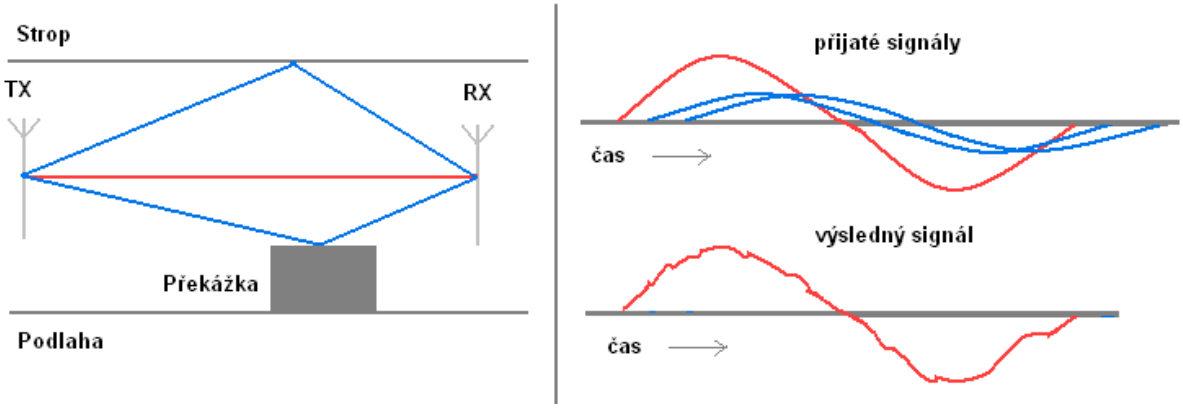
Provádí prostorový multiplex několika nezávislých datových toků přenášených současně uvnitř jednoho kanálu. Zjednodušený model je ukázán na obr. 3.4. SDM může výrazně zvýšit datovou propustnost s rostoucím počtem jednotlivých datových toků. Každý jednotlivý datový tok vlastní přijímací a vysílací anténu. Vysílač vysílá nezávislý signál pro každou anténu v určité přenosové cestě. Přijímač pomocí techniky chytrých antén demultiplexuje signál. Pokud zná vysílač informaci o stavu kanálu, může dopředu zatížit přenosovou cestu, tak aby přijímači usnadnil demultiplexování přijatého signálu a zlepšil kvalitu přenosu na dané přenosové cestě.



Obr. 3.4: Prostorové multiplexování

Diverzita antén:

Protože při šíření signálu prostředím dochází k různým nechtěným odrazům, které nám u přijímače způsobují zkreslení původního signálu. Jak vzniká toto zkreslení, je patrné z obr. 3.5. Toto nechtěné chování odstraňuje diverzita antén. Ke své funkci využívají vícenásobné antény, které jsou fyzicky na stejném místě, anebo vzájemně oddělené, ale pokrývající stejný prostor. Na přijímací straně je pak vybrán signál z antény s nejmíň zkresleným signálem. Její typické využití je při použití většího počtu antén na straně přijímače, než jaký je počet přenášených prostorových toků, anebo naopak pokud má vysílač více antén než přijímač. Toto je velmi důležité protože standard n podporuje až čtyři antény na vysílací a až 4 antény na přijímací straně. Například notebook se dvěma anténami, muže být připojen k AP se třemi anténami. V tomto případě mohou být použity pouze 2 prostorově oddělené toky, i když AP by mohl vysílat tři. Antény, které nejsou využívány pro přenos prostorového toku, můžou být použity ke zvýšení intenzity signálu a tím většího pokrytí signálem.



Obr. 3.5: Působení odražených signálů na přenášenou informaci

3.2.2 Pásmo 20 MHz vs. 40 MHz

Protože na vývoji standardu se od začátku podílely dvě vývojové skupiny, vznikly také dva koncepty.

První byla skupina **TGn Sync.** Ta prosazovala šířku komunikačního kanálu 40 MHz, což by ale v pásmu 5 GHz znamenalo snížení celkového počtu přenosových kanálů, ale za cenu dvojnásobného zrychlení a dvojnásobného rozšíření pásma. Maximální navrhovaná rychlost s využitím technologie MIMO potom byla až 600 Mbit/s.

Druhá byla skupina **WWiSE,** která by naopak nejraději zůstala u stávajícího členění na 20 MHz kanály, což by znamenalo zvýšení teoretické rychlosti přenosu na celých 135 Mb/s a již v základu počítala s nasazením technologie MIMO. Maximální teoretické rychlosti dosahovaly v návrhu až 250 Mbit/s.

Nakonec se zachovala šířka kanálu 20 MHz, aby byla umožněna zpětná kompatibilita s původními zařízeními. Zařízení, která budou certifikována pod tímto standardem, budou schopna pracovat i s kanály o šířce 40 MHz, ale bude to pouze nadstandardní výbava, hlavně z důvodu, jak již bylo uvedeno, aby byla zajištěna zpětná kompatibilita s původními zařízeními, také z důvodu používaní v různých regulačních doménách a kvůli spektrální efektivitě. [6]

Uvedení kanálů o šířce 40 MHz u zařízení 802.11n přineslo velké komplikace, protože bylo těžké zvládnout komplikovanost současného použití kanálů se šířkou 20 a 40 MHz. To se stalo obzvláště obtížné, pokud jsme v pásmu 2,4 GHz, kde se středy jednotlivých kanálů liší pouze o 5 MHz, to způsobuje částečné překrývání kanálů. Bylo přidáno pravidlo, které nařizuje, aby AP před založením spojení, nejdříve snímali ostatní sousední BSS a předcházeli založení spojení se sousedními BSS, které jsou detekovány v překrývajícím se kanálu. Také během operací s 40 MHz BSS v pásmu 2.4 GHz musí aktivní stanice pravidelně snímat překrývající se kanály. Když se objeví nová BSS s 20

MHz kanálem, zamítne operaci s 40 MHz kanálem a AP se pak musí přepnout do módu, ve kterém bude pracovat s kanály o šířce 20 MHz [6].

3.2.3 Kompatibilita se standardem 802.11g

Další funkční požadavek na 802.11n byl, aby byla umožněna zpětná kompatibilita s 802.11a/g. Skupina TGn Sync. se rozhodla zasadit tento požadavek do fyzické vrstvy definováním takového průběhu signálu, který bude zpětně kompatibilní s 802.11a se zařízeními pracujícími s OFDM 802.11g.

Preambule u 802.11n smíšeného formátu začíná preambule jako u 802.11a/g. Ten zahrnuje krátká trénovací pole (short training field), dlouhá trénovací pole (long training field), a řídící pole (signal field). To dovoluje zařízením 802.11a/g, aby detekovali pakety 802.11n ve smíšeném formátu a mohli následně detekovat řídící pole. Třebaže zařízení 802.11a/g nebudou schopna dekódovat zbytek paketů vysílané standardem 802.11n, budou schopna vhodně odložit svůj přenos podle délky specifikované v řídícím poli. Zbytek buněk tvoří u smíšeného formátu druhé krátké trénovací pole (second short training field), přídavná dlouhá trénovací pole (additional long training fields), a přídavná řídící pole (additional signal fields), nakonec následují data.

Tato nová pole jsou požadována pro MIMO trénink a řízení mnoha nových módů a operací. Pro zajištění zpětné kompatibility mezi 20 MHz pásmem a 40 MHz pásmem je preambule pro 40 MHz stejná jako pro 20 MHz, akorát je opakována na dvou přiléhajících 20 MHz kanálech a informuje, že tvoří kanál o 40 MHz. To povoluje zařízením pracující se šířkou pásma 20 MHz na obou přiléhajících kanálech dekódovat řídící pole a odložit přenos. Preambule u 802.11a má délku 20 µs. Smíšený formát u 802.11n bude mít potom se všemi řídícími a tréninkovými poli délku 36 µs pro jeden prostorový kanál a 48 µs pro 4 prostorové kanály.

Bohužel MIMO trénink a zpětná kompatibilita zvyšuje režii, což snižuje efektivitu přenosu. V prostředích kde se nevyskytují původní zařízení (nazýváme greenfield) nebude zpětná kompatibilita potřeba. Tím že vyloučíme podmínku zajištění zpětné kompatibility, můžeme preambuli u greenfield formátu zkrátit o 12 µs oproti smíšenému formátu. Tento rozdíl je velmi znatelný, a je stále víc prosazována kratší délka paketů, jak je tomu třeba v případě VoIP telefonie.

3.3 MAC podvrstva:

3.3.1 MAC rámec:

Rámec MAC má podobné složení jako předešlé standardy. Skládá se z tří hlavních částí. První je MAC hlavička, následuje samotné tělo rámce a nakonec ochrana proti chybám [1]. Složení MAC rámce můžeme vidět na obr. 3.6.

Obr. 3.6: Struktura MAC rámce

Význam jednotlivých polí:

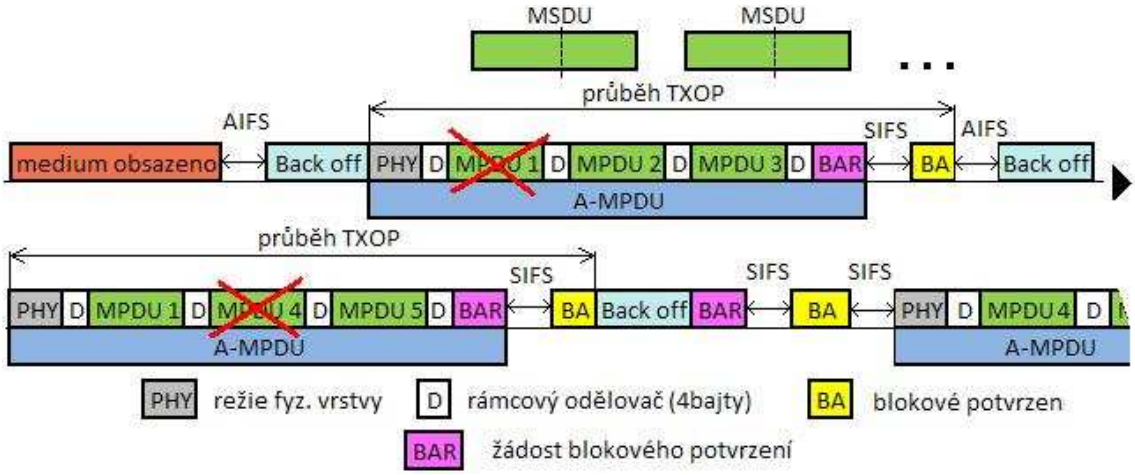
- **Řídící pole:** udává mnoho parametrů důležitých pro přenos. Nejdůležitější je údaj o typu rámce, jestli se jedná o rámec řídící, datový nebo management a udává také jejich podtyp. Dále indikuje např. fragmentaci, nebo režim úspory energie.
- **Doba trvání / ID:** obsah tohoto pole se liší u různých typů rámců, nejčastěji se toto pole využívá k přenášení informace o délce obsazení media.
- **Adresa 1-4:** tyto pole slouží k identifikaci BSS, obsahují zdrojovou a cílovou adresu a adresu vysílací a přijímací stanice.
- **Kontrola pořadí:** udává sekvenční číslo daných MSDU nebo MPDU a čísluje jejich jednotlivé fragmenty, slouží k zajištění správného pořadí.
- **QoS**: zajištění QoS
- **Tělo rámce**: Samotné tělo rámce, obsahující data. Má variabilní délku, maximální délka je však 2304 B
- **FCS**: zabezpečení 32-bitovým kontrolním součtem CRC

Pro zvýšení propustnosti na MAC vrstvě využívá standard 802.11n fakt, že hlavička MAC rámce obsahuje informace, které jsou pro jednotlivé fragmenty MSDU stejné. Proto se bude hlavička přidávat pouze k prvnímu fragmentu, dosáhneme tím výrazné snížení režie. Pole, která jsou pro všechny fragmenty stejná, jsou na obr. 3.6 vybarvena modrou barvou. Nevýhoda je však v tom, že pokud bude první fragment z MSDU porušený, stejně jako i v případě kontrolního rámce BAR (žádost o blokové potvrzení) u A-MPDU, bude celý A-MPDU na přijímací straně zahozen. Avšak pravděpodobnost, že k tomu dojde je zanedbatelná, zvláště když vezmeme v úvahu, velikost BAR.

3.3.2 Agregace/fragmentace rámců:

Fragmentace MSDU u standardu 802.11 vede při vysokých rychlostech k rapidnímu snížení výkonu. Ve vysokých přenosových rychlostech totiž výrazně narůstá režie a tím se snižuje propustnost na MAC vrstvě. Snížením této režie, dosáhneme většího výkonu. Na druhou stranu fragmentace zajišťuje větší spolehlivost přenosu. Tím že vysílá kratší datové rámce, je větší pravděpodobnost, že data budou v pořádku přijata. Tahle vlastnost je velmi užitečná v prostředích, kde není zřízeno spolehlivé spojení a může docházet k výpadkům, protože pravděpodobnost úspěchu přenosu velkého datového rámce by byla velmi malá. Standard 802.11n musel zvolit kompromis mezi spolehlivostí a vysokou propustností. Navrhované fragmentační/agregační schéma kombinuje velmi účinné využití rozsahu agregace s robustní ochranou proti chybnému přenosu [2][9].

Jak vidíme na obr. 3.7 hlavní myšlenkou je fragmentace MSDU z vrstvy LLC na několik MPDU, které se pak budou přenášet v jednom kontejneru A-MPDU. Pro potvrzování bylo použito blokové potvrzování ze standardu 802.11e, které výrazně snižuje režii.



Obr. 3.7: Časový diagram průběhu agregace/fragmentace

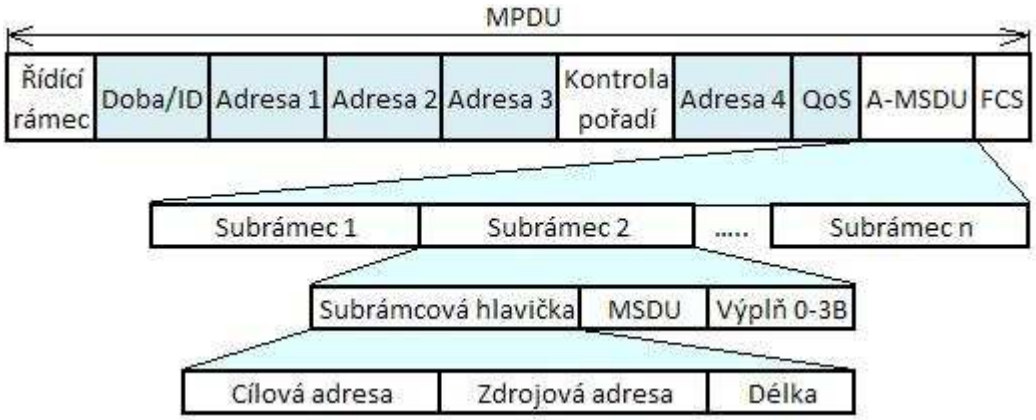
V případě, že jsou vysílací příležitosti dostatečně dlouhé, může být umístěno do jednoho A-MPDU více MSDU. Obr. 3.7 ukazuje, že každá MSDU je rozdělena do dvou stejně velkých částí (MPDU 1,2 a MPDU 3,4 jsou každá z jiné MSDU). Pokud se po určitou dobu (AIFS) jeví medium jako volné, dojde k vygenerování náhodného intervalu (Back Off). Po jeho ukončení jsou data vysílána po dobu trvání intervalu TXOP. Přeškrtnuté části znamenají chybu při přenosu MPDU. Pokud došlo k chybě fragmentu, avšak výměna žádosti o blokové potvrzení (BAR) a blokového potvrzení proběhla v pořádku, bude interval Back Off (náhodně vygenerovaný interval) podle pravidla EDCA resetován na minimum. Pokud nedojde k úspěšné výměně BAR/BA, měl by odesílatel zvýšit interval Back Off a znovu posílat žádost BAR, dokud neobdrží potvrzení BA. Pokud bude ještě volné místo v intervalu TXOP, bude odesílatel vysílat více MPDU v jedné A-MPDU [2][9].

V tomto standardu existují dvě možnosti agregace:

- Agregace MSDU
- Agregace MPDU

Agregace MSDU (A-MSDU)

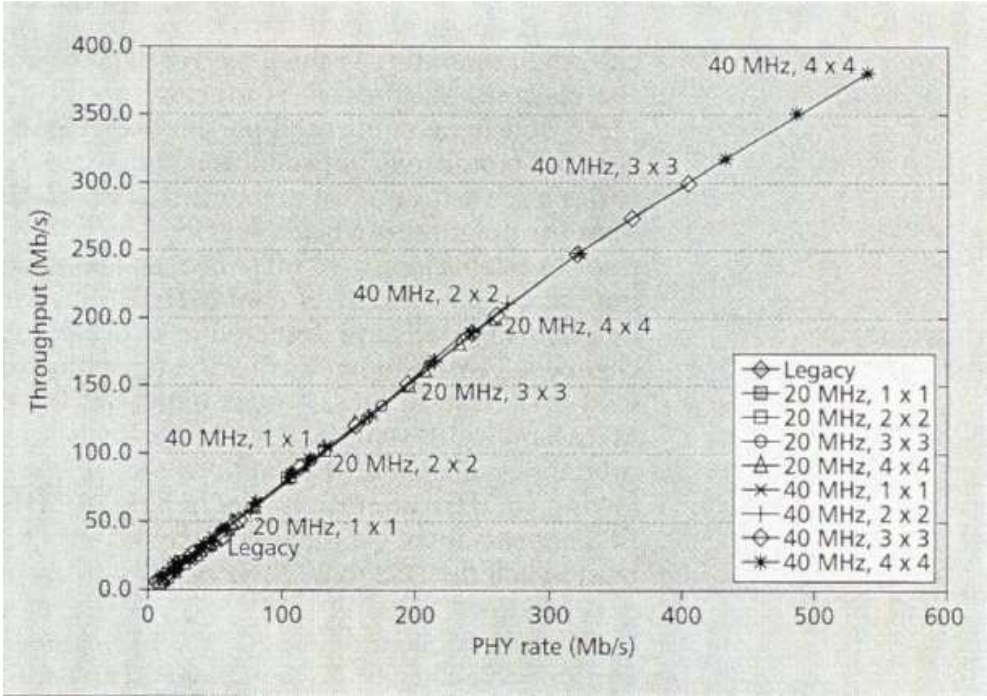
A-MSDU (MAC service data unit aggregation) spočívá na vrcholu MAC vrstvy a shromažďuje mnohonásobné MSDU do jedné MPDU. Jak vidíme z obr. 3.8 před každým MSDU je přidána subrámcová hlavička, která se skládá z cílové a zdrojové adresy a z pole udávající délku v bajtech. Mezery mezi jednotlivými MSDU jsou pak vyplněny čtyřmi bajty. Jednotlivé řetězce takových subrámců dohromady tvoří jednotlivé MPDU [6].



Obr. 3.8: Struktura agregace MSDU

Agregace MPDU (A-MPDU)

A-MPDU (MAC protocol data unit aggregation) spočívá na dně MAC vrstvy a shromažďuje vícenásobné MPDU. Každý MPDU předchází pole udávající délku, 8 bitů zabezpečení CRC a 8-bitové podpisové pole. Mezi tyto subrámce se vkládá výplň o velikosti 4 bajty. Všechny subrámce jsou spojeny dohromady. Výhodou A-MDPU je to, že pokud je určité MPDU porušeno, přijímač může snímat data dál k další MPDU detekováním podpisového pole v hlavičce dalšího MPDU. U A-MSDU tato výhoda není a každá chyba bude znamenat, že agregace nebude fungovat [6].
Díky rámcové agregaci je závislost propustnosti na MAC vrstvě a datového toku na fyzické vrstvě lineární, jak můžeme vidět na obr. 3.9. Při přenosové rychlosti 600 Mb/s na fyzické vrstvě můžeme dnes dosáhnout 400 Mb/s na MAC vrstvě.



Obr. 3.9: Závislost propustnosti na datovém toku na fyzické s použitím agregace [7]

3.3.3 Další vylepšení MAC vrstvy:

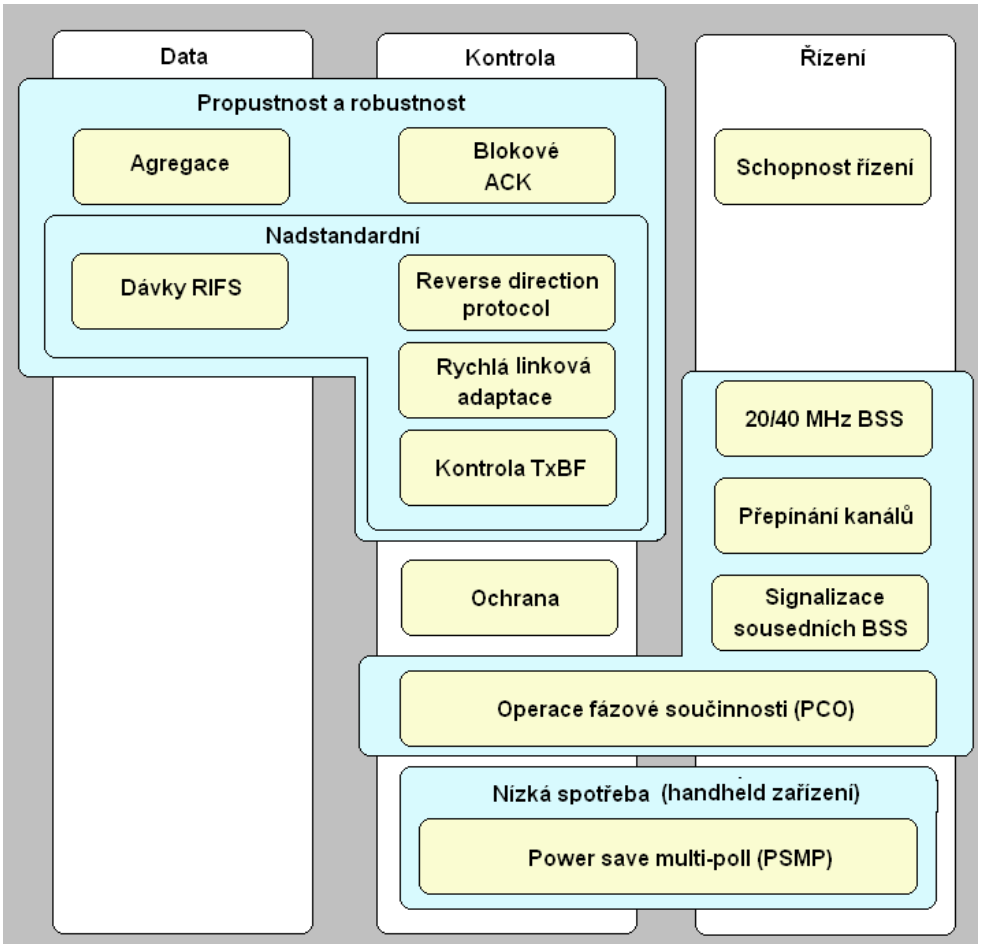
V předcházejících kapitolách byly popsány hlavní změny a doplňky MAC vrstvy. Ve standardu 802.11n je jich však více, jak můžeme vidět na obr. 3.10.

Dávky RIFS:

Standard n používá mezi jednotlivými vysíláními interval RIFS (Reduced inter-frame spacing). Jak už název napovídá je tento interval o něco kratší než intervaly DIFS (DCF inter-frame space) a AIFS (arbitration inter-framespace), které používali standardy 802.11a 802.11g. RIFS se použije tehdy, kdy není využita agregace rámců pro zkrácení mezer mezi jednotlivými rámci.

Blokové potvrzování (BA):

Pokud použijeme blokové potvrzování (BA) ze standardu 802.11e, stanice může vysílat dávku paketů ještě před přijmutím potvrzení. Přídavné zlepšení k blokovému potvrzování v 802.11e obsahovalo kompresi BA rámců, za pomocí eliminace podpory pro fragmentaci. Byl také začleněn zpětný protokol, který stanici dovoloval, aby sdílela své vysílací příležitosti TXOP jiným stanicím. TXOP je časově ohraničený interval, během kterého může stanice odeslat tolik rámců paketů kolik je schopna.



Obr. 3.10: Vylepšené a přidané součásti na MAC vrstvě

Zpětný protokol (Reverse direction protokol):

Byl také začleněn zpětný protokol (dále RD), který stanici dovoloval, aby sdílela své vysílací příležitosti TXOP jiným stanicím. Smysl použití zpětného protokolu je v mnohem efektivnějším přenosu dat mezi dvěma zařízeními. Zpětný protokol během trvání TXOP eliminuje potřebu založit nový přenos dat druhého zařízení. Před zpětným protokolem požadoval každý jednosměrný přenos stanici zahajující spojení, aby mohl zachytit, případně i rezervovat, spojení na bezdrátovém mediu. Se zpětným protokolem dostane jedna stanice vysílací příležitosti TXOP a může v podstatě udělit povolení druhé stanici, tím že jí pošle příslušné informace během TXOP. Protokol definuje dva stavy:

- RD initiator – posílá potvrzení RDG (Reverse direction grand) v řídícím poli PPDU MAC rámce
- RD responder – je to příjemce potvrzení RDG

Rychlá linková adaptace (Fast link adatation):

Je to algoritmus sloužící k výběru vhodné modulace a kódovacího schématu.

Podpora kapesních zařízení:

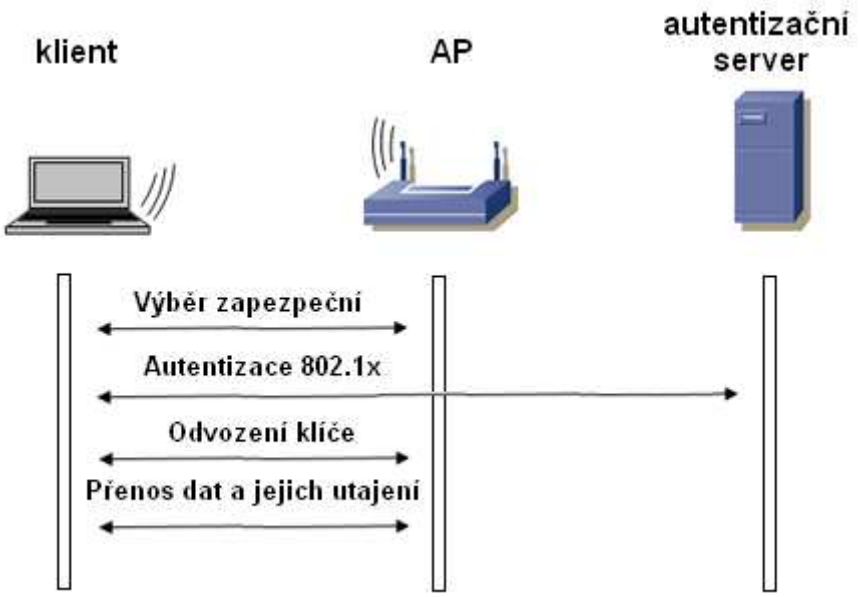
Protože obliba bezdrátových sítí stále stoupá a WiFi adaptéry už nejsou součástí jenom stolních PC a notebooků, ale stále častěji jsou osazovány v PDA, mobilních telefonech nebo přehrávačích. Proto byl do MAC vrstvy implementován mechanismus PSMP Power Save Multi-Poll, který má snížit kanálové využití a snížit spotřebu energie, při přijímání a vysílání malých dat. Tyto požadavky vyvstaly s přenosem hlasu (VoIP) v BSS. Vysílání směrem k uživateli jsou seskupena dohromady a přenosy v opačném směru jsou plánovány. Plánování pro download přenosy je poskytováno na začátku PSMP fáze a dovoluje snížení výkonu vysílače jednotlivým zařízením, dokud je potřeba.

3.4 Zabezpečení WPA/WPA2:

Bezdrátové sítě jsou obzvláště náchylné na neoprávněné útoky zvenčí. Jako ochranu před těmito útočníky používá tento standard ochranu WPA/WPA2 (WiFi protected access), která je převzata ze standardu 802.11i. Opravuje a vylepšuje předchozí ochranu WEP. Protože ani ochrana WPA/WPA2 není dokonalá, nebude na 100% ochránění před neoprávněnými průniky do Vaší sítě. Důkazem jsou ruští hackeři, kteří toto šifrování prolomili pomocí grafické karty GeForce.

Šifrování WPA pracuje s autentizačním serverem IEEE 802.1x, který rozesílá uživatelům rozdílné klíče. Průběh autentizace klienta k serveru vidíme na obr. 3.11. Je možné použít i mód, který se nazývá Pre-shared key PSK. Při použití tohoto protokolu, používají všichni uživatelé stejné heslo [11]. K šifrování komunikace zde slouží protokol TKIP (Temporal Key Integrity Protocol), který dynamicky mění klíče. TKIP pracuje s automatickým klíčovým mechanismem, který mění každých 10000 paketů svůj dočasný klíč. Dalším vylepšením WPA oproti WEP je kontrola integrity zpráv MIC (Message Intergity Check), který zajišťuje výrazné zabezpečení integrity zpráv oproti dříve užívanému CRC [4][8].

WPA2 implementuje povinné prvky IEEE 802.11i. Obsahuje nový algoritmus CCMP (Counter-Mode with Cipher Block Chaining Message Authentication Code Protocol), který je založen na AES (Advanced Encryption Standard).



Obr. 3.11: Diagram připojení klienta do WLAN

Výběr zabezpečení

Výběr ochranného mechanismu je prováděn na základě rámců beacon a probe. Po výběru vhodného mechanismu dojde k autentizaci. Používají se dva typy:

- **WPA enterprise mode:** využívá k ověření uživatele protokol 801.1X a Radius (Remote Authentication Dial In User Service). K úspěšné autentizaci je nutné znát jméno a heslo. Tato metoda je vhodná pro velké firemní sítě [11].

- **WPA personal mode:** používá pre-shared key (PSK), AP i každý klient zná heslo (zde 8 až 63 znaků) [11]. Každý uživatel v síti zná veřejné heslo, pomocí kterého jsou generovány další bezpečnostní klíče. Tento typ autentizace je vhodný pro domácí sítě, protože autentizaci provádí AP.

4. OPNET Modeler:

Program OPNET Modeler (dále OM) je simulační prostředí, které bylo vyvinuto firmou OPNET Technologies Inc., a slouží pro návrh, simulaci a analýzu různých síťových technologií a mechanismů [5]. Pomocí něho jsme schopní simulovat velké množství topologií, standardů, protokolů a aplikací. Nejsme omezeni pouze modely, které jsou po instalaci k dispozici, ale můžeme implementovat nově vytvořené modely pro OM.

OM se ovládá pomocí interaktivního grafického prostředí, kdy pomocí myši na plochu vkládáme objekty, které pomocí modelů simulující přenosová media propojujeme. Důležitou funkcí je duplikace scénářů, pomocí které se snadno srovnávají výsledky simulací s odlišnými prvky nebo nastaveními. Výstupem z OM je vykreslení charakteristik, nebo můžeme naměřená data exportovat např. do Excelu. Použití OM je výhodné pro simulací sítí, které by bylo finančně náročné fyzicky sestavit. Nebo naopak, můžeme využít teoretických výsledků z OM při výstavbě reálné sítě. Můžeme simulovat extrémní situace, jako jsou je přetížení serverů, nebo jeho výpadky a těmto situacím předcházet.

Základní prvky prostředí OPNET Modeler:

- *Subnet (podsíť)* - složená ze stanic, routerů, firewallů, přenosových medií a všech možných síťových komponentů
- Node model (model uzlu) - složený ze základních funkčních bloků jako zdroj, paměti, procesor [5].
- process model (model procesu) – zde jsou popsány procesy modelu uzlu, jako např. stavy procesu, události, přechody. [5].

Editory:

Struktura OM je rozložena do tří vrstev. Těmto vrstvám se říká editory:

- *Project Editor* (editor projektu)- hlavní grafický editor umožňující vytváření různých topologií, pomocí definovaných modelů. Můžeme zde generovat různé druhy zátěží, které jsou definovány, nebo vytvářet vlastní.

- *Node Editor (editor uzlu)* – umožňuje pohled na vnitřní uspořádání síťového zařízení nebo sytému a naznačuje vazby mezi jednotlivými procesy a funkcemi.

- *Process Editor* (editor procesu) – každý stav a proces modelu obsahuje kód v C/C++ podporovaný rozsáhlou knihovnou s funkcemi vytvořenými pro protokolové programování [5].

4.1 Implementace popis modelů standardu 802.11n:

Modely 802.11n mi dodal můj vedoucí z webových stránek http://www.opnet.com. Jejich autorem je Dmitry Akhmetov, který pracuje pro firmu Intel. Tyto modely jsou o mnoho složitější než standardní bezdrátové modely, které jsou přítomny v OM. Obsahují podrobné nastavení fyzické vrstvy a MAC podvrstvy. Na obr. 4.1 je jsou vidět parametry pro nastavení OFDM. Pro porozumění funkce modelů zde uvádím souhrn těch nejdůležitějších parametrů.

Basic rate – definuje typ modulace a použitý kódovací poměr u kontrolních a řídících rámců.

OFDM PHY parametrs:

Subcarrier number – udává počet subnosných.
Starting Frequency – udává počáteční frekvenci v příslušném pásmu.
Symbol Duration – udává délku jednoho OFDM symbolu.
Pilot Tones – počet pilotních nosných (4 pro 20Mhz pásmo, 6 pro 40Mhz pásmo).
Extended symbol duration – udává délku nestandardního symbolu (symbol s krátkým Guard Interval).

Operational Rate - definuje typ modulace a použitý kódovací poměr pro datové rámce.

PHY Capabililities - definuje, zda stanice podporuje i původní zařízení, nebo pracuje v režimu Greenfield.

PHY type - tento parametr má vliv na to, jestli stanice může podporovat různé typy fyzických vrstev.

Channel:

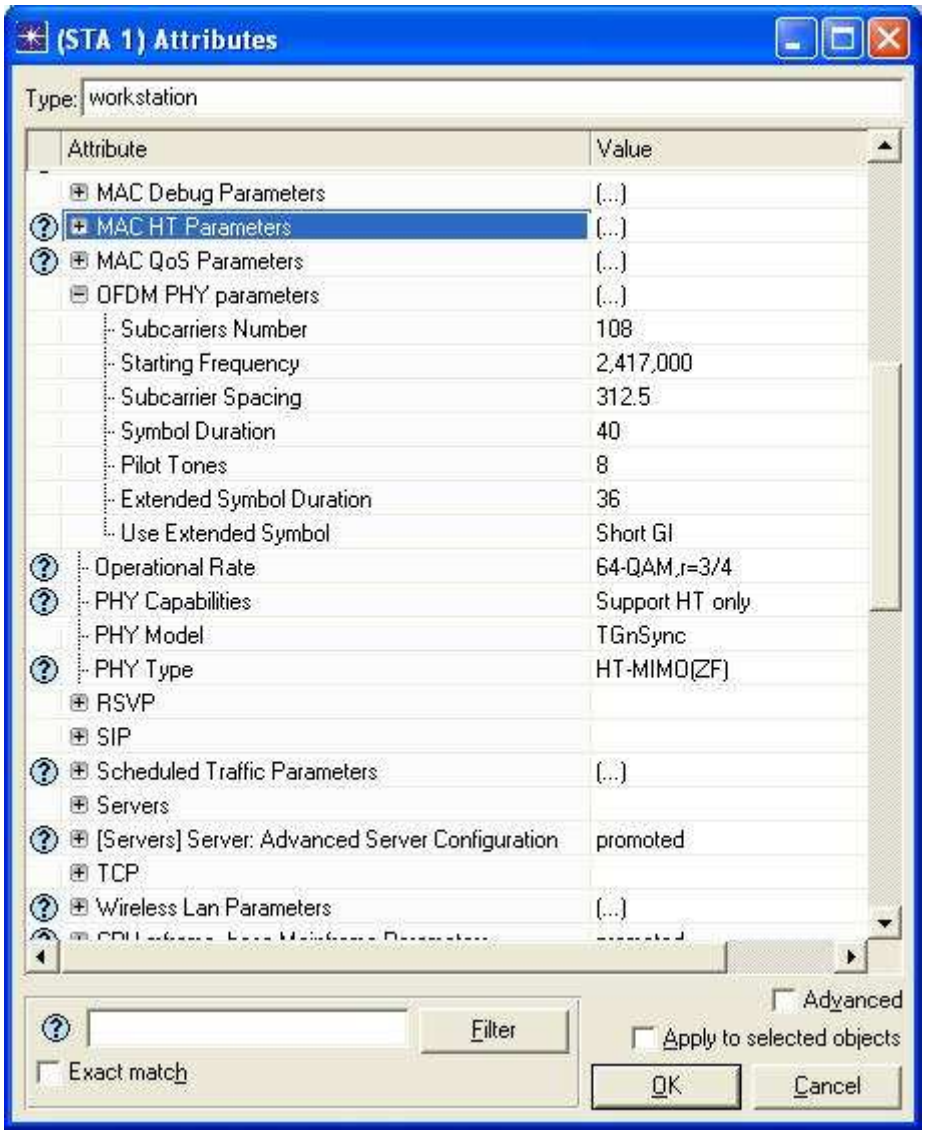
CCA threshold – energetický práh pro detekci paketu.
Channel attributes – zde se nachází nastavení počtu vysílacích (Tx number antennas) a přijímacích (Rx number antennas) antén. Typ modelu kanálu (výběr mezi LOS a NLOS podle vzdálenosti mezi stanicemi).
RX channel, TX channel – zde se zadává datový tok (Data Rate[bps]), formát paketu (packet formats), šířka kanálu (bandwidth), základní frekvence kanálu (min frequency [Mhz]).

MAC HT Parametrs:

Use ACC backoff – umožňuje vypnout nebo zapnout přístupovou funkci ACC.
Lambda for ACC – specifický parametr ACC.
IAC retry limit – udává, kolikrát může být aktuální IAC znovu odesláno.
BlockAckRequest retry limit – pokud tento limit vyprší, dochází ke smazání celého burstu.
Trained Singleton – umožňuje tréninkovou výměnu pro obyčejné datové přenosy.

TXOP usage rules:

TX sequence policy – umožňuje Full TXOP, nebo One TX sequence. Při Full TXOP stanice používá celý interval TXOP. Při One TX sequence se uskuteční pouze jeden datový přenos a pak začíná soutěžení o medium.
Extension by BURST renewal – umožňuje stanicím přidat další MPDU do vysílaných Burstů
Retry Rules - definuje pravidla pro opakován vysílání. Používá dvě pravidla Immediate "in-time" retry a Immediate "start" retry. Immediate "in-time" retry umožňuje přeposlání každého mezilehlého rámce po SIFS. Immediate "start" retry umožňuje přeposlání startovního rámce každé přenosové sekvence při intervalu SIFS



Obr. 4.1: Parametry bezdrátové stanice standardu 802.11n

Implementace modelů do prostředí OM:

Implementace těchto modelů byla velmi náročná a problémová. Byl to hlavní problém při práci na tomto projektu. Opravením jednoho problému se objevil další. Hlavní problém byl s tím, že se mi nepodařilo zkontaktovat s někým, kdo by měl s těmito modely zkušenosti. Všechno je to dáno tím, že standard není ještě plně schválen a organizace IEEE si informace o něm dost chrání.

Modely nejdříve nakopírujeme do složky C:\Documents and Settings\User Name\op_models (můžeme použít libovolnou složku). Poté v OM vybereme volbu **File ->Manage Model Files -> Add Model Directory**, vybereme složku, kam jsme modely umístili a dáme OK. Ještě zatrhneme možnost Include All Subdirectories.

V krátkosti zde popíši hlavní problémy při spouštění simulace s modely 802.11n:

První problém, že kompilátor u určitých proměnných očekával strukturu, viz výpis z konzole pod odstavcem. Tento problém jsem vyřešil změnou nastavení v Opnet Modeler:

Opnet -> Edit -> Preference-> Discrete Event Simulation-> Code Generation -> Allow Access To State Variables Wihout FIN -> TRUE

Zde je výpis z konzole:

Location Line Message
Function Block 1227 left of '->last_frametx_type' must point to struct/union
Function Block 1228 left of '->priorities' must point to struct/union
Function Block 1228 left of '->current_time' must point to struct/union
Function Block 1229 left of '->priorities' must point to struct/union
Function Block 13245 left of '->tx_queue' must point to struct/union
Function Block 13245 left of '->tx_queue' must point to struct/union
Function Block 13245 unable to recover from previous error(s); stopping compilation
---
| <<< Recoverable Error >>>
| Process (wlan_80211HT_mac_tx_state_edca_tcp_udp_21) compilation failed.
| Compile it individually for actual errors.

Po vyřešení tohoto problému se objevilo další chybové hlášení. Zde je zkrácený výpis z konzole:

gna_ace_support.opt32.i0.ex.obj : error LNK2019: unresolved external symbol _Oms_Resource_Handle_Get referenced in function _gna_ace_apprun_node_info_create
ip_dgram_sup.opt32.i0.ex.obj : error LNK2019: unresolved external symbol _ipv6_routing_header_destroy referenced in function _ip_dgram_extension_headers_info_destroy
ip_dgram_sup.opt32.i0.ex.obj : error LNK2019: unresolved external symbol _ipv6_destination_header_destroy referenced in function _ip_dgram_extension_headers_info_destroy

```
--------------------------------------------------------------------------
<<< Program Abort >>>
  * Error:     Error encountered rebuilding repository -- unable to proceed
           T (0), EV (-), MOD (NONE)
```

Problém byl v tom, že hlavní procesní model, nebyl správně svázán se standardními knihovnami OM, takže procesy modelů volali neznámé funkce. Problém byl vyřešen definováním externích knihoven v menu OM. **File -> Declare External Files**, zde jsem nadefinoval potřebné knihovny.

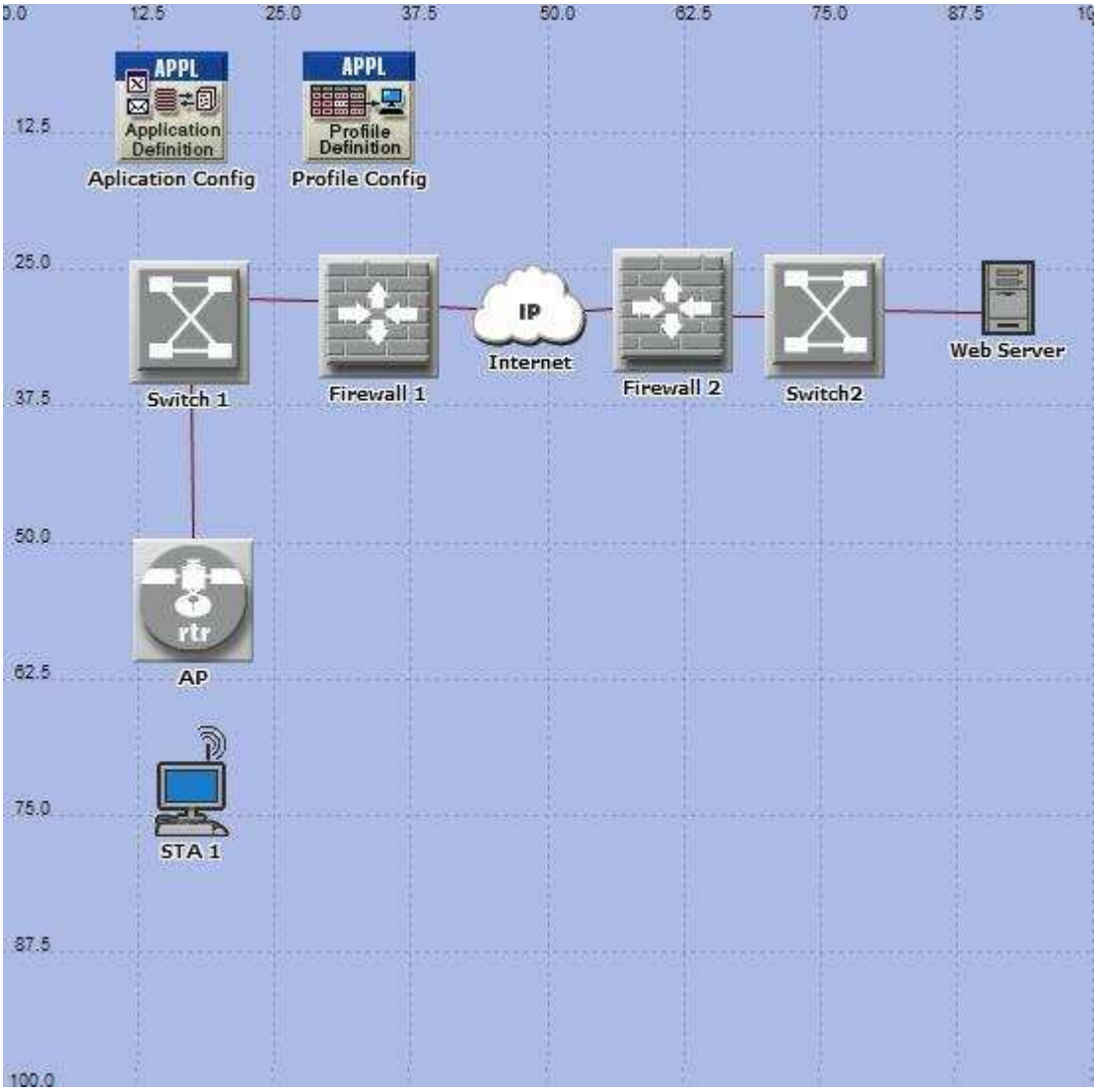
Po přidání všech potřebných knihoven, se objevila chyba ve funkci *ip3_radio_address_resolve*. Výpis je pod tímto odstavcem. Tahle funkce souvisí s adresováním stanic. Tuto chybu jsem obešel tím, že jsem vypnul automatické adresování. Avšak když po správném nakonfigurování a nastavení adres stanic spustil simulaci, negenerovala se v síti žádná doprava. OM nehlásí žádné chyby, i výpis DES logu je v pořádku. Myslím, že chyba bude někde ve funkci, která souvisí s adresací.

```
          Call   Block
          Count  Line#  Function
    ------------------------------------------------------------
0)        9        5  ip_dispatch [wait_2 -> cmn_rte_tbl : SELF_NOTIFICATION /
                      ip_dispatch_init_phase_2 ()]
1)        1     1111  ip_dispatch_init_phase_2 ()
2)        1     2390  ip3_radio_address_resolve (List* radio_nodes_list_ptr, Objid subnet,
                       Objid self_id)
3)        1     3627  sim_error_hndl_abort
4)        1     3600  sim_error_hndl_output
5)        4     3551  sim_error_hndl_log
6)        4     3948  Sim_Log_Message
```

Z důvodu těchto problému, které se nepodařilo odstranit i po četných konzultacích, jsme se s vedoucím bakalářské práce dohodli, že simulace bude obsahovat pouze srovnání standardů 802.11a, b, g.

4.2 Návrh bezdrátové sítě pro simulaci streamového videa

Navržená bezdrátová síť obsahuje dvě hlavní části. A to konkrétně bezdrátovou pracovní stanici a webový server, z kterého budeme stahovat požadovaná data. Topologii sítě vidíme na obr 4.2. V našem případě budeme simulovat stahovaní multimediálních dat, skládající se z obrazové a zvukové stopy a to v reálném čase.



Obr. 4.2: Schéma simulované sítě

Mrak IP v této simulaci prezentuje sít Internet. Webový server je od IP sítě oddělen pomocí ochranné brány (firewall), stejně jako bezdrátová stanice. Toto opatření je z důvodu zajištění bezpečnosti. Dále jsou tu dva přepínače, jak na straně serveru, tak na uživatelské straně. Mohou být použity k připojení dalších zařízení a tím k rozšíření sítě. Pak je tu AP, které slouží k připojení pracovní stanice do sítě. Application Config a Profile Config nejsou fyzicky součástí sítě, slouží pouze k nakonfigurování simulovaných aplikací a nastavení příslušného profilu.

4.3 Vytvoření a konfigurace navržené sítě

Vytvoření nového projektu:

Nejdříve musíme vytvořit nový projekt. Z menu OM založíme nový projekt kliknutím na **File -> New**, zadáme jméno nového projektu a scénáře. Název mého projektu je **wlan_realtime_video** a jméno prvního scénáře **scenarion1_802.11a_stream_video**.

Po správném vytvoření projektu se nám spustí průvodce k vytvoření nového scénáře. Jako počáteční topologii zvolíme **Create empty scenário**, prostředí pro simulaci vybereme **Office** o rozměrech 100x100 metrů. Poslední volbou bude vybrání technologií, které se nám zobrazí v paletě objektů. Vybereme **wireless_lan_adv**, **ethernet_adv**.

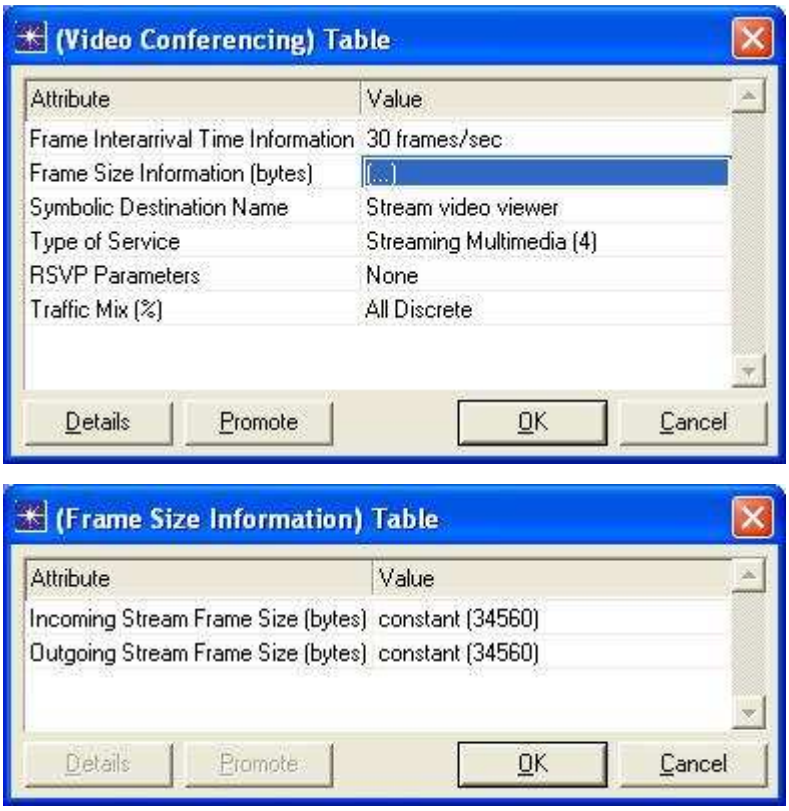
Vytvoření a konfigurace sítě:

Na pracovní plochu si z palety objektů přeneseme objekty: **wlan_wkstn_adv (**model bezdrátové stanice, umožňující simulaci aplikací typu klient-server**)**, **wlan_ethernet_router_adv** (bezdrátový router s jedním rozhraním Ethernet), 2x **ethernet16_switch_adv** (klasický 16-ti portový přepínač s podporou protokolu STP**)**, 2x **ethernet2_slip8_firewall_adv** (brána založená na IP protokolu s funkcemi Firewallu, obsahuje 10 portů), **ip32_cloud_adv** (reprezentuje IP síť s počtem portů 32) a **ethernet_server_adv** (server pro sítě typu Ethernet, umožňuje simulací aplikací přes TCP/UDP). Ještě přidáme konfigurační bloky **Profile Config** a **Application Config**. K propojení jednotlivých objektů použijeme **Ethernet 1000BaseX**, mohli bychom použít i nižší verzi, ale abychom měli rezervu, použil jsem tuto verzi. K propojení mezi Firewallem a Internet použijeme linku **PPP_DS3**.

Konfigurace Application a Profile Config:

Application Config slouží k vytváření nových aplikací, nebo zde můžeme upravovat parametry již definovaných aplikací, které pak budou v síti sloužit jako zátěž. V tomto projektu budeme pracovat se streamovým videem. Tato aplikace není v OM defaultně vytvořena, proto jsem ji musel nakonfigurovat.

Pravým tlačítkem myši klikneme na objekt **Application Config** a zvolíme **Edit Attributes**. Objekt nejdříve přejmenujeme na **Application Config**. Potom v menu **Application Definition** změníme položku **Number of Rows na 17**. Tím jsme si vytvořili nový slot pro novou aplikaci. Aplikaci pojmenujeme na **Stream video**. Otevřeme nabídku **Description** kde vybereme **Conferencing Video** a dáme **Edit**. Hodnoty nastavíme podle obr. 4.3.



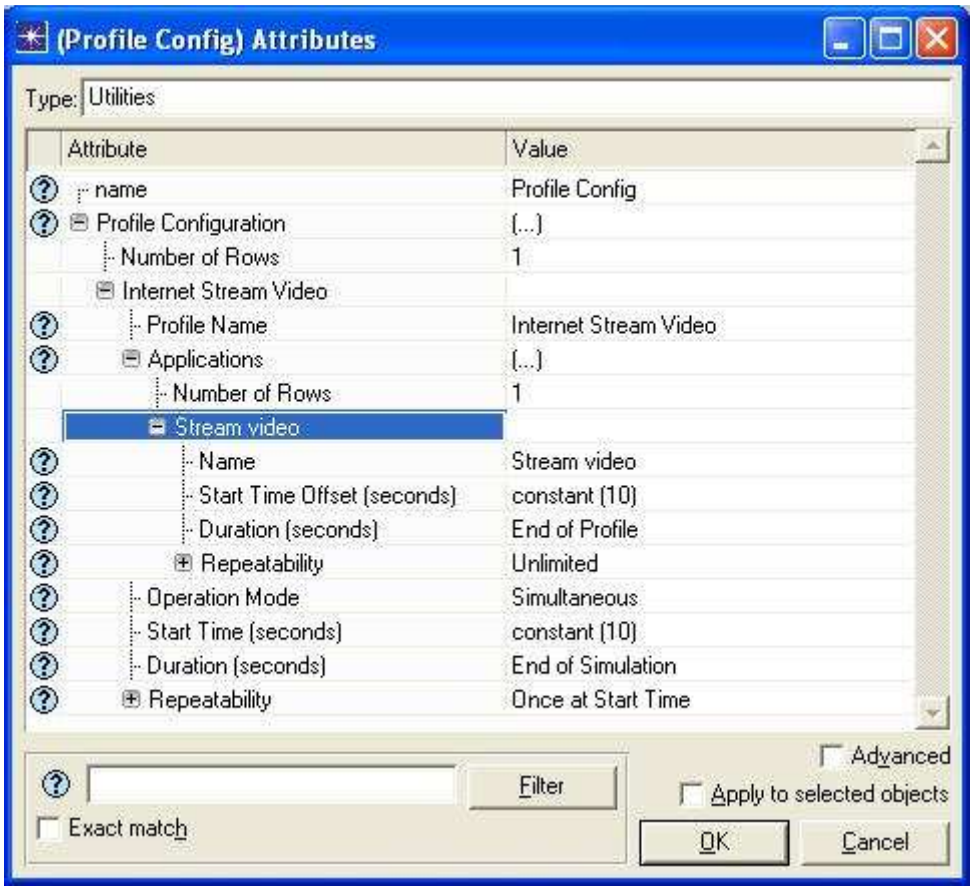
Obr. 4.3: Nastavení aplikace Stream video

Snímkovou frekvenci zvolíme na 30 snímků za sekundu. Druhá položka je nastavení velikosti jednoho snímku. Nastavil jsem hodnotu 34560 bajtů, která odpovídá rozlišení 120x240 pixelů při použití kódování na 9 bitů.

Velikost jednoho snímku [B] = (128*240*9)/8 = 34560 B

Symbolické jméno jsem zvolil **Stream video viewer**. Poslední změnu provedeme v položce **Type of Service**, která udává, jakou budou mít pakety v IP frontách prioritu. Nastavíme tento parametr na **Streaming Multimedia (4).**

Pro definici profilů se používá objekt **Profile Config**. V tomto objektu můžeme nastavit na jak dlouho a kdy se jaká aplikace spustí. Aplikace můžeme pouštět současně nebo po sobě. Otevřeme opět nastavení pomocí **Edit Attributes**. Objekt pojmenujeme **Profile Config**. Protože si v tomto projektu vystačíme pouze s jedním profilem, v **Profile Configuration** zadáme **Number of Rows -> 1**. Profil pojmenujeme **Internet Stream Video**. **Operational mode** značí, zda aplikace běží současně nebo v pořadí po sobě. Protože je v našem projektu jenom jedna aplikace tato položka pro nás není důležitá. Nastavíme na **Simultaneous**. Čas spuštění profilu nastavíme na konstantních 10 sekund a délku běhu profilu na dobu do ukončení simulace. V nabídce **Application** bude **Number of Rows -> 1**, a z roletové nabídky vybereme námi definovanou aplikaci **Stream Video**. Offset začátku aplikace zvolíme na konstantních 10 sekund. Čas trvání bude do konce profilu. Nastavení profilu je na obr. 4.4.



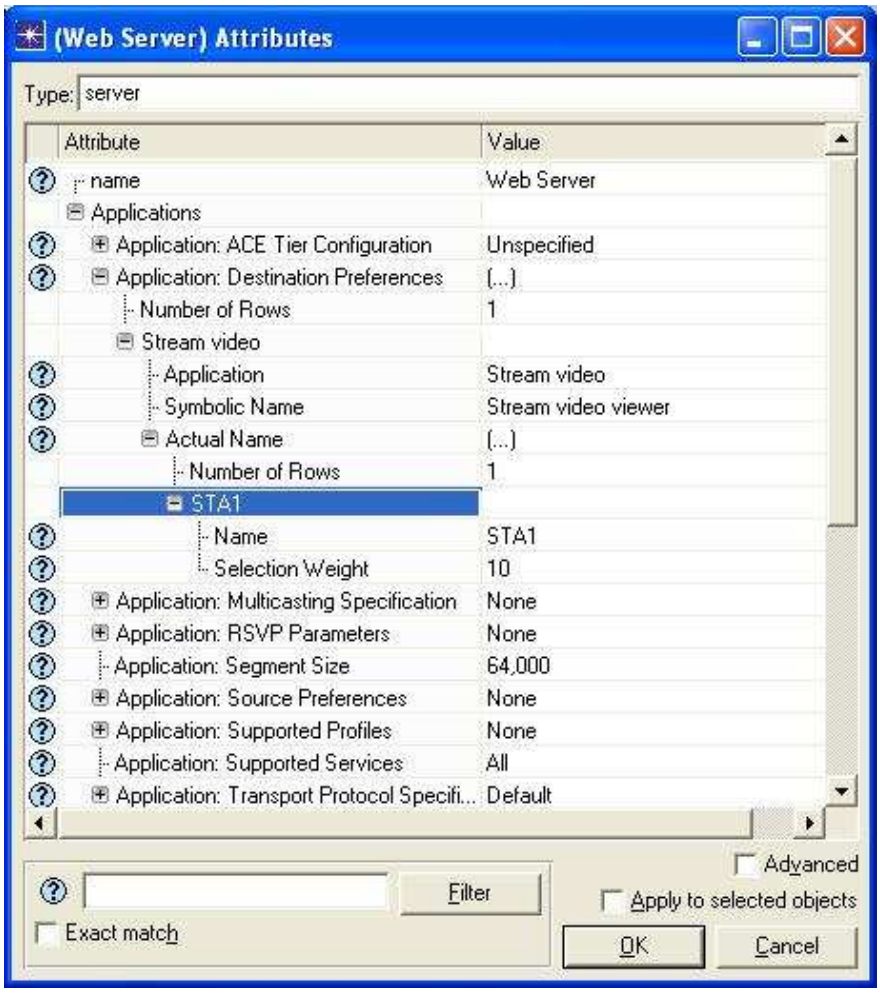
Obr. 4.4: Nastavení profilu

Konfigurace Web Serveru:

Otevřeme nastavení kliknutím na **Edit Attributes**. Nejdříve objekt pojmenujeme na **Web Server**. **Server Address** nastavíme na **2**. Další položka, která nás bude zajímat je **Application**. Měnit budeme tyto nastavení:

- **Application: Destination Preferences** - provádí mapování symbolických jmen cíle definovaných v **Application Config**, se jmény klientů (Client name) nebo adresami (Server Address).
- **Application: Supported Profiles** - seznam profilů, které jsou na tomto objektu dostupné.
- **Application: Supported Services** – seznam aplikací, které budou k dispozici na tomto objektu

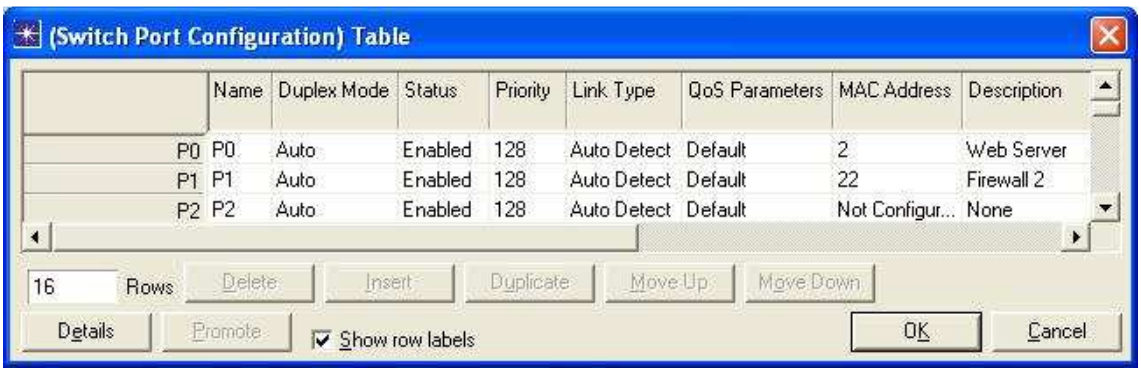
V **Application: Destination Preferences** nastavíme počet řádků (Number of Rows) na **1**. Vybereme aplikaci **Stream Video**. Vyplníme symbolické jméno na **Stream video viewer**. U položky **Actual name** zvolíme počet řádků 1 a v kolonce **Name** Vybereme jméno námi požadovaného cíle. V našem případě **STA1.** Dále musíme nastavit, jaké aplikace budou k dispozici v tomto objektu. Provedeme to nastavením **Application: Supported Services** na **All**. Nastavení Web serveru vidíte na obr. 4.5.



Obr. 4.5: Nastavení Web Serveru

Konfigurace přepínačů:

Na přepínačích musíme provést správné nasměrování portů na cílové MAC adresy. To provedeme editací položky **Switch Port Configuration -> Edit.** Otevře se nám okno, které je na obr. 4.6. Portu P0 u objektu **Switch 2** přiřadíme MAC adresu Web Serveru. **MAC Address -> 2**, **Description -> Web Server**. Portu P1 přiřadíme adresu **Firewallu 2. MAC Address -> 22**, **Description -> Firewall 2. Switch 1** bude konfigurován stejně, akorát budou jeho portům P0, P1 přiřazeny MAC adresy **AP** a **Firewallu 1.**



Obr. 4.6: Nastavení přepínače

Nastavení Firewalů:

Oba Firewally nejdříve pojmenujeme a nastavíme jejich serverové adresy.

Firewall 1: Server Address -> 11
Firewall 2: Server Address -> 22

U obou Firewallů nastavíme zpoždění průchodem Proxy. **Proxy Server Information -> Rows 7 -> Latency (secs) -> 0.0001.** Další nastavení bude stejné jako u Web Serveru.

Konfigurace Access Pointu (AP):

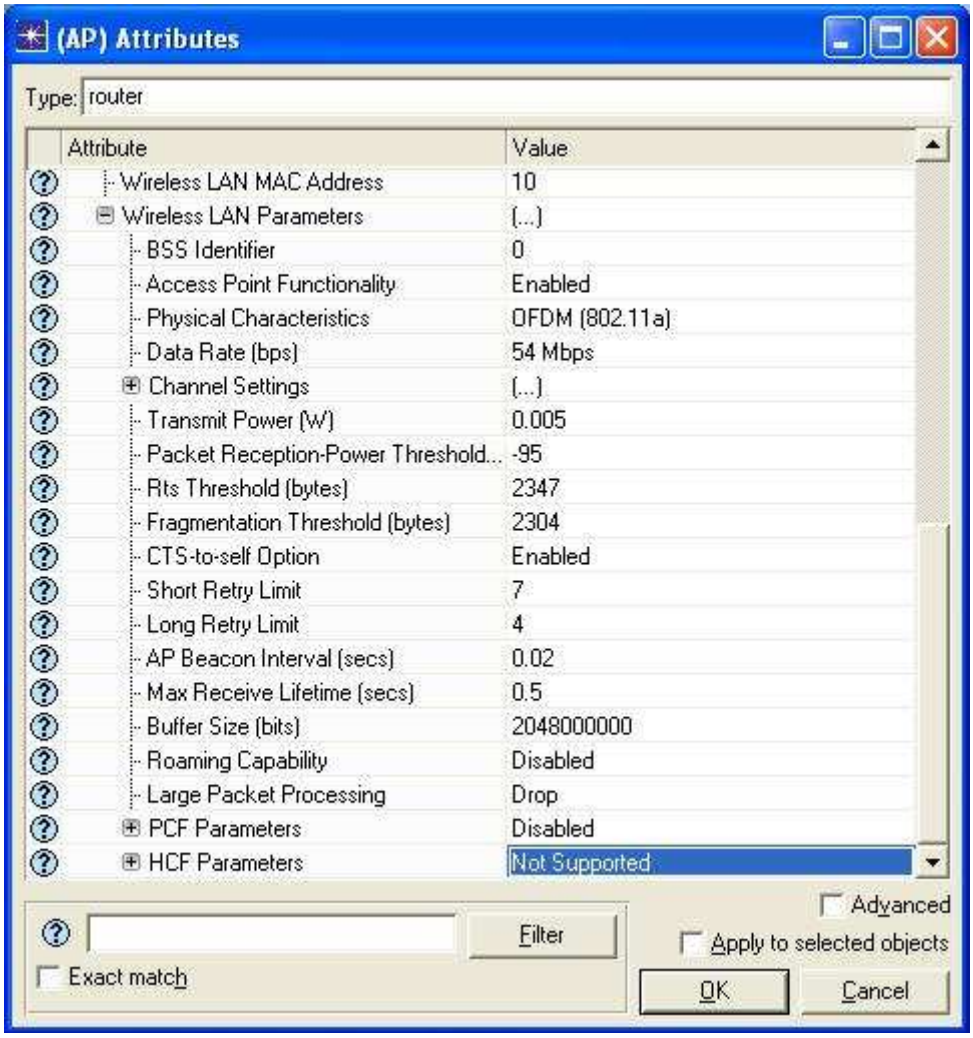
Access point v této síti slouží k propojení bezdrátové a metalické sítě. V naší síti AP spravuje pouze jednu stanici. Aby spolu mohli komunikovat, musí mít nastavený stejný identifikátor BSS, který nastavíme na **Wireless LAN -> Wireless LAN Parameters -> BSS Identifier -> 0.** Všechny klientské stanice musí mít stejný identifikátor BSS, aby se mohli připojit do této sítě.

Popis jednotlivých položek **Wireless LAN Parameters**:

Access Point functionality - povolení/zakázání funkce AP.
Physical Characteristic – určuje standard, který bude AP simulovat.
Transmit Power – udává vysílací výkon stanic ve watech.
Data Rate – určuje rychlost datového toku.
Buffer Size – určuje velikost vyrovnávací paměti pro vyšší vrstvy (bit/s).
Fragmentation Threshold – Práh fragmentace, udává hodnotu od které se data začnou dělit, na menší fragmenty.
CTS/RST Thresold – tato prahová hodnota říká, kdy bude místo přístupové metody CSMA/CA využívat systém zpráv RTS/CTS.
CTS-to-self Option - použití ochranného mechanismu CTS-to-self místo RTS/CTS.
Short Retry Limit – udává maximální počet pokusů o přenos pro rámce menší nebo stejně velké jako u Rts Threshold.
Long Retry Limit – udává maximální počet pokusů o přenos pro rámce větší nebo stejně velké jako u Rts Threshold.
AP Beacon Interval – udava periodu opakování rámce Beacon.
Roaming Capability – umožňuje hledání jiných AP, pokud dojde ke zhoršení signálu.

Konkrétní nastavení **Wireless LAN Parameters**:

Nejdříve musíme povolit funkci AP tím, že nastavíme **Access Point functionality** na **Enabled**. První scénář bude simulovat standard 802.11a, proto v **Physical Characteristic** vybereme **OFDM (802.11a).** Zvolíme maximální přenosovou rychlost **54 Mbit/s**. Zvětšíme velikost vyrovnávací paměti na **204800000 bitů**. Podrobnější nastavení AP vidíme na obr. 4.7.



Obr. 4.7: Nastavení AP

Konfigurace bezdrátové stanice:

V první řadě objekt pojmenujeme **Name -> STA 1** a nastavíme adresu **Client Address -> STA1**. Protože chceme, aby se stanice připojovala k AP, které jsme nastavovali výše, musíme nastavit **Wireless LAN Parameters** stejně jako u něho. Výjimka je pouze u **Access Point functionality**, která bude **Disabled.** Nakonec budeme editovat položku **Application**. V **Application: Supported Profiles** zvolíme **Edit.** Počet podporovaných profilů bude **1**. V **Profile Name** vybereme námi vytvořený profil **Internet Stream Video**. A nakonec **Application: Supported Services -> All.** Ještě se ujistíme, že stanice bude přijímat pakety aplikace streamového videa na portu UDP. To provedeme v **Application -> Application: Transport Protocol Specification -> Video Conference Transport -> UDP.**

4.4 Duplikace scénáře, nastavení sledovaných charakteristik a spuštění simulace:

Protože chceme vytvořit simulaci, která bude srovnávat standardy 802.11a, 802.11b, 802.11g a 802.11n, musíme si vytvořit duplicitní scénáře. Potom můžeme porovnávat jednotlivé charakteristiky mezi sebou. Duplicitní scénář vytvoříme klinutím v hlavním menu na **Scenarios -> Duplicate Scenario.** Takto vytvoříme další tři scénáře, které náležitě pojmenujeme podle příslušného standardu. Nakonec nesmíme zapomenout, překonfigurovat nastavení bezdrátových prvků sítě. U AP a bezdrátové stanice musíme změnit parametr **Wireless LAN -> Wireless LAN Parameters -> Physical Characteristic** a **Wireless LAN -> Wireless LAN Parameters -> Data Rate (bps)** aby odpovídal danému standardu.

Tímto je síť vytvořena a nakonfigurována. Teď už jen stačí vybrat vhodné charakteristiky. K tomu slouží **Individual DES Statistics**.

V OM slouží k vyobrazování výsledku simulací tři typy charakteristik:

- **Global statistic** - tento typ charakteristik určuje měřený parametr v rámci celé sítě.
- **Node Statistic** - tento typ charakteristik určuje měřený parametr pouze v rámci námi vybraného objektu.
- **Link Statistic** - tento typ charakteristik určuje měřený parametr mezi objekty.

V tomto projektu použijeme globální charakteristiky pro bezdrátové sítě pro měření zpoždění (Delay) a propustnost (Throuthput). A pak charakteristiky pro měření videokonferencí, konkrétně pro měření zpoždění (Packet End-to-End Delay) a kolísání zpoždění (Packet Delay Variation), které budou měřeny na bezdrátové stanici STA 1.

Nastavení parametrů simulace:

- **Duration** – doba trvání simulace. Vzhledem k velké náročnosti na výpočet při námi simulované aplikaci, nastavíme dobu trvání pouze na **10 minut**.
- **Values per Statistic** – udává počet naměřených hodnot, které budou vykreslovány do grafu charakteristiky. Platí, čím větší hodnota, tím je simulace delší, ale zato detailnější. V našem projektu nastavíme **100**.
- **Update interval** - udává, jak často se budě měnit křivka počtu událostí probíhající simulace.[5] Nastavíme hodnotu 100 000 událostí.
- **Simulation Kernel** – specifikuje způsob překladu modelu do spustitelného kódu.[5] Nastavíme Optimized.

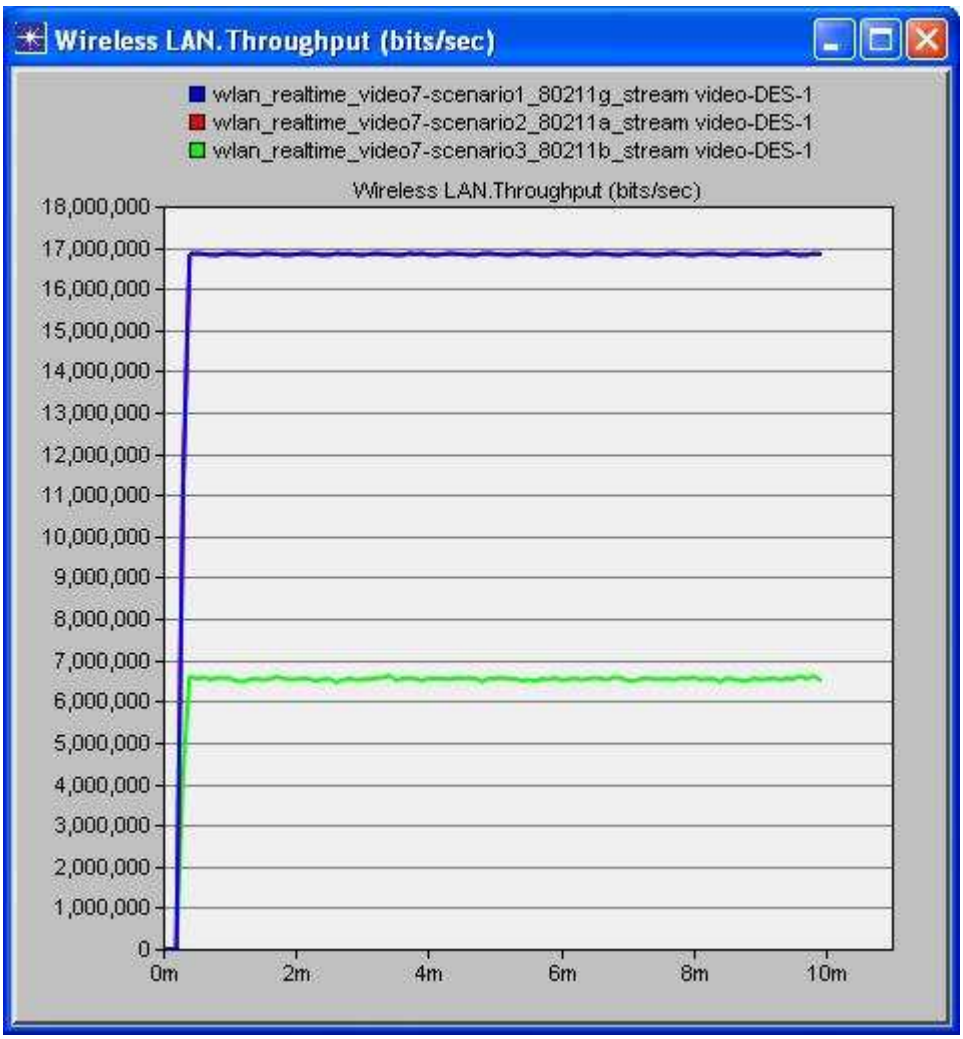
Tlačítkem **Run** spustíme simulaci. Naměřené grafy si můžeme prohlédnout, když klikneme kamkoli na pracovní plochu projektu pravým tlačítkem myši a vybereme **View Results**. Případné informace o průběhu simulace nebo chybová hlášení můžeme prohlížet v **DES Log**.

4.5 Zhodnocení naměřených výsledků

V této kapitole budu pomocí jednotlivých scénářů, porovnávat naměřené charakteristiky jednotlivých scénářů. K objektivnímu porovnání, nám poslouží funkce OM, která umožňuje seskupovat vybrané charakteristiky do jednoho grafu. Kliknutím na **View Results** se nám otevře **Results Browser**. Zde v menu **Results for:** vybereme **Current Project** a vybereme námi požadované projekty. A nakonec, aby se nám charakteristiky zobrazovali do jednoho grafu, zvolíme v menu **Presentation** volbu **Overlaid Statistics.** Pro přehlednost, jsem u všech uvedených grafů exportoval data do Excelu a vytvořil větší a přehlednější grafy, které jsem umístil do přílohy.

Propustnost WLAN:

Tato charakteristika udává celkový počet bitů, který je schopný projít z bezdrátové LAN vrstvy do vyšších vrstev na všech bezdrátových uzlech v síti. Z této charakteristiky na obr. 4.8 vidíme, v jak intenzivně simulovaná aplikace zatěžuje naši síť.

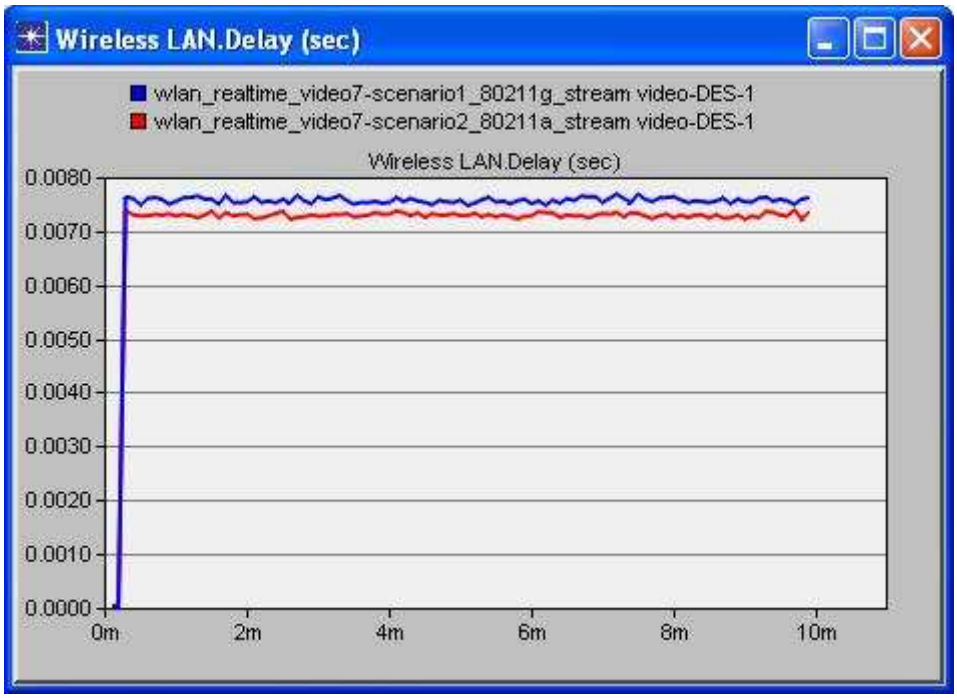


Obr. 4.8: Graf globální propustnosti ve WLAN síti

V úvodní kapitole bylo uvedeno, že skutečné rychlosti dosahované u standardu 802.11g jsou okolo 19 Mbit/s, 802.11a 23 Mbit/s a u 802.11b je to 6 Mbit/s. Z grafu na obr. č. 4.8 je vidět, že simulovaná aplikace u standardů 802.11g 802.11a, nevyužívá celé přenosové pásmo. Naměřené charakteristiky těchto dvou standardů se téměř překrývají a dosahují hodnoty okolo 17 Mbit/s. Při simulaci standardu 802.11b byla síť maximálně zatížena. Propustnost dosahovala hodnot okolo 6,5 Mbit/s Propustnost tohoto standardu je pro naši aplikaci nedostačující. Ostatně to uvidíme z dalších grafů.

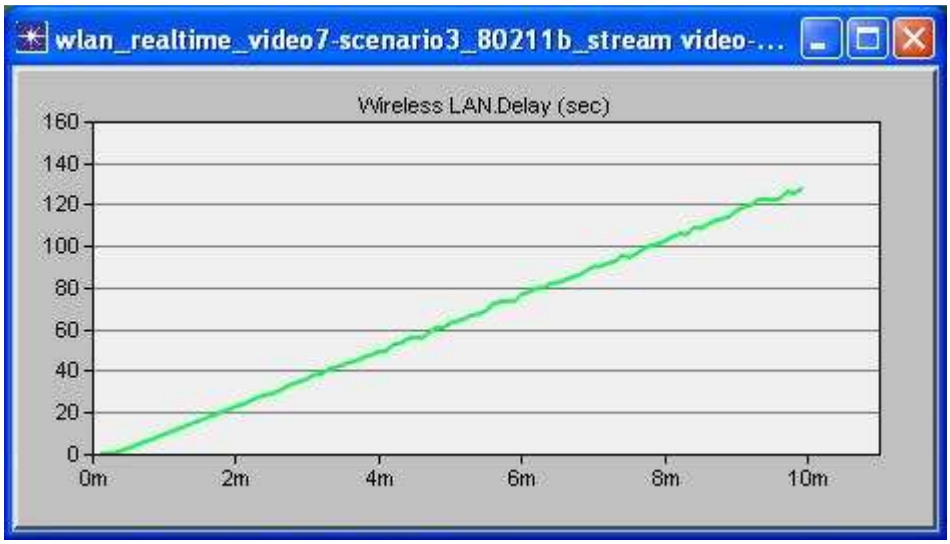
Zpoždění WLAN:

Tato charakteristika je definována jako celkové zpoždění tzv. End-to End všech paketů v bezdrátové síti přijatých MAC vrstvou a přeposlaných do vyšších vrstev. V tomto případě jsem zobrazil výsledky do dvou grafů, protože zpoždění u standardu 802.11b bylo tak výrazné a charakteristiky standardů 802.11g a 802.11a by byli oproti 802.11b téměř nulové. Z obr. 4.9 vidíme, že standard 802.11g dosahuje nepatrně většího zpoždění než standard 802.11a. Avšak naměřené hodnoty u obou standardů, které se pohybují v rozmezí od 7ms - 8ms jsou minimální a nijak nebudou omezovat chod sítě, nebo omezovat aplikaci.



Obr. 4.9: Graf globálního zpoždění v WLAN síti pro standardy 802.11g a 802.11a

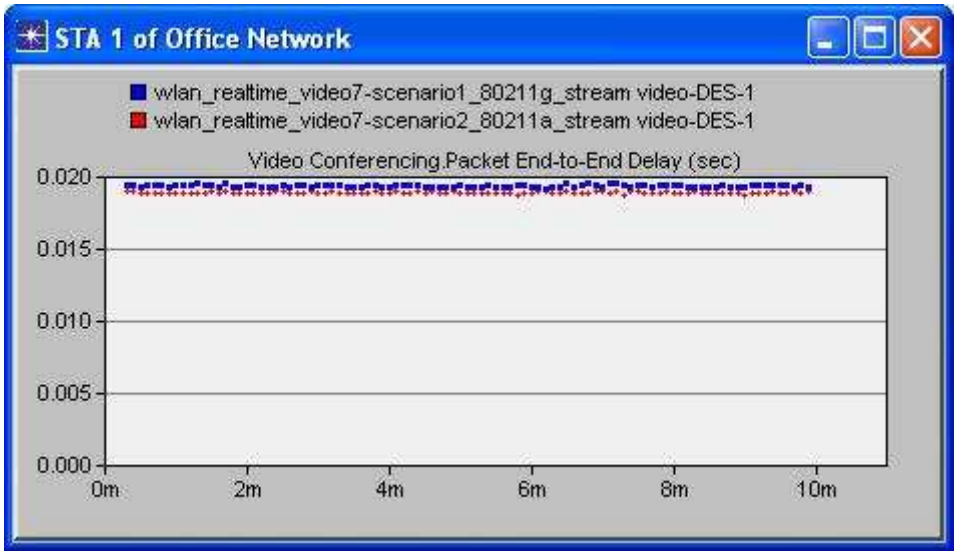
To se však nedá říci o standardu 802.11b. Hodnoty zpoždění jsou nepřijatelné. Jak vidíme na obr. 4.10, zpoždění lineárně narůstá až k hodnotám okolo 120s. Takové hodnoty zpoždění nejsou přijatelné pro žádnou síť ani aplikaci. Zpoždění je způsobeno nedostatečnou přenosovou kapacitou kanálu. Datový tok naší aplikace je příliš velký, AP jej nedokáže obsluhovat a dochází k ukládání do vyrovnávací paměti a k zahazování paketů, tím dochází k narůstání zpoždění.



Obr. 4.10: Graf globálního zpoždění v WLAN síti pro standard 802.11b

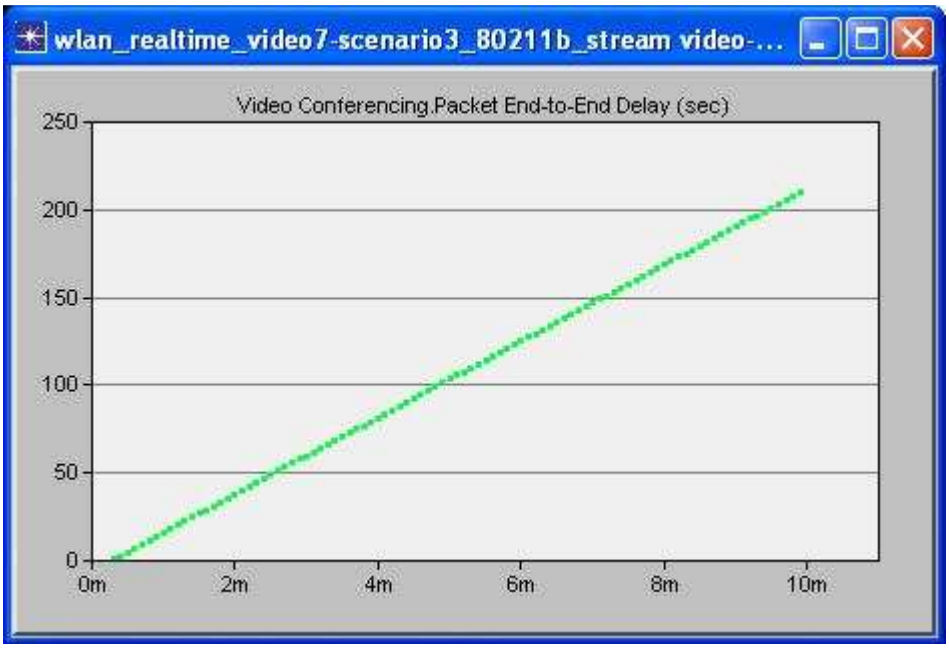
Zpoždění paketů streamového videa:

Doba zpoždění u této charakteristiky je dána dobou od odeslání paketů ze zdroje až po jeho přijmutí v cílové jednotce. V našem případě toto zpoždění udává dobu než se paket dostane z Web Serveru až k bezdrátové stanici STA1. Graf na obr. 4.11 potvrzuje pouze to, co bylo řečeno v minulých odstavcích. Zpoždění u standardů 802.11g a 802.11a je téměř konstantní a nepřesahuje hodnotu 20ms, což je pro naše účely plně dostačující.



Obr. 4.11: Graf zpoždění paketů streamového videa v síti pro standardy 802.11g a 802.11a

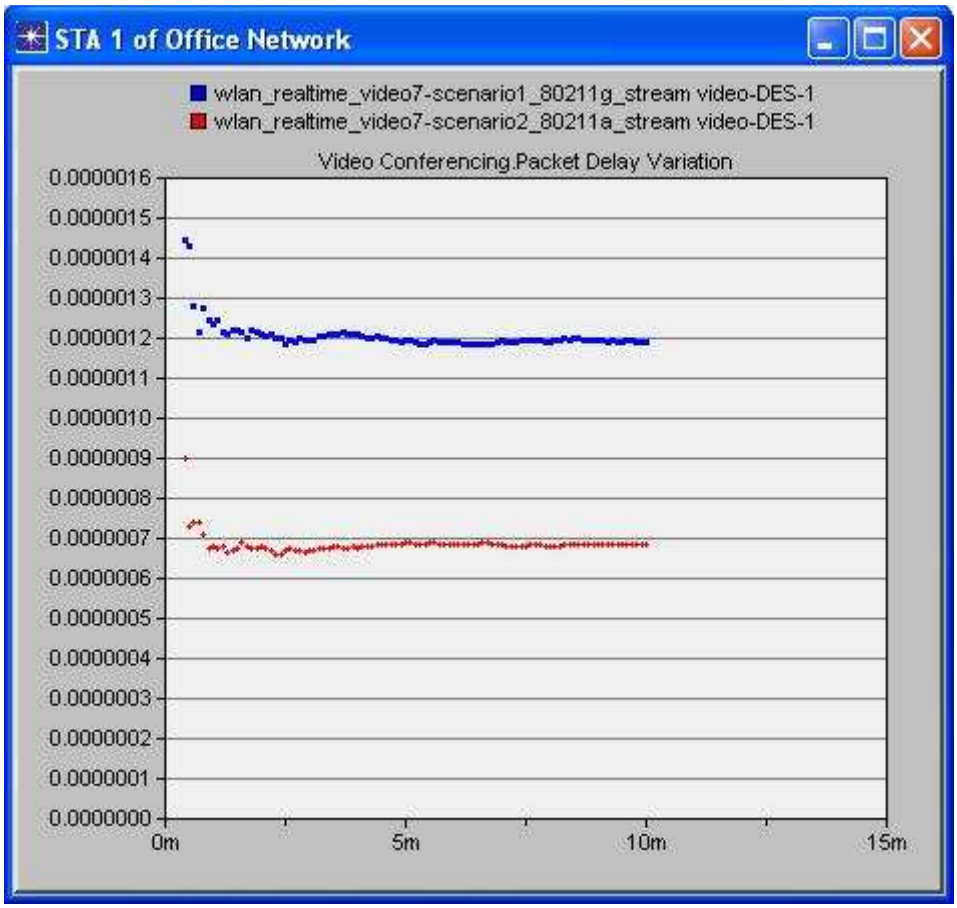
Z obr. 4.12 vidíme, že zpoždění paketů aplikace je také nevyhovující. Což je pochopitelné, z předcházejícího textu. Zpoždění lineárně roste až k hodnotám přes 200s.



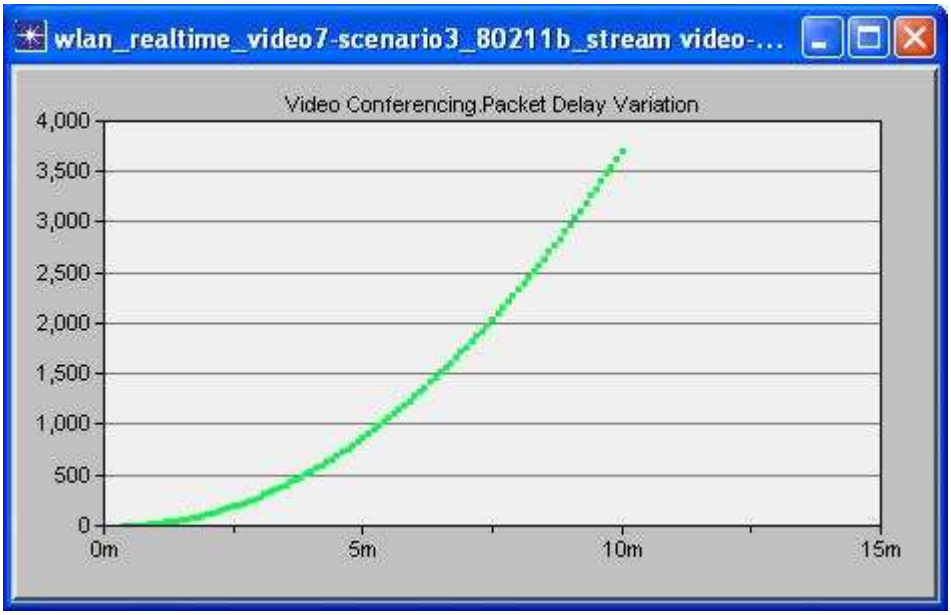
Obr. 4.12: Graf zpoždění paketů streamového videa v síti pro standard 802.11b

Kolísání zpoždění paketů streamového videa:

Tato charakteristika udává, v jakém rozmezí kolísá zpoždění paketů dané aplikace. Požadavek u aplikací přenosu dat v reálném čase je, aby zpoždění kolísalo co nejméně. Tedy aby datové jednotky přicházeli k cílové stanici v pravidelných intervalech. Pro zajištění tohoto požadavku je do sítí zaváděna QoS, která upřednostňuje pakety s větší prioritou. Z grafu na obr. 4.13 je vidět jak kolísá zpoždění v průběhu simulace. U obou standardů je vidět, že na počátku přenosu dat dochází k většímu kolísání, které se však během simulace ustálí. Lepších výsledků bylo dosaženo opět u standardu 802.11a. Jeho hodnota byla pod 0,7µs. U standardu 802.11g to byla hodnota okolo 1,2µs U standardu 802.11b, jak vidíme z obr. 4.14, hodnota exponenciálně narůstala.



Obr. 4.13: Graf kolísání zpoždění paketů streamového videa v síti pro standard 802.11g a 802.11a



Obr. 4.14: Graf kolísání zpoždění paketů streamového videa v síti pro standard 802.11b

6. Závěr:

V této práci jsem se seznámil se standardem 802.11n. Snažil jsem se popsat jeho hlavní charakteristické rysy a jeho nové nebo převzaté součásti, které slouží k požadovanému navýšení rychlosti. Výrazný posun oproti 802.11a a 802.11g je v použití agregace na MAC vrstvě a technologie MIMO na vrstvě fyzické. Není pochyb, že 802.11n přináší znatelné zrychlení do bezdrátových sítí. Jak velké toto navýšení bude, si asi budeme muset počkat do úplného schválení standardu, které je stále zatím v nedohlednu. Jistě můžeme říct, že podle prvních testů nepůjde propustnost na MAC vrstvě pod 100Mb/s. Důležitým faktorem pro masovější rozšíření bude to, jaká bude zpětná kompatibilita s původními zařízeními. Pokud nenastanou komplikace s připojováním starších standardů, nebo pokud nebudou tyto starší zařízení příliš zpomalovat síť, nebude nic bránit velkoplošnému rozšíření standardu 802.11n. Trochu zklamán jsem byl ohledně zabezpečení. Ochrana WPA/WPA2 je sice pro stávají uživatele ve většině případů dostačující, ale vývojáři mohli tuto ochranu přinejmenším vylepšit. Hlavně z toho důvodu, jak jsem psal již výše, že již byla prolomena. Podle cen, za které se prodávají již certifikovaná zařízení, můžeme usoudit, že zařízení budou určena pro širokou veřejnost. Standard najde uplatnění jak pro menší domácí sítě, tak i pro rozsáhlé firemní sítě, ale také pro venkovní použití, zejména hlavně kvůli eliminaci odražených signálů díky diverzně antén. V rámci navazující bakalářské práce se budu snažit podrobněji prostudovat tento standard a detailněji popsat jeho součásti.

V praktické části jsem se snažil o implementaci existujících modelů a následující simulaci. Po mnoha problémech, které jsem popisoval v kapitole 4.1, se mi simulaci s modely 802.11n podařilo spustit, avšak v síti se negenerovala žádná doprava. Podle mého mínění je problém ve funkci, která obstarává adresaci stanic. Příčina je podle mě nejspíše v tom, že model je odladěn na jiné verzi Opnet Modeleru. Po konzultaci s vedoucím jsme se dohodli, že simulace bude obsahovat pouze standardy 802.11a, b, g. Síť byla navržena tak, aby odpovídala reálné topologii. Pomocí mraku IP je simulována síť Internet, pomocí které se koncový uživatel může připojit k webovému serveru a získávat data ve formě stremového videa. Z důvodu bezpečnosti je bezdrátová síť a server odděleny bránami Firewall. Z výsledků simulace v kapitole 4.5 je vidět, že standard 802.11b, již svojí propustností moderním aplikacím nedostačuje. V síti s tímto standardem byli naměřená velká zpoždění a tento standard je pro aplikace v reálném čase nevhodný. Výsledky standardů 802.11g a 802.11a dopadli velice podobně. Propustnosti obou standardů byly téměř totožné. Co se týče zpoždění, byl na tom o něco lépe standard 802.11a, avšak ten rozdíl byl minimální. S jistotou můžeme říct, že oba standardy 802.11a a 802.11g jsou vhodné pro přenos streamového videa v tomto rozlišení. Avšak nároky na síťové prvky neustále rostou, to způsobí, že za určitou dobu se propustnost těchto standardů stane nedostačující a právě proto je vyvíjen nový standard 802.11n, který by měl být budoucností bezdrátových sítí.

Seznam literatury a použitých zdrojů:

[1] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* [online]. 2007 [cit. 2008-11-1]. Dostupný z URL: <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>.

[2] KIM Y.; CHOI S.; JANG K.; HWANG H. *Throughput Enhancement of IEEE 802.11 WLAN via Frame Aggregation* [online]. 2004 [cit. 2008-11-15]. Dostupný z URL: < http://www.mwnl.snu.ac.kr/~schoi/publication/Conferences/04-VTC-Frame_aggregation.pdf>

[3] KOCUR Z.; ŠAFRÁNEK M**.** *Fyzická vrstva Wi-Fi* [online] 2008 [cit. 2008-10-28]. Dostupný na URL: <http://access.feld.cvut.cz/rservice.php?akce=tisk&cisloclanku=2008050006>

[4] LEHEMBRE, G. *Bezpečnost Wi-Fi - WEP, WPA a WPA2, Hakin9* [online]. 2006, vol. 1 [cit. 2009-12-11]. Dostupný z URL: < www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf>.

[5] MOLNÁR K.; ZEMAN O.; SKOŘEPA M. *Moderní síťové technologie – Laboratorní cvičení* [online]. VUT v Brně, 2008. Dostupný z URL: <http://www.utko.feec.vutbr.cz/~molnar/mmos/MMOS_lab.pdf>

[6] PERAHIA, E. IEEE 802.11n Development: History, Process, and Technology. *Communications Magazine, IEEE* [online]. 2008, vol. 46, is. 7 [cit. 2008-11-10], s. 48-55. Dostupný z WWW: <http://ieeexplore.ieee.org/Xplore/login.jsp?url=/stamp/stamp.jsp?arnumber=4557042&isnumber=4557031>. ISSN 0163-6804.

[7] PERAHIA E.; STACEY R. *Next Generation wireless LANs: Throughtput, Robustness, and Reliabity in 802.11n*, Cambrige Univ. Press, 2008

[8] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno: Computer Press, 2005. 179 s. ISBN 80-251-0791-4.

[9] SIDELNIKOV A.; YU J.; CHOI S.; *Fragmentation/Aggregation Scheme for Throughput Enhancement of IEEE 802.11n WLAN* [online]. 2006 [cit. 2008-11-15]. Dostupný z URL: <http://www.mwnl.snu.ac.kr/~schoi/publication/Conferences/06-APWCS.pdf>

[10] ZANDL, P. *Bezdrátové sítě WiFi : Praktický průvodce*. 1. vyd. Brno : Computer Press, 2003. 204 s. ISBN 80-7226-632-2.

[11] ŠKODÁK, Jaroslav. *Zabezpečení bezdrátových sítí 802.11*. Brno, 2008. 75 s. VUT. Vedoucí bakalářské práce Koutný Martin

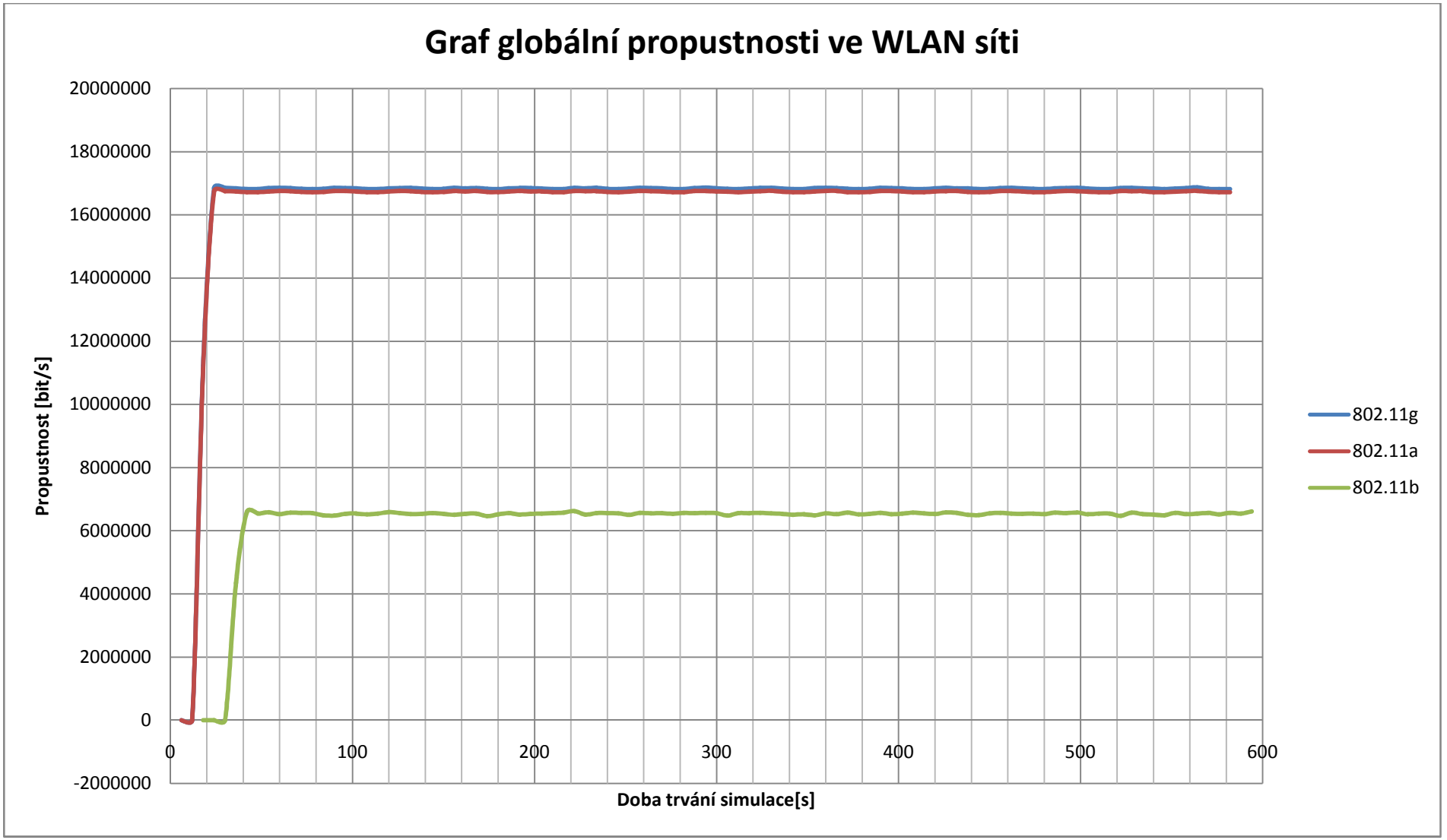
[12] FUJITSU, INC. *Beamforming Boosts the Range and Capacity of WiMAX Networks.* [online]. 2008 [cit. 2009-04-15] Dostupný z URL: <http://www.fujitsu.com/downloads/MICRO/fma/formpdf/WiMAXbeamform.pdf>

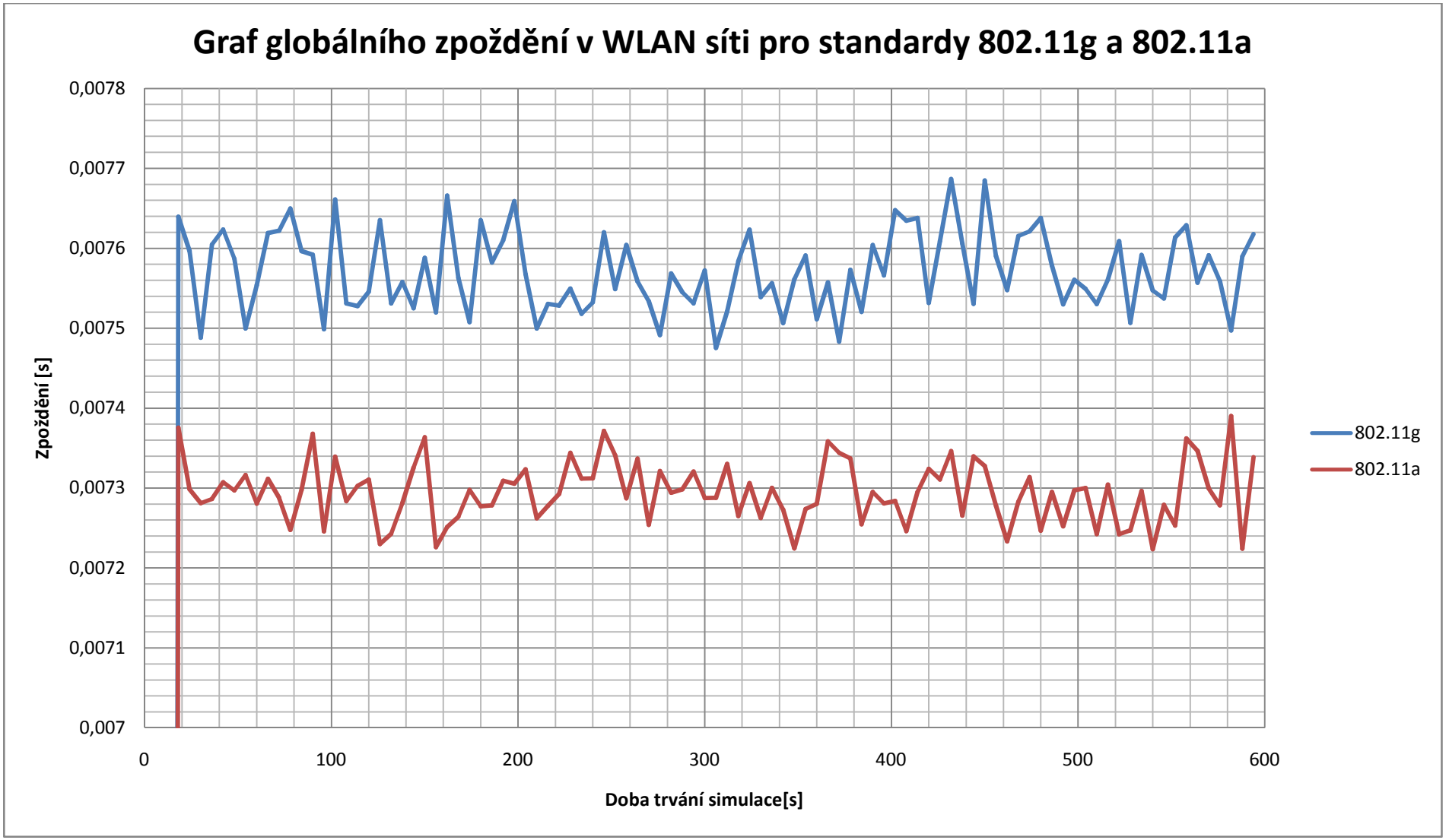
Abecední přehled použitých zkratek:

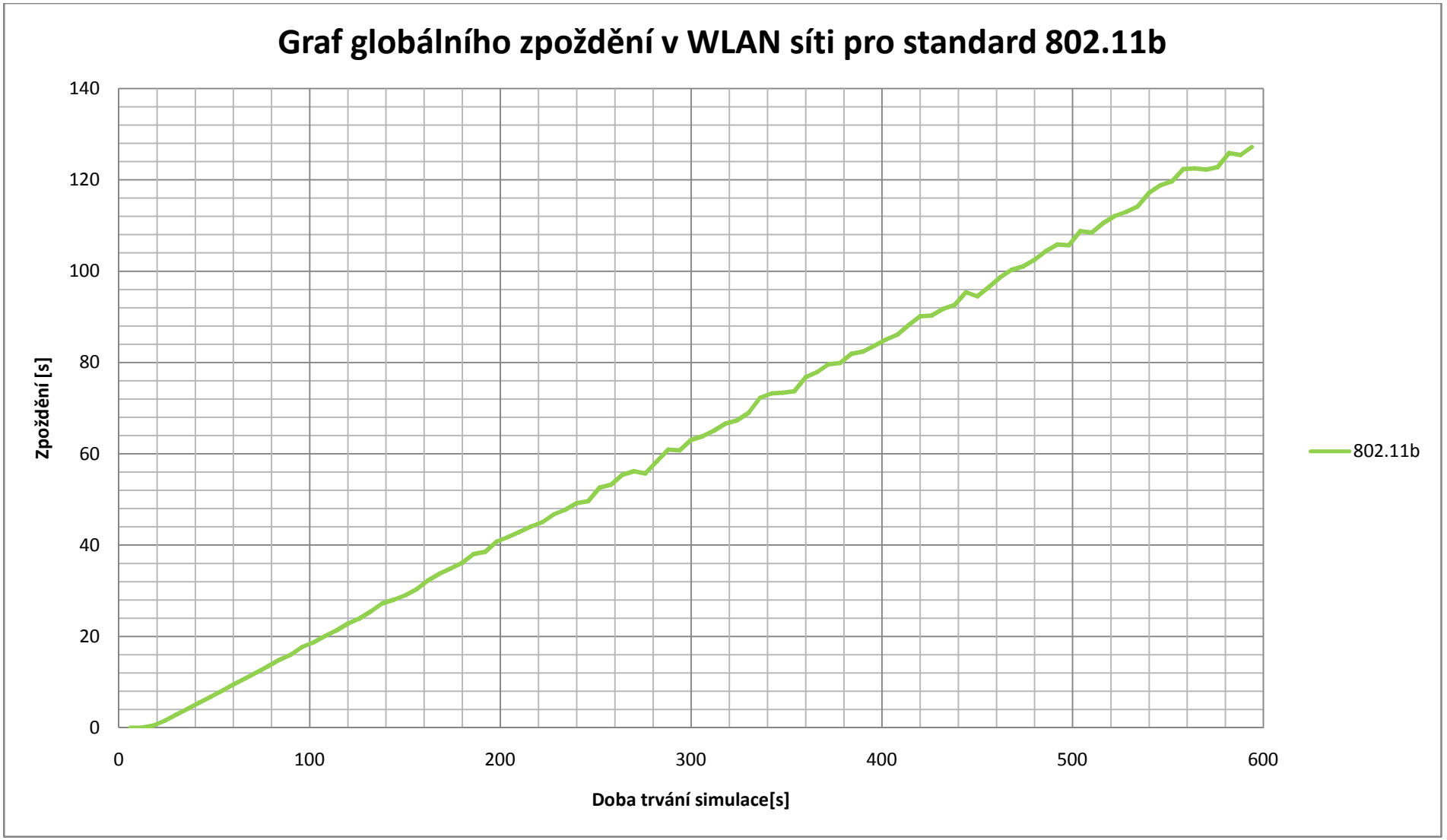
ACK - Acknowledgement
AES - Advanced Encryption Standard
AIFS - arbitration inter-framespace
A-MPDU - MAC protocol data unit aggregation
A-MSDU - MAC service data unit aggregation
AP - Access-point
BA - Block Acknowledgement
BAR - Block Acknowledgement Request
BPSK - Binary Phase-shift keying
BSS - Basic Service Set
C/I - Carrier to Interference
CCA - Clear Channel Assessment
CCK – Complimentary Code Keying
CCMP - Counter-Mode with Cipher Block Chaining Message Authentication Code Protocol
CRC - Cyclic Redundancy Check
CSMA/CA - Carrier Sense Multiple Access With Collision Avoidance.
CSMA/CD - Carrier Sense Multiple Access With Collision Detection
DIFS - DCF inter-frame space
DSSS - Direct Sequence Spread Spectrum
EDCA - Enhanced Distributed Channel Access
FCS - Frame Check Sequence
FHSS -Frequency Hopping Spread Spectrum
FSK - Frequency-shift keying
GI - Guard Interval
HCF – Hybrid Coordinate Function
HCCA -HCF controlled channel access
HDTV - High Definition TV
Hi-Fi - High Fidelity
IEEE - Institute of Electrical and Electronics Engineers
IPTV - Internet Protocol TV
IrDA - Infrared Data Association
LAN - Local Area Network
LDPC - Low-density Parity-check Code
LLC - Logical Link Control
MAC - Media Access Control
MIC - Message Intergity Check
MIMO - Multiple Input Multiple Output
MPDU - MAC Protocol data unit
MSDU - MAC Service Data Unit.
OFDM - Orthogonal Frequency Division Multiplexing
OOK - On-Off Keying
PDA - Personal Digital Assistant
PHY - Physical Layer
PLCP - Physical Layer Convergence Procedure
PMD - Physical Medium Dependent
PMM - Pulse-position Modulation

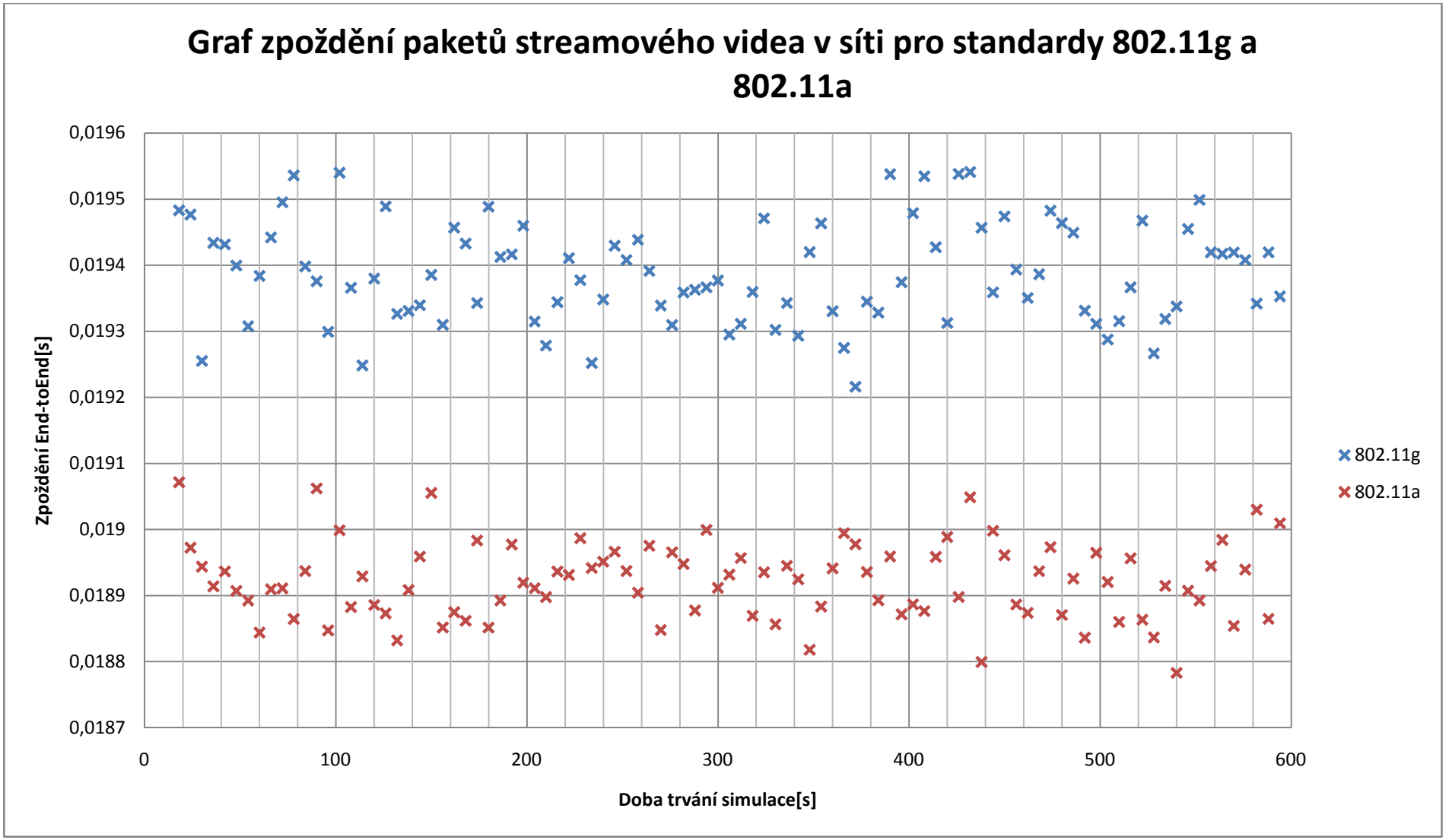
PPDU - Protocol data unit
PSK - Phase-shift keying
PSK - Pre-shared key
PSMP - Power Save Multi-Poll
QAM - Quadrature Amplitude Modulation
QoS - Quality of Service
QPSK - Quadrature Phase-shift keying
RDG - Reverse direction grand
RIFS - Reduced inter-frame sparing
RSN - Robust Security Network
RTS/CTS - Request To Send/ Clear to Send
SDM - Space Division Multiplex
SNR - Signal-to-Noise Ratio
STBC - Space–time Block Coding
TCP/IP - Transmission Control Protocol/Internet Protocol
TKIP - Temporal Key Integrity Protocol
TXOP - Transmit Opportunity
VoIP - Voice over Internet Protocol
WEP - Wired Equivalent Privacy
Wi-Fi - Wireless Fidelity
WLAN - Wireless Local Area Network
WPA - Wi-Fi Protected Access
WWiSE - World-Wide Spectrum Efficiency

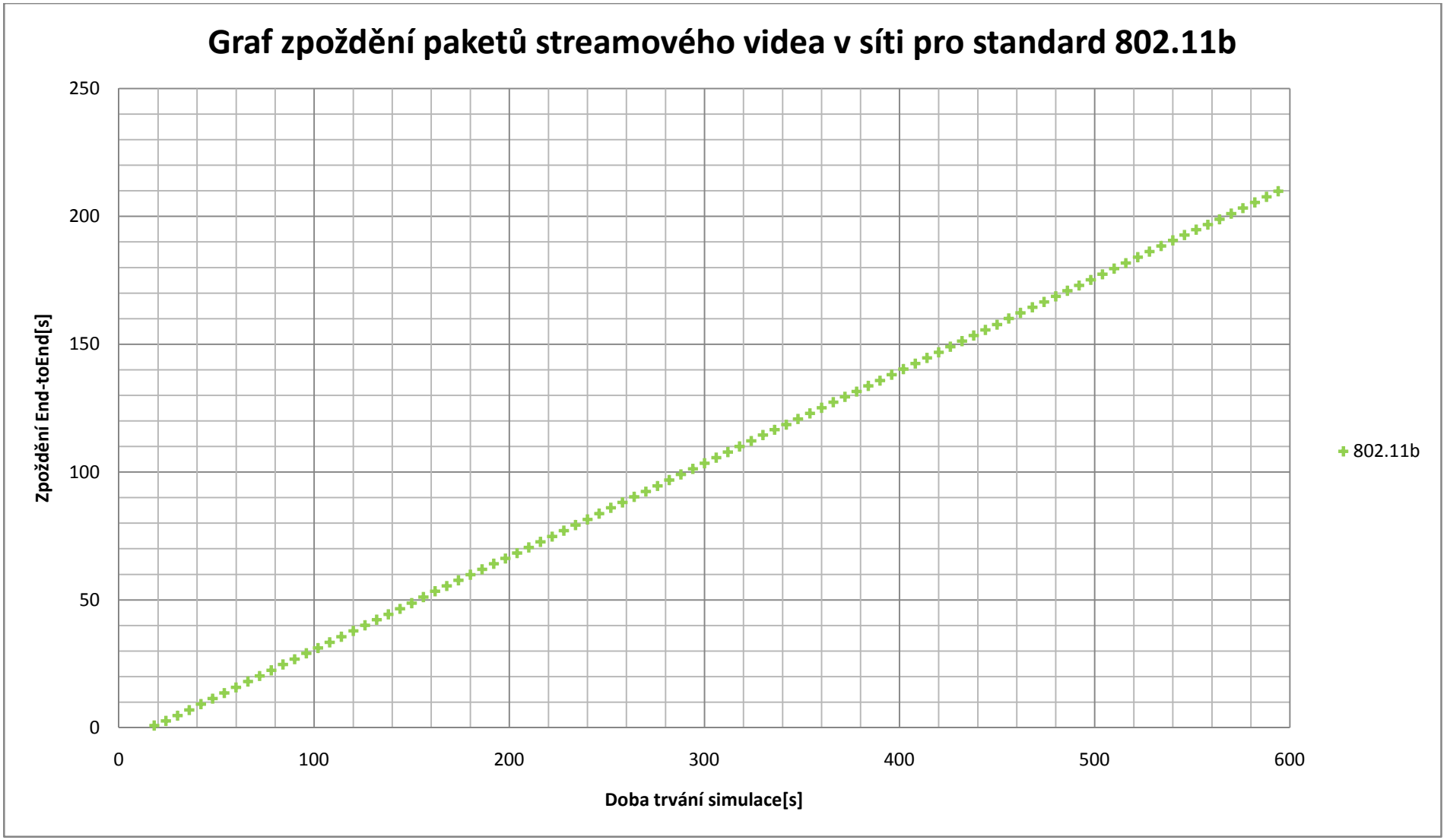
Seznam příloh:

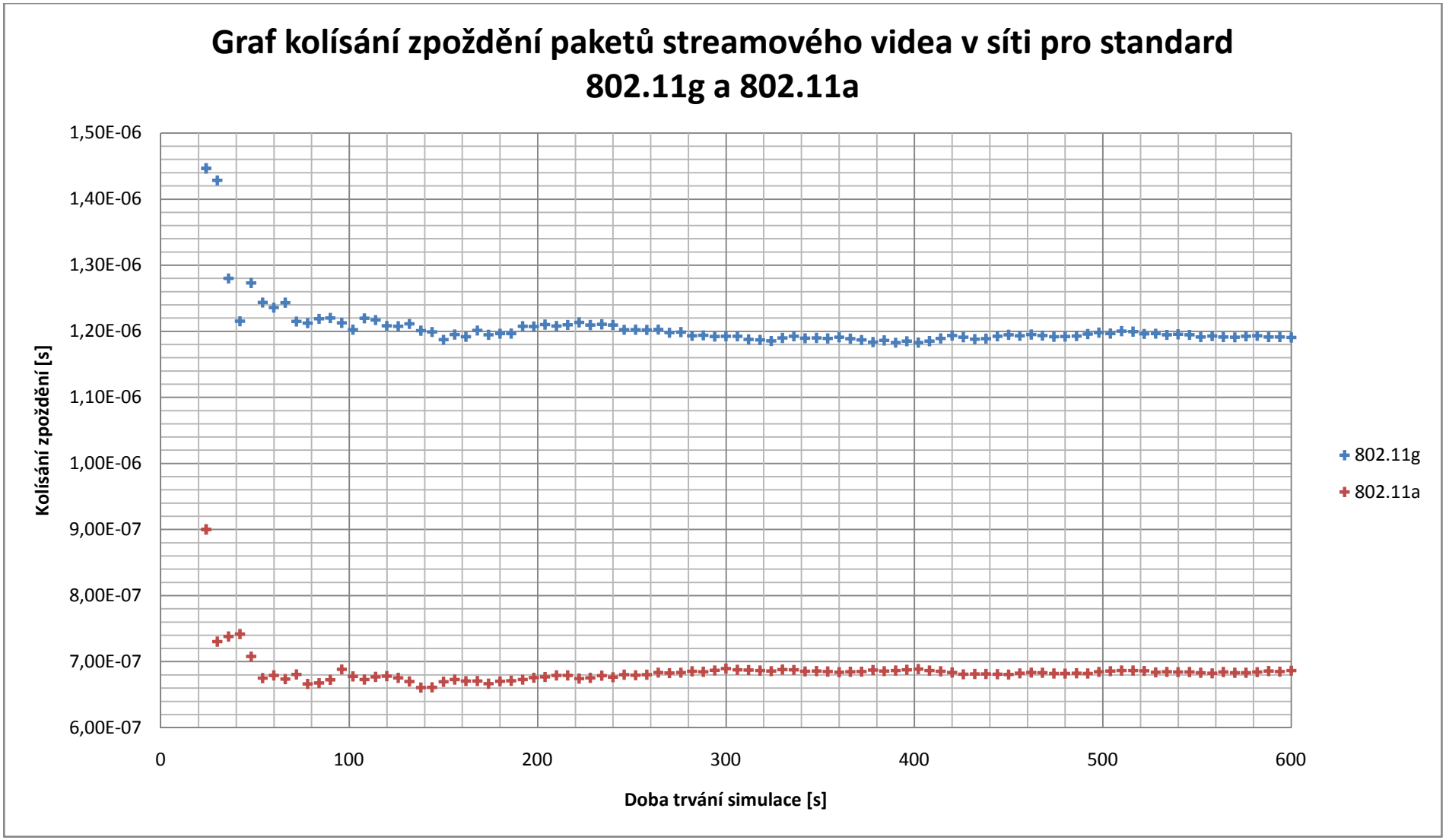

Graf globální propustnosti ve WLAN síti
Propustnost [bit/s]
20000000
18000000
16000000
14000000
12000000
10000000
8000000
6000000
4000000
2000000
0
-2000000
0
100
200
300
400
500
600
Doba trvání simulace[s]
802.11g
802.11a
802.11b

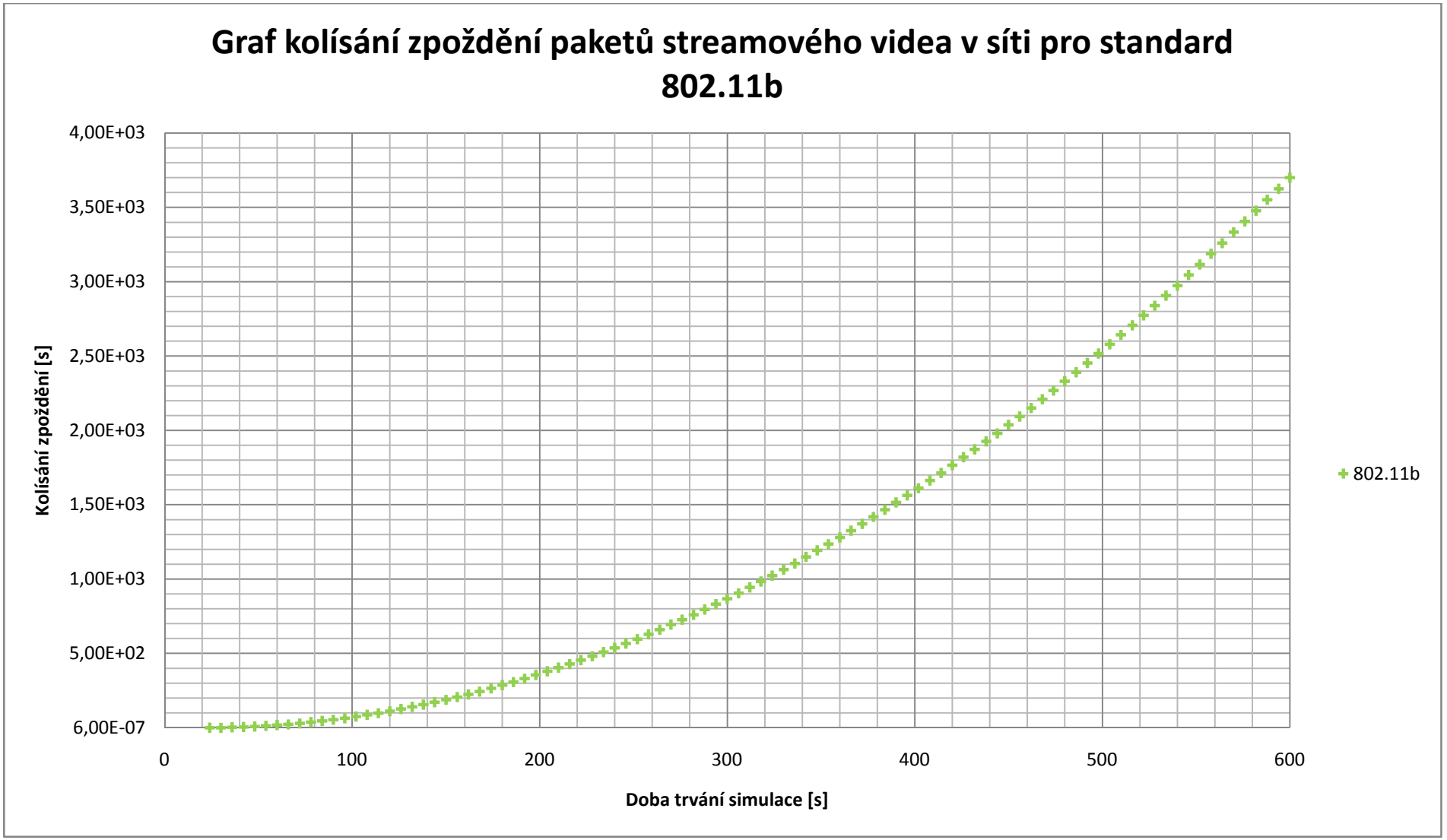

Graf globálního zpoždění v WLAN síti pro standardy 802.11g a 802.11a
0,0078
0,0077
0,0076
0,0075
0,0074
0,0073
0,0072
0,0071
0,007
Zpoždění [s]
0
100
200
300
400
500
600
Doba trvání simulace[s]
802.11g
802.11a


Graf globálního zpoždění v WLAN síti pro standard 802.11b
Zpoždění [s]
140
120
100
80
60
40
20
0
0
100
200
300
400
500
600
Doba trvání simulace[s]
802.11b


Graf zpoždění paketů streamového videa v síti pro standardy 802.11g a 802.11a
0,0196
0,0195
0,0194
0,0193
0,0192
0,0191
0,019
0,0189
0,0188
0,0187
Zpoždění End-toEnd[s]
0
100
200
300
400
500
600
Doba trvání simulace[s]
802.11g
802.11a


Graf zpoždění paketů streamového videa v síti pro standard 802.11b
Zpoždění End-toEnd[s]
250
200
150
100
50
0
0
100
200
300
400
500
600
Doba trvání simulace[s]
802.11b


Graf kolísání zpoždění paketů streamového videa v síti pro standard 802.11g a 802.11a
1,50E-06
1,40E-06
1,30E-06
1,20E-06
1,10E-06
1,00E-06
9,00E-07
8,00E-07
7,00E-07
6,00E-07
Kolísání zpoždění [s]
0
100
200
300
400
500
600
Doba trvání simulace [s]
802.11g
802.11a


Graf kolísání zpoždění paketů streamového videa v síti pro standard 802.11b
4,00E+03
3,50E+03
3,00E+03
2,50E+03
2,00E+03
1,50E+03
1,00E+03
5,00E+02
6,00E-07
Kolísání zpoždění [s]
0
100
200
300
400
500
600
Doba trvání simulace [s]
802.11b