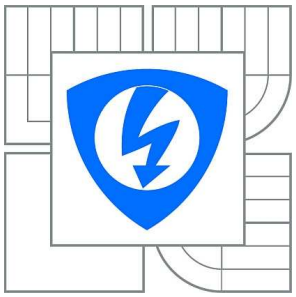
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA ZÁVISLOSTI MODERNÍCH KOMUNIKAČNÍCH SLUŽEB A KANÁLŮ NA ZPOŽDĚNÍ, OPTIMALIZACE QOS

ANALYSIS OF DELAY DEPENDENCE OF MODERN COMMUNICATION SERVICES AND CHANNELS, QOS OPTIMIZATION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

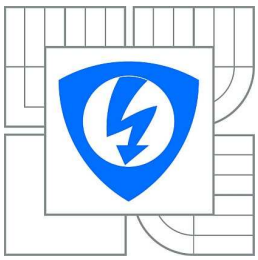
AUTOR PRÁCE — Bc. JIŘÍ ROZMAN

AUTHOR

VEDOUCÍ PRÁCE — Ing. PAVEL ENDRLE

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Jiří Rozman	***ID:***	72903
Ročník:	2	***Akademický rok:***	2011/2012

NÁZEV TÉMATU:

Analýza závislosti moderních komunikačních služeb a kanálů na zpoždění, optimalizace QoS

POKYNY PRO VYPRACOVÁNÍ:

Podrobně popište parametry a využitelnost zajištění kvality služeb (QoS) v bezdrátových sítích pro standardy IEEE 802.11 a/b/g/n. Analyzujte provoz na počítačové síti v závislosti na přenosu hlasu a videa. Zaměřte se na protokoly zajišťující přenos dat v reálném čase. V prostředí Opnet Modeler vytvořte bezdrátovou lokální síť, ve které nakonfigurujte mechanismy pro zajištění kvality služeb daných standardů. Vytvořte simulaci porovnávající technologie 802.11 a/b/g/n z hlediska přenosu dat citlivých na zpoždění. Navrhněte opatření pro zajištění QoS na dané síti a porovnejte výsledky.

DOPORUČENÁ LITERATURA:

[1] Bigelow, S., J.: Mistrovství v počítačových sítích. Nakladatelství CPRESS 2004. ISBN 80-251-0178-9.
[2] Matas, J.: Linux jako brána do sítě Internet. [Bakalářská práce]. Ústav Telekomunikací FEKT VUT v Brně. 2007.
[3] BARKEN, Lee. Wi-Fi : jak zabezpečit bezdrátovou síť. 1. vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.
[4] ZANDL, Patrick. Bezdrátové sítě WiFi. 2003. 204 s. ISBN 80-722-6632.

Termín zadání:	6.2.2012	***Termín odevzdání:***	24.5.2012

Vedoucí práce: Ing. Pavel Endrle
Konzultanti diplomové práce:

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

ABSTRAKT

Hlavním obsahem práce je seznámení se s možnostmi služeb využívajícími přenos dat v reálném čase v bezdrátových sítích. Teoretická část prezentuje bezdrátové sítě založené na standardu IEEE 802.11 a jejich využití v praxi. Velká část je věnována standardu 802.11e zajišťujícím podporu kvality služeb pro bezdrátové sítě. Dále pak práce řeší transportní protokoly a aplikační protokoly zajišťující multimediální přenos dat po síti. Druhá kapitola je věnována analýze reálné počítačové sítě za účelem proměření parametrů ovlivňujících kvalitu služeb, kterými jsou šířka pásma, zpoždění, jitter a ztrátovost. Poslední část práce se zabývá samotným návrhem bezdrátové sítě v prostředí OPNET Modeler za účelem simulace parametrů působících na kvalitu služeb.

KLÍČOVÁ SLOVA

IEEE 802.11, bezdrátová síť, kvalita služeb – QoS, MOS faktor, zpoždění, ztrátovost, jitter, šířka pásma, OPNET Modeler

ABSTRACT

The main aim of this thesis is to familiarize with options of services using real-time data transfer in wireless networks. Theoretical part presents wireless network based on IEEE 802.11 standard and its practical use. Large part is focuses on 802.11e standart, that provides support for quality of service in wireless networks. Furthemore this thesis deals with transport and applicaton protocols supporting multimedia streaming over computer network. Second chapter is focused on analyzing real computer network with purpose in measuring parametrs influencing quality of service such as bandwith, delay, jitter and loss. Last part deals with the design of wireless network in OPNET Modeler enviroment with focus on simulating parameters that influence quality of service.

KEYWORDS

IEEE 802.11, wireless network, quality of service – QoS, MOS factor, delay, loss, jitter, bandwidth, OPNET Modeler

ROZMAN, J. *Analýza závislosti moderních komunikačních služeb a kanálů na zpoždění, optimalizace QoS*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2012. 52 s. Diplomová práce. Vedoucí práce: Ing. Pavel Endrle.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma Analýza závislosti moderních komunikačních služeb a kanálů na zpoždění, optimalizace QoS jsem vypracoval samostatně pod vedením vedoucího diplomové 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 diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce Ing. Pavlu Endrle za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce.

V Brně dne ....

(podpis autora)

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

OBSAH

Seznam obrázků x

Seznam tabulek xi

Seznam Grafů xii

Úvod 1

1 Teoretický úvod 2

1.1 Modely sítě ... 2

1.2 Využívané technologie ... 2

1.3 Bezdrátové sítě ... 3

1.3.1 Standard 802.11 ... 3

1.3.2 Standard 802.11b ... 3

1.3.3 Standard 802.11g ... 4

1.3.4 Standard 802.11a ... 4

1.3.5 Standard 802.11n ... 4

1.3.6 Rozdělení kanálů ... 5

1.3.7 Definice rámce ... 5

1.3.8 Standard 802.11e – Kvalita služeb ... 6

1.3.9 Zabezpečení Wi-Fi ... 9

1.4 Transportní vrstva ... 9

1.4.1 Protokol TCP ... 10

1.4.2 Protokol UDP ... 11

1.5 Aplikační vrstva ... 12

1.5.1 Protokol RTP ... 12

1.5.2 Protokol SIP ... 14

1.5.3 Protokol RTSP ... 14

1.5.4 VoIP kodeky ... 14

2 Měření na síti 15

2.1 Parametry QoS ... 16

2.1.1 Šířka pásma ... 16

2.1.2 Zpoždění ... 16

2.1.3 Jitter ... 17

2.1.4 Ztrátovost ... 17

2.2 MOS faktor ... 17

2.3 Zapojení měřené sítě ... 18
2.4 Analýza SIP provozu VoIP ... 19
2.5 Analýza MOS faktoru ... 19
3 Návrh sítě v prostředí opnet modeler 26
3.1 Program OPNET Modeler ... 26
3.2 Návrh bezdrátové sítě ... 27
3.2.1 Vytvoření modelu ... 27
3.2.2 Nastavení WLAN sítě ... 28
3.2.3 Nastavení Aplikací ... 30
3.2.4 Natavení profilů ... 33
3.2.5 Nastavení aplikací na stanicích a serverech ... 36
3.2.6 Nastavení připojení k Internetu ... 39
3.2.7 Nastavení simulace ... 40
3.2.8 Duplikování scénáře ... 41
3.3 Výsledky simulace ... 42
3.3.1 Statistiky WLAN ... 43
3.3.2 Statistiky Hlasových služeb ... 45
3.3.3 Statistika datových služeb ... 47
3.3.4 Statistika Video přenosu ... 49
3.3.5 Srovnání výsledků simulace standardů 802.11 ... 49
Závěr 51
Literatura 53
Seznam zkratek 54
Přílohy 55

SEZNAM OBRÁZKŮ

Obr. 1 Modely sítě 2
Obr. 2 TCP segment 11
Obr. 3 UDP Datagram 11
Obr. 4 Testovaná síť pro MOS faktor 18
Obr. 5 Nastavení WAN portu na směrovači Draytek 19
Obr. 6 Analýza SIP protokolu 19
Obr. 7 Prostředí WANem 20
Obr. 8 Schéma zapojení v OPNET Modeleru 28
Obr. 9 Nastavení parametrů WiFi sítě 30
Obr. 10 Nastavení Hlasové aplikace 33
Obr. 11 Profil aplikace Hlasových služeb 36
Obr. 12 Nastavení aplikace na klientské stanici 37
Obr. 13 Nastavení aplikace na serveru 38
Obr. 14 Nastavení přepínače 40
Obr. 15 Nastavení simulace scénářů 42
Obr. 16 Zpoždění na Routeru 43
Obr. 17 Data přeposílaná směrovačem 44
Obr. 18 Znovu zasílaná data 45
Obr. 19 Statistika jitteru 45
Obr. 20 Statistika MOS 46
Obr. 21 Statistika zpoždění 47
Obr. 22 Odpovědi Web Serveru 48
Obr. 23 Odpovědi FTP Serveru 48
Obr. 24 Video posílané po síti 49
Obr. 25 Srovnání Jitteru mezi standardy 50
Obr. 26 Srovnání MOS mezi standardy 50

SEZNAM TABULEK

Tab. 1 Priority v IEEE 802.11e 8
Tab. 2 Srovnání kodeků pro VoIP 15
Tab. 3 Doporučené hodnoty pro kvalitu VoIP 16
Tab. 4 Hodnoty MOS na lince bez konfiguračních změn 20
Tab. 5 Parametry MOS v závislosti na šířce pásma 21
Tab. 6 Parametry MOS v závislosti na zpoždění 22
Tab. 7 Parametry MOS v závislosti na jitteru 23
Tab. 8 Parametry MOS v závislosti na ztrátovosti 24

SEZNAM GRAFŮ

Graf č.1 Závislost MOS na Šířce pásma 21
Graf č.2 Závislost MOS na Zpoždění 22
Graf č.3 Závislost MOS na Jitteru 23
Graf č.4 Závislost MOS na Ztrátovosti 25

ÚVOD

Tato práce se zabývá kvalitou služeb v bezdrátových sítích pro standardy IEEE 802.11. V dnešní době se velmi často setkáváme se službami přenosu hlasu a videa v reálném čase a lidé využívají tyto služby jak pro zábavu, tak i pro práci. Mladí lidé využívají zejména hlasových služeb pro bezplatnou komunikaci se svými přáteli i na velké vzdálenosti nebo při hraní počítačových her. Stejně tak jsou v současné době populární přenosy videa společně s hlasem, aby účastníci na obou koncích měli možnost vidět, s kým komunikují. Tohoto se využívá např. i ve firmách či velkých společnostech pro různé konferenční hovory. V poslední době je také velmi populární streamovaný přenos videa v jakékoliv formě, zejména proto, že si účastníci nemusí pořizovat televizi a vše tak mohou sledovat přímo na počítači.

Bezdrátové sítě jsou v současné době velmi rozšířené, zejména pro hojné používání notebooků, netbooků a tabletů. Jednotliví uživatelé tak nejsou omezováni kabely a mohou se volně pohybovat se svými mobilními stanicemi. Takový komfort má i své nevýhody a to zejména reálnou možností rušení elektromagnetických vln. Uživatelé jsou také omezeni dosahem bezdrátových síti a kvalitou signálu dále od přístupového bodu. Nově se můžeme od roku 2009 setkávat se zatím ne moc rozšířenými, ale stále populárnějšími sítěmi na standartu IEEE 802.11n, který nabízí oproti starším standardům větší stabilitu.

První část práce se zabývá teoretickými poznatky o modelu sítě využívající bezdrátové přístupové body s podporou kvality služeb QoS. Důležitý z tohoto hlediska je zejména standart IEEE 802.11e. Další kapitoly se zabývají řešením přenosu multimediálních služeb na transportní a aplikační vrstvě. Dále se práce zabývá měřením objektivních parametrů kvality služeb při přenosu hlasu po laboratorní síti. Poslední část je věnovaná vytvoření modelu bezdrátové sítě v prostředí OPNET Modeler za účelem proměření a simulace parametrů této simulované sítě.

1 TEORETICKÝ ÚVOD

V následující kapitole jsou představeny základní teoretické poznatky, o které se tato práce opírá, a z kterých při analýze provozu na síti vychází.

1.1 Modely sítě

V dnešní době jsou známy dva teoretické modely sítě, které se v praxi využívají. Jako první je znám standardizovaný model ISO OSI, který zavedl mezinárodní standardizační úřad – ISO a dále model TCP/IP, který využívá protokoly sady TCP/IP a je zjednodušený oproti prvnímu uvedenému modelu. Ačkoliv jsou se tyto modely na první pohled odlišné, jsou ve své podstatě velmi podobné a musí být kompatibilní, jinak by většina sítí nemohla správně fungovat. Na obr. 1 je vidět srovnání obou modelů sítě.

Model	**OSI ISO**	**TCP/IP**
Vrstva		
7	aplikační	aplikační
6	relační	
5	prezentační	
4	transportní	TCP/UDP
3	síťová	internet (IP)
2	linková	linková a fyzická
1	fyzická	

Obr. 1 Modely sítě

1.2 Využívané technologie

V praxi existuje nepřeberné množství koncových zařízení a způsobů jak je připojit do sítě, avšak tato práce se zabývá především bezdrátovými sítěmi a tedy zařízeními, která umožňují provoz a přenos dat vzduchem. Z hlediska přenosu dat je dále nutné se zabývat protokoly na čtvrté vrstvě, tomto případě transportními protokoly TCP a UDP. V neposlední řadě je pro tuto práci také důležitý protokol RTP, který na aplikační vrstvě modelu TCP/IP zajišťuje přenos hlasu a videa v reálném čase, stejně tak jsou klíčové

protokoly pro řízení spojení v reálném čase, jako jsou např. protokoly SIP s RTSP. Nakonec je také důležité znát, jaké kodeky jsou využívány pro přenos hlasu a videa po internetu.

1.3 Bezdrátové sítě

Bezdrátovými sítěmi jsou myšleny sítě, kde je možné se volně pohybovat v okolí vysílače a jako přenosové médium je bráno rádiové prostředí. Zřejmou výhodou oproti drátovým sítím je schopnost mobility účastníků. Hlavní nevýhodou je fakt, že je signál šířen ve vzduchu a může tak být ovlivněn řadou nežádoucích faktorů jako jsou útlum, rušení apod. Dalším problémem zejména v dnešní době je nutnost zajištění bezpečnosti, jelikož zachytit rádiové vlny je mnohem snadnější než se nabourat do nainstalované kabeláže.

Bezdrátové sítě se dělí podle šířky pásma na sítě širokopásmové a úzkopásmové. Hranice mezi těmito sítěmi není pevně stanovena, avšak sítě s propustností nad 2 Mb/s se považují již za širokopásmové.

1.3.1 Standard 802.11

IEEE 802.11 je soubor standardů pro implementaci bezdrátové lokální sítě (tzv. WLAN – z anglického Wireless Local Area Network) v pásmech 2,4 a 5 GHz. Byly vytvořeny standardizační komisí IEEE. V současné době se standardy bezdrátové sítě označují názvem WiFi (Wireless Fidelity).

Rodina standardů 802.11 obsahuje několik řad modulačních technik pro přenos dat vzduchem za použití stejného základního protokolu. V současnosti jsou nejpoužívanější ty s označením 802.11b a 802.11g a nově od roku 2009 i standard 802.11n, který se postupně začíná hojně využívat jak pro komerční tak i osobní účely.

1.3.2 Standard 802.11b

802.11b pracuje v bezlicenčním bezdrátovém pásmu 2,4 GHz a proto mohou být stanice v reálném prostředí rušeny mikrovlnnými troubami, zařízeními Bluetooth nebo např. bezdrátovými telefony. Standard 802.11b má maximální propustnost o velikosti

11Mb/s. V praxi je ale z přenosového pásma použito asi 30 – 40% pásma na režii provozu, a proto v reálném prostředí sítě dosahují sítě tohoto standardu rychlostí menších než výše uvedených teoretických. Z důvodů nízkých rychlostí se také bezdrátové sítě začali rozšiřovat masivně až od uvedení standardu 802.11b, který využívá techniku DSSS (Direct Sequence Spread Spectrum).

1.3.3 Standard 802.11g

Jedná se o nejrozšířenější standard, který je ale postupně vytlačován novým a modernějším 802.11n. 802.11g dovoluje využít rychlostí až 54 Mb/s, což je daleko více než původní verze, která v době uvedení na trh v roce 1997 umožňovala pouze rychlosti od 1 do 2 Mb/s a asi pětkrát více než 802.11b, na rozdíl o které využívá přenosovou techniku OFDM (Orthogonal Frequency Division Multiplexing). Tento standard byl ale uveden na trh mnohem později a byla nutnost, aby umožňoval zpětnou kompatibilitu s jeho starším protějškem, proto byla zavedena techniku DSSS pro standard 802.11g, pouze ale pro modulace nižších rychlostí. Vyšší rychlosti pak pracují s modulacemi 16-QAM, QPSK a BPSK.

1.3.4 Standard 802.11a

Tento standard využívá pásmo o šířce 5 GHz a nabízí tak 23 kanálů, které se vzájemně nepřekrývají na rozdíl od 2,4 GHz pásma, kde máme k dispozici pouze 13 kanálů, které se ke všemu výrazně překrývají. Pokud bychom ve verzi 802.11b/g chtěli vybrat kanály bez překryvu, abychom tak eliminovali většinu rušení, máme k dispozici pouze 3, maximálně 4 kanály. Standard 802.11a využívá také techniku přenosu OFDM a umožňuje také špičkové propustnosti o rychlostech až 54 Mb/s, s ohledem na režii spíše kolem 36 Mb/s. Nevýhodou vyšší frekvence, na které této standard operuje je zejména nižší dosah bezdrátové sítě, kdy zdi a další pevné objekty v cestě snadněji pohlcují signál s menší vlnovou délkou.

1.3.5 Standard 802.11n

802.11n je nejnovější standard představený na trh v roce 2009. Jedná se spíše o dodatek k předchozím standardům, kdy je přidána tzv. MIMO (multiple input multiple output)

technologie. Tato technologie využívá vícero antén pro příjem i pro vysílání, aby se zajistil lepší chod bezdrátové sítě. 802.11n se používá jak pro sítě s pásmem 2,4 GHz tak i pro méně využívané s pásmem 5 GHz. Maximální teoretická rychlost na fyzické vrstvě je udávána jako 600 Mb/s avšak v praxi dosahuje rychlostí kolem 200 Mb/s. Této rychlosti dosahuje především sdružováním kanálů na velikosti až 40 MHz a spojováním rámců. Technologie MIMO pracuje tak, že umožňuje zároveň vysílat a přijímat vícero nezávislých signálů různými kanály a anténami v jednom frekvenčním kanále, kdy dochází k výraznému poklesu chybovosti a zvýší se tak i kapacita spoje. Využívá se také odrazů signálů od překážek. U starších standardů byl tento jev považován za nežádoucí, kdy se jednalo o rušení z důvodu příchodu signálu s rozdílným zpožděním. Zde však přijímač dokáže různými algoritmy signál poskládat ve správném pořadí. Frame aggregation neboli spojování rámců je dalším z užitečných rozšíření v tomto standardu. Rámce se spojují na podvrstvě MAC a dochází tak ke snížení času mezi vysílanými rámci a dojde tak i k snížení celkové režie přenosu.

1.3.6 Rozdělení kanálů

Kanály ve 2,4 GHz standardech jsou rozděleny od 2,4000 GHz do 2,4835 GHz na 13 kanálů rozložených od sebe v 5 MHz intervalech. První kanál má střed na frekvenci 2,412 GHz a poslední 13. kanál, má střed na frekvenci 2,472 GHz. V Japonsku se pak využívá ještě 14. kanál, který je dostupný pouze pro standard 802.11g a jeho střed je 12 MHz nad kanálem č. 13. Ve standartu 802.11b, který využívá modulaci DSSS jsou vlny o šířce 22 MHz a umožňují tak efektivní využité pouze tří nepřekrývajících se kanálu a to kanálů 1, 6 a 11. Ve standardu 802.11g, kde je použita OFDM modulace, je tvar vlny široký pouze 20 MHz a tak umožňuje využití čtyř nepřekrývajících se kanálu a to: 1, 5, 9 a 13. Standardy 802.11 definují kromě středního kmitočtu také spektrální masku pro každý kanál, která určuje jeho výkonové rozdělení. Je definováno, že každá kanál má signál zesílený o 30 dB na kmitočtech +/-11 MHz od středního kmitočtu.

1.3.7 Definice rámce

Současný standard 802.11 také definuje, jak vypadají rámce v bezdrátových sítích a také management a řízení bezdrátových spojů. Rámce jsou rozděleny do velmi specifických sekcí. Každý rámec má MAC hlavičku, datovou část (označovanou jako

payload) a kontrolní součet. První dva byty hlavičky definují tzv. kontrolní pole, které určuje formu a funkci daného rámce. První dva bity určují verzi protokolu, kdy se v současné době používá pouze protokol s verzí 0, další hodnoty jsou rezervovány pro budoucí použití. Další dva bity určují typ rámce, nejčastěji jestli se jedná o rámec kontrolní, datový nebo řídící. Společně s dalšími 4 bity, které určují podtyp, definují celkovou identitu daného rámce. Následují ToDS a FromDS bity, které určují, jestli se jedná o hlavičky distribučních systémů. Následuje bit, který určuje, zda-li jsou přicházející pakety fragmentovány na více rámců. Následují další bity jako Retry, Power Management, More Data a WEP, který určuje, zda byl daná rámec již dešifrován. Následuje poslední bit Order.

Rámec ve standardu 802.11 může nést informaci až o 4 adresách. V praxi se využívají nejčastěji tři z nich a to na první pozici MAC adresa příjemce, na druhé pozici MAC adresa odesílatele a třetí pozice se používá k možnosti filtrování na straně příjemce.

Před datovou částí jsou ještě dvě sekce a to sekce, která sleduje pořadí jednotlivých rámců a eliminuje duplicity. Další sekce o velikosti 2 byty obsahuje pole Quality of Service (QoS) definované ve standardu 802.11e.

Následuje datová část o velikosti 0 až 2304 bytů s možností nástavby, která obsahuje informace o zapouzdření popř. informace z protokolů vyšších vrstev.

Po datové části následuje poslední sekce o velikosti 4 bytů, tzv. kontrolní součet, který si příjemce kontroluje sám a porovnává ho s údaji v daném rámci. Pokud se čísla shodují, tak předpokládá, že rámec dorazil v pořádku a nebyl po cestě znehodnocen.

1.3.8 Standard 802.11e – Kvalita služeb

802.11e je oficiální dodatek pro IEEE 802.11 standardy vydaný v roce 2005. Tento dodatek definuje kvalitu služeb pro bezdrátové sítě pomocí modifikace MAC (Media Access Control) vrstvy. Tento standard má velkou důležitost zejména pro aplikace, které jsou citlivé na vysoké zpoždění, jako jsou například přenos hlasu a videa, a proto je také pro tuto práci důležité se jím zabývat.

Základní MAC vrstva ve standardech 802.11 využívá distribuční koordinační funkci (DFC) k zajišťování spojení mezi více stanicemi. V praxi to vypadá tak, že pokud více stanic bude chtít komunikovat ve stejnou dobu, tak dojde k mnoha kolizím, které

výrazně omezí dostupnost služby. Pokud se pak zásobníky na přístupových bodech zaplní, tak dojde k zahazování jednotlivých rámců, což je velmi nežádoucí zejména pro služby přenosu v reálném čase. V základní standardu tedy nejsou žádné prostředky, jak odlišit prioritní provoz od toho méně důležitého a např. pokud se stanice připojí k nějakému médiu, může využívat prostředků sítě neomezeně dlouhou dobu bez ohledu na ostatní stanice.

V základu standardu 802.11 je pro řízení spojení využívána ještě funkce PCF (Point Coordination Function). Tato se využívá pouze v infrastruktuře, kde jsou stanice připojeny přes Access Point a není tak hojně využívaná jako funkce DFC.

Standard 802.11e vylepšuje algoritmy funkcí DCF a PFC pomocí nové funkce HCF (Hybrid Coordination Function). V HFC jsou dvě metody přístupu k bezdrátovému kanálu podobné jako v základní verzi standardu 802.11 a to HCF Controlled Channel Access (HCCA) and Enhanced Distributed Channel Access (EDCA). Obě metody definují přenosové kategorie, do kterých přiřazují jednotlivé služby. Např. protokolům zajišťujícím přístup na e-mailové servery tak může být přiřazena nejnižší třída a naopak službám využívajícím přenos dat v reálním čase jako VoIP může být přiřazena nejvyšší priorita.

Pomocí EDCA má provoz s vyšší prioritou větší šanci na to být odeslán, než provoz ze stanice s nižší prioritou. V praxi tak důležitější provoz čeká kratší intervaly než ostatní pakety. Tohoto je docíleno zejména zmenšením hodnoty Arbitration Inter Frame Spacing (AIFS), která určuje interval odesílání mezi jednotlivými rámci. Dále tato metoda umožňuje vysílat v tzv. Transmit Opportunity oknech, během kterých mohou vysílat všechny stanice neomezené množství rámců, pokud nepřesáhnou dobu daného okna. Tímto algoritmem se eliminuje problém z původní verze, kdy stanice mohla získat přístup k určitým systémovým zdrojům na neomezeně dlouhou dobu, i když je téměř vůbec nevyužívala a blokovala tak tyto zdroje pro ostatní stanice či aplikace.

Tabulka č. 1 uvádí nastavení priorit ve standardu 802.11e. Celkově existuje osm priorit, kdy priorita 0 je nejnižší a je používána zejména pro aplikace běžící na pozadí až po prioritu 7, kterou mají přiřazeny procesy zajišťující řízení sítě. Jednotlivé priority mají přiděleny na jednotlivých kanálech rozdílné šířky pásem, které jsou posílány v beacon rámcích a tak je možné, aby správce sítě ověřil, zda je v dané kategorii ještě dostatek

systémových zdrojů před přidáním dalších služeb. Dříve se používala ještě metoda WME (Wireless Media Extension). Jednalo se o jakého si předchůdce standartu 802.11e z důvodu potřeby rychlého zajištění QoS pro služby náchylné na zpoždění. WME dělila data do 4 tříd: hlas (nyní 6,7 viz tabulka níže), video (4,5), Best Effort (0,3) a Background (1,2). Současná zařízení jsou s metodou WME kompatibilní a pokud nemají třídu nastavenu tak jsou automaticky zařazeny do třídy Best Effort.

Tab. 1 Priority v IEEE 802.11e

Priorita	Charakteristika
0	Aplikace na pozadí
1	Best Effort
2	Excellent Effort
3	Kritické aplikace
4	Video
5	Hlasové služby
6	Řízení práce se sítí
7	Řízení sítě

HCCA je obecně považována za nejpokročilejší a nejkomplexnější koordinační funkci díky které může být QoS nastavena velmi dobře. HCCA se využívá obdobně jako PCF jen na sítích, kde jsou stanice připojeny přes Access Pointy. Není tedy tak hojně využívána, zejména proto, že velmi málo přístupových bodů má tuto funkci implementovánu. Přístupové body posílají Beacon rámce v pevně stanovených intervalech a HCCA je obdobně jako PCF dělí na dva úseky. V prvním úseku se používá standartní metody EDCA. V druhém pak umožňuje všem stanicím vysílat. Tento interval se nazývá Controlled Access Phase (CAP).

Ve standardu 802.11e jsou ještě dále definovány některé dodatečné funkce jako např. možnost nastavení hodnoty QoSNoAck v dané třídě, které zablokuje znovu odesílání rámců. Tohoto jevu se využívá zejména v situacích, kdy je kriticky důležitá časová náročnost.

1.3.9 Zabezpečení Wi-Fi

Problém bezpečnosti bezdrátových sítí se odráží především v jejich způsobu šíření a to tak, že nelze efektivně omezit prostor dosahu nehledě na stěny budov. Je tedy možné se připojit na nezabezpečené sítě, kdekoliv je signál dostupný.

Základním zabezpečením Wi-Fi je používání tzv. SSID (Service Set ID), tedy identifikátoru dané sítě. SSID se standardně přenáší v tzv. Beacon rámci. Kdokoliv v dosahu dané sítě může tento rámec zachytit a zjistit tak, že je v dosahu daného přístupového bodu. Vysílání SSID jde zakázat, čím se síť stane na oko neviditelná a pouze uživatele co znají přesný název se na ni mohou připojit. Avšak i skryté sítě se dají objevit pomocí tzv. Probe Request rámce, na ten totiž odpoví i neviditelný přístupový bod pomocí tzv. Probe Response rámce.

Základním šifrováním pro Wi-Fi je WEP. Ten používá symetrickou šifru RC4. Klíč tak musí být znám jak vysílači, tak přijímači. Základní WEP poskytuje formu pouze 64 bitového šifrování. WEP2 umožňuje zabezpečení ve formě 128 bitového šifrování, kdy klíč má délku 104b a inicializační vektor, používaný k expandování klíče na velikost zprávy, s délkou 24b. Nevýhoda WEP je, že používá statické klíče a krátké inicializační vektory. Je tedy lehce prolomitelný.

WPA je šifrování pomocí protokolu TKIP - Temporal Key Integrity Protocol. Je využíván podobný šifrovací algoritmus jako u WEP s délkou klíče 128b, ale na rozdíl od WEP používá dynamické klíče. Klíč je měněn každých 10000 paketů. Další výhodou je použití MIC - Message Integrity Check, tedy kontrola integrity zprávy. MIC je podstatně lepší než obyčejný kontrolní součet CRC.

1.4 Transportní vrstva

Protokoly TCP a UDP jsou dva protokoly zajišťující přenos dat na úrovni transportní vrstvě v modelu ISO OSI. Protokoly TCP a UDP se zcela spoléhají na správnou funkčnost protokolů na nižších vrstvách. Předpokládá se tedy, že spojení již mezi stanicí a směrovači bylo vytvořeno a že bezdrátová síť funguje zcela v pořádku. Stanice mezi sebou mohou využívat velké množství různých služeb. V protokolu TCP se data přenášejí pomocí TCP segmentů a jsou směrovány vždy přímo jednotlivým aplikacím.

Po protokolu UPD jsou pak data přenášena pomocí UDP datagramů. Nejdůležitějším rozdílem mezi těmito dvěma protokoly je, zda se jedná o spojovanou službu či nikoliv. TCP je spojovanou službou a příjemce tak vždy odesílateli potvrzuje přijatá data. V případě ztráty dat nebo jejich poškození si pak příjemce vyžádá jejich opětovné zaslání od odesílatele. V UDP protokolu nejsou data vůbec potvrzována a tak odesílatele nezajímá, zda odeslaná data dorazili do cíle v pořádku či nikoliv. Z výše uvedeného je tedy vidět, že z hlediska využití protokolů vyšších vrstev je volba transportního protokolu celkem zásadní. Při použití protokolu TCP, se žádá vždy o potvrzení doručení segmentu. Tento jev sice prudce omezuje ztrátovost na lince, ale také může zapříčinit vyšší zpoždění v případech častého opakovaného zaslání segmentů z důvodů poškození dat na trase. V případě použití protokolu UDP aplikace vyšších vrstev nezajímá, jestli byl datagram doručen a tak se na spoji nevytváří dodatečné zpoždění, kvůli opětovnému zasílání poškozených dat, avšak při vysokém počtu znehodnocených dat a nemožnosti opravy z podstaty protokolu, může tento jev vést k znehodnocení celkové komunikace do takové míry, že to způsobí výpadky zvuku nebo obrazu.

1.4.1 Protokol TCP

Protokol TCP (Transmission Control Protocol) pracující na čtvrté vrstvě předpokládá, že spojení mezi jednotlivými stanicemi je již zajištěno pomocí IP protokolu na třetí vrstvě. Protokol TCP pak zajišťuje přímé spojení mezi dvěma běžícími aplikacemi na takto propojených počítačích v síti. Protokol TCP využívá k adresaci tzv. port. Port je dvoubajtové číslo, které může nabývat hodnot od 0 do 65535. Po navázání spojení se mezi dvěma aplikacemi vytvoří tzv. relační okruh a je tak umožněna oboustranná komunikace mezi stanicemi nezávisle jedna na druhé. Je tak docíleno toho, že např. během hlasové komunikace mohou oba zainteresovaní hovořit zároveň.

Z výše uvedeného vyplývá, že komunikace po TCP zajišťuje potvrzování přijatých dat. Toho jevu je docíleno tím, že všechny odeslané segmenty jsou očíslované. Při přenosu dat tak může nastat situace, kdy příjemci nějaký segment nedorazí v pořádku, popřípadě nedorazí vůbec. V takovém případě si příjemce vyžádá znovu zaslání segmentu

s chybějícím číslem nebo s číslem segmentu s poškozenými daty. Současně s číslováním je přenos dat zabezpečen kontrolním součtem. Kontrolní součet je odeslán odesílatelem společně s daty. Pokud příjemce obdrží segment s jiným součtem, snaží se problém následně vyřešit opětovným zasláním daných dat.

Velikost segmentu se může lišit pro každou síť a každé spojení. TCP segment totiž nemá pevně danou velikost, ale jeho velikost tzv. maximum segment size (MSS) je odvozena od maximum transmission unit (MTU), tedy maximální velikosti dat na nižší vrstvě. Při sestavování spojení je tak zjištěno jaké je na lince povolena MTU – většinou 1500 B – a stanice i pak vyjednají, jaká bude velikost segmentů včetně hlavičky tak, aby nedocházelo k IP fragmentaci. Při přenosu větších souborů je ale stejně nutné rozdělit soubor do několika segmentů. Příklad segmentu je uveden v obrázku č. 2 inspirovaném podle [5].

IP záhlaví (zpravidla 20 B)	TCP záhlaví (zpravidla 20 B)	Data (rozdílná velikost)

Obr. 2 TCP segment

1.4.2 Protokol UDP

Protokol UDP (User Datagram Protokol) je v podstatě jednodušší formou protokolu TCP. Jedná se o nespojovanou službu, což znamená, že jakmile odesílatel odešle datagram, už se nezajímá o to, jestli byl doručen, jako je tomu v případě protokolu TCP. Příklad UDP datagramu je znázorněn na obrázku č. 3 inspirovaném podle [5].

IP záhlaví (zpravidla 20 B)	UDP záhlaví (zpravidla 8 B)	Data (rozdílná velikost)

Obr. 3 UDP Datagram

Hlavička UDP protokolu obsahuje obdobně jako protokol TCP mimo jiné také číslo portu odesílatele a příjemce. Čísla portů v protokolu UDP jsou stejná jako čísla portů v protokolu TCP a tedy od 0 do 65535, ale nijak nesouvisí s čísly portů TCP. Protokol UDP totiž využívá svoji vlastní řadu portů. U protokolu UDP je také nepovinná položka

kontrolního součtu, protože se data nemohou znovu odeslat při jejich nedoručení nebo znehodnocení, a tak se velmi často bity zajišťující funkci kontrolní součet vypínají, aby se přenos dat po síti urychlil a neposílali se tak nadbytečné informace.

Velkou předností protokolu UDP na rozdíl od jeho protějšku je jedna z jeho důležitých vlastností. Protokol UDP není omezen na adresování přímo jedné stanice a může tak adresovat více příjemců. V praxi tak každá účastnická stanice není povinna navazovat spojení přímo se serverem, ale díky UDP protokolu dokáže využít nižších vrstev a může rozesílat pakety systémem broadcastů a multicastů. Při poslání datagramů s využitím broadcastu se tak datagramy rozesílají na všechny účastníky v dané podsíti, kdežto při posílání datagramů s využitím multicastu se datagramy pošlou na vybranou skupinu stanic.

1.5 Aplikační vrstva

Tato práce se zaobírá na aplikační vrstvě zejména protokolem RTP, který zajišťuje přenos dat v reálném čase a dále sekundárními protokoly, které zajišťují řízení datových a streamovaných přenosů. Důležité jsou taký z hlediska přenosu hlasu a videa použité kodeky jednotlivých aplikací.

1.5.1 Protokol RTP

Real-time Transport Protocol (RTP) definuje standardizovaný paketový formát pro doručování audio a video paketů po internetu. RTP protokol je masově využívám právě v systémech, které se zabývají internetovou telefonii a streamováním videa. RTP protokol se používá v souběhu s protokolem RTPC (RTP Control Protocol). RTP se totiž stará o přenos jednotlivých multimediálních dat zatímco RTPC monitoruje přenosové statistiky a QoS a také pomáhá při synchronizaci u vysílání více proudů. Provoz RTP je uskutečňován na sudých portech a řízení protokolem RTPC je vždy na nejbližším vyšším lichém portu. RTP protokol pro data v reálném čase obstarává časové známky a sekvenční čísla pro správnou synchronizaci. V porovnání s RTP využívá RTPC pouze 5% šířky pásma pro daný multimediální přenos.

Hlavními přednostmi protokolu RTP jsou možnosti kompenzace jitteru a detekce příchodu sekvence dat. V případě špatného pořadí pak tuto sekvenci jednoduše napravuje. RTP dále podporuje přenos dat na více koncových stanic pomocí multicastů.

Většina aplikací využívající RTP protokol pro přenos multimediálních dat upřednostňuje používání protokolu UDP na nižších vrstvách díky jeho vlastnostem popsaných v kapitole 1.4. Zejména proto, že preferuje rychlost před spolehlivostí. Jeden nebo pár ztracených dat při hlasovém přenosu totiž může mít za následek ztrátu pouze zlomku sekundy a účastníci si této ztráty nemusí vůbec povšimnout.

Pro každý multimediální proud dat je sestavena samostatná relace. Relace se skládá z IP adresy a portů RTP a RTPC. Např. při vysílání audia a videa bude mít každý proud svoji vlastní relaci tak, aby si mohl příjemce vybrat jen to, co potřebuje. Porty jsou vyjednány především pomocí protokolu Real Time Streaming Protocol (RTSP) a Session Initiation Protocol (SIP). Většinou se využívá neprivilegovaných portů tedy portů vyšších než 1024.

Designéři protokolu RTP si stanovili za cíl podporu všech možných multimediálních formátů a tak informace, které aplikace potřebují k dekódování jednotlivých proudů, nejsou obsaženy v hlavičce RTP nýbrž jsou definovány přímo v RTP pomocí profilů a datových formátů. Pro každou třídu je tak definován vlastní profil a datový formát. Profily definují jednotlivé kodeky použité ke kódování dat a jsou dále mapovány na příslušné datové formáty.

Protokol RTPC má za úkol tři základní funkce. Primární funkcí je sběr statistik ohledně kvality přenosu pro každou relaci. Tyto data poté zasílá zdrojovému médiu a následně všem účastníkům. Tyto informace mohou být použit např. k změně kodeku při vysokém zpoždění linky, pokud tyto funkce daná aplikace podporuje. Dále RTPC přiřazuje každému účastníkovi relace jedinečný identifikátor. Posledním funkcí RTPC je to, že si sám hlídá použitou šířku pásma, která by neměla překročit 5% celkového multimediálního provozu tak, aby příliš nezahlcoval síť. Pokud je tato hodnota překročena tak zvýší interval zasílání informačních zpráv na koncové stanice.

1.5.2 Protokol SIP

Session Initiation Protocol (SIP) je signalizační protokol pro řízení a kontrolu relací v multimediálních přenosech. Protokol SIP standardně využívá porty 5060 a 5061 pro TCP i UDP protokol. Protokol SIP v současnosti nahradil starší verzi použitou pro signalizaci v internetové telefonii a to standart H.323. Protokol SIP je mnohem jednodušší a těží z již prověřených principů. SIP protokol je textově orientovaný a byl designován na podobném principu jako model HTTP – tedy na systému dotaz-odpověď. Aplikacím využívající protokol SIP je umožněno navazovat relaci přímo mezi sebou, ale v praxi častěji dochází k tomu, že k tomu účelu používají jeden nebo více SIP proxy serverů.

1.5.3 Protokol RTSP

Real Time Streaming Protocol (RTSP) je protokol vytvořený pro kontrolu stramovaných přenosů zejména na media serverech. Používá se k vytvoření a kontrole relace mezi koncovými účastníky obdobně jako protokol SIP. Klienti pak mají možnost ovládat datové přenosy příkazy jako „play“ či „stop“. RTSP je opět přirovnáván k protokolu HTTP avšak na rozdíl od bezstavového protokolu HTTP je RSTP stavový. Využívá identifikátor, který dokáže sledovat aktuální relaci. Pro komunikace mezi klientem a serverem využívá RSTP především protokol TCP na portu číslo 554.

1.5.4 VoIP kodeky

Jendou z velmi důležitých vlastností při provozování IP telefonie je volba kodeku pro komunikaci mezi stanicemi. Kodeky se starají o konvertování analogového zvuku do digitální podoby. Jednotlivé kodeky se liší především v kvalitě přenášeného hlasu, potřebné šířce pásma a výpočetních náročnostech. Tabulka č. 2 udává porovnání často používaných kodeků v závislosti na šířce pásma.

V praxi se často využívá kodek G.711, který má kvalitu srovnatelnou s hovory v mobilní síti GSM. Často není ale kodek nastaven fixně, ale mění se v závislosti na dostupných prostředcích sítě, kdy si moderní SW aplikace pro VoIP samy dokáží zjistit,

jaký je nejlepší kodek pro aktuální spojení, při daných aktuálních provozních podmínkách na síti.

Tab. 2 Srovnání kodeků pro VoIP

Kodek	**Algoritmus**	**Šířka pásma (Kb/s)**
G.711	PCM	64
G.726	ADPCM	32
G.728	LD-CELP	16
G.729	CS-ACELP	8
Speex	CELP	8
G.723.1	MP-MLQ	6,3
G.723.1	ACELP	5,3

Co se týká kodeků pro videa tak i zde má uživatel na výběr z více možností. V praxi se ale v současné době hojně využívá kodeku H.264, který poskytuje zatím nejlepší poměr komprese ku přenosové rychlosti a je i jednoduchý na implementaci. Další možnostmi jsou kodeky H.261, H263 či MPEG4.

2 MĚŘENÍ NA SÍTI

Tato kapitola se zabývá vytvořením jednoduché bezdrátové sítě v laboratoři VUT za účelem proměření základních parametrů ovlivňujících přenos dat v reálném čase. Těmito parametry jsou především šířka pásma přenosového kanálu, ztrátovost, zpoždění a kolísání zpoždění neboli jitter. Aplikace využívající hlasových služeb jsou citlivé zejména na zpoždění, video aplikace pak na ztrátovost a jitter. Důležité je také zajištění dostatečné kapacity zdrojů na lince – šířky pásma. Tabulka č. 3 uvádí doporučené hodnoty uvedených parametrů na síti pro určení kvality VoIP hovorů [6]. Tyto parametry je objektivně možné měřit pomocí tzv. MOS faktoru (Mean Opinion Score).

Tab. 3 Doporučené hodnoty pro kvalitu VoIP

Kvalita sítě	Dobrá	Vyhovující	Nevyhovující
Zpoždění [ms]	0 – 150	150 – 300	nad 300
Jitter [ms]	0 – 20	20 – 50	nad 50
Ztrátovost [%]	0 – 0,5	0,5 – 1,5	nad 1,5

2.1 Parametry QoS

Kvalita služeb je složena z několika parametrů. Konkrétně se jedná především o následující:

- šířka pásma – bandwidth – určuje kapacitu linky
- zpoždění – souvisí se šířkou pásma a úzkými hrdly sítě
- jitter – kolísavé zpoždění – ovlivňuje pořadí doručených paketů
- ztrátovost – je ovlivněna od spolehlivosti přenosu

2.1.1 Šířka pásma

Udává šířku frekvenčního pásma nutného k přenosu dat požadovanou rychlostí a s požadovanou přesností. Analogová šířka pásma se měří v Hertzích (Hz), kdežto digitální šířka pásma se udává v bitech za sekundu. Důležité je rozpoznat rozdíl mezi šířkou pásma a pásmem v kterém stanice pracuje. Šířka pásma udává pouze prostor, který daná stanice zabírá v rámci vymezeného pásma.

2.1.2 Zpoždění

Zpoždění neboli latence udává dobu trvání přenosu paketu od vysílače k příjemci. Je tak ovlivněn fyzickou topologií sítě, jelikož odráží skutečnost průchodu dat jednotlivými prvky sítě. Celkové zpoždění je složeno z několika dílčích zpoždění: zpoždění kódováním, paketizací, přípravou na přenos, zpoždění při přenosu a v zásobnících aktivních prvků sítě a při přepínání paketů. Z hlediska interaktivních přenosů po síti je zpoždění jeden z parametrů co ovlivňuje výslednou kvalitu nejvíce.

2.1.3 Jitter

Jitter neboli kolísání zpoždění udává rozdíl v příchodu paketů od zdroje k cíli. V rámci jednoho vysílání totiž nemusí pakety přicházet k cílovému účastníkovi se stejným zpožděním a tím pádem dojdou pakety v rozdílném pořadí. Jitter je způsoben především zpožděním při paketizaci a při čekání v rozdílně velkých zásobnících na síťových prvcích.

2.1.4 Ztrátovost

Ztrátovost udává procentuální poměr ztracených paketů k všem přeneseným. Je způsobena mnoha faktory, ale často je to z důvodu přetížení či zahlcení prvků sítě, kdy dochází k tomu, že paměti front nestíhají odbavovat přicházející paket a dochází k jejich zahazování. Ztráta paketů pro časově nenáročné aplikace není nijak zásadní, oproti tomu v interaktivních komunikacích může i menší ztrátovost způsobit rozpad celé komunikace. Streamované video je vůči ztrátovosti o něco tolerantnější než hlasové aplikace, jelikož se část dat v paměti před přehráváním na koncové stanici.

2.2 MOS faktor

MOS faktor (Mean Opinion Score) je parametr, kterým se dají objektivně hodnotit kvality hovorů na síti. Může nabývat hodnot od 1 do 5. Většinou se uvádí pouze jako čísla s maximálně jedním desetinným místem. Hodnota 5 je nejlepším výsledkem a udává takovou kvalitu hovoru, jako by účastníci hovoru stáli vedle sebe a normálně spolu hovořili. U hodnot kolem 4 se již objevuje mírné rušení, většinou ale nepostřehnutelné pro velkou část populace. Takové hovory jsou stále velmi kvalitní a dají se přirovnat k hovorům v klasické analogové síti. U hodnoty 3 je již rušení účastníky vnímáno, jedná se o průměrnou kvalitu hovoru. Při ještě větším zarušení spoje se udává hodnota 2, kdy už si účastníci na protějších stranách spoje špatně rozumí a dochází k výpadkům v plynulosti hovoru. Nejhorším hodnocením je číslo 1. V takovém případě je již provoz tak znehodnocen, že není možné vést normální konverzaci. V praxi se ve VoIP technologiích dosahuje maximálních průměrných hodnot v rozsahu 3,5 – 4,5.

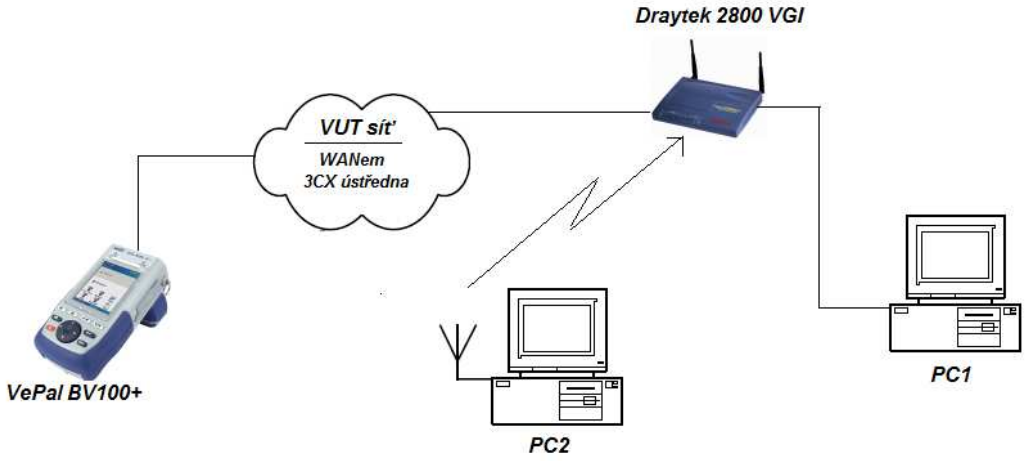
2.3 Zapojení měřené sítě

K měření MOS faktoru jako prostředku pro zjištění kvality sítě byla použita školní síť v laboratoř PA-339.

Použitý HW a SW:

- Konfigurační PC pro nastavení směrovače (PC1)
- PC s bezdrátovou kartou a VoIP klientem (PC2)
- Směrovač Draytek 2800VGI
- VePal BX100V+ tester
- Emulátor WANem
- Laboratorní síť s 3CX ústřednou pro VoIP

Zařízení jsme k síti připojili podle obrázku 4.



Obr. 4 Testovaná síť pro MOS faktor

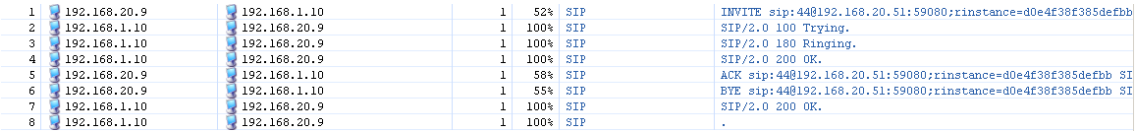
Pomocí PC 1 byl nakonfigurován směrovač Draytek nejprve pro připojení do WAN sítě – sítě VUT. Jelikož se jedná o ADSL2+ síť tak bylo nutné nastavit virtuální kanál VPI a virtuální cestu VCI dále typ služby, protokol a zapouzdření, viz obr. 5. Také bylo nastaveno automatické získávání IP adresy ze školního DHCP serveru.

Obr. 5 Nastavení WAN portu na směrovači Draytek

Dále byla nastavena lokální WiFi síť. Byl vybrán kanál 1 se středním kmitočtem 2412 MHz. Tento kanál byl zvolen proto, že v okolí už bylo několik sítí avšak všechny s kanály 6 a výše. Takto bylo eliminováno nežádoucí rušení mezi kanály. Na směrovači bylo ještě nutné nastavit konfiguraci VoIP brány pro připojení k ústředně na adrese 192.168.20.9. Následně bylo PC2 připojeno pomocí bezdrátového adaptéru k této nově vytvořené síti. Na PC2 byl nakonfigurován obdobný způsobem klient X-Lite pro připojení k virtuální ústředně 3CX. Pro přenos hlasu byl zvolen kodek G.711. V posledním kroku byl nakonfigurován tester VePal BV100+ tak, aby se choval jako VoIP telefon, který bude mít možnost měřit parametr MOS. Následně byla ověřena funkčnost provozu mezi stanicemi. Při vytočení klapky testeru se ozývaly předem namluvené hlasy, hovor tak byl spojen.

2.4 Analýza SIP provozu VoIP

Pro lepší přehled byl na PC2 spuštěn paketový analyzátor WildPacketsOmniPeek, který běžel na paralelním bezdrátovém adaptéru a umožňoval zaznamenávat všechny pakety přicházející na dané rozhraní. Z hlediska přehledu v množství zaznamenaných paketů byl navíc zvolen filtr na SIP protokol, který řídil daný VoIP přenos. Na obr. 6 je vidět podoba SIP protokolu, který řídil spojení mezi dvěma stanicemi a následně i jejich odpojení.



Obr. 6 Analýza SIP protokolu

2.5 Analýza MOS faktoru

Dále bylo využito funkcí testeru a změřeny parametry MOS na lince. Tester umožňoval zobrazení dvou hodnot parametrů MOS, a to MOS:LQ a MOS:CQ. Hodnota MOS:LQ

bere v potaz pouze jednosměrný provoz paketů na síti a neřeší tedy v potaz parametry jako zpoždění a ozvěny. Hodnota MOS:CQ tyto jevy obousměrné komunikace již bere v potaz, avšak jelikož na jedné straně je pouze tester, který vysílá a na druhé straně klient na PC2 pouze naslouchá, tak pro toto měření nemá daný parametr valný význam.

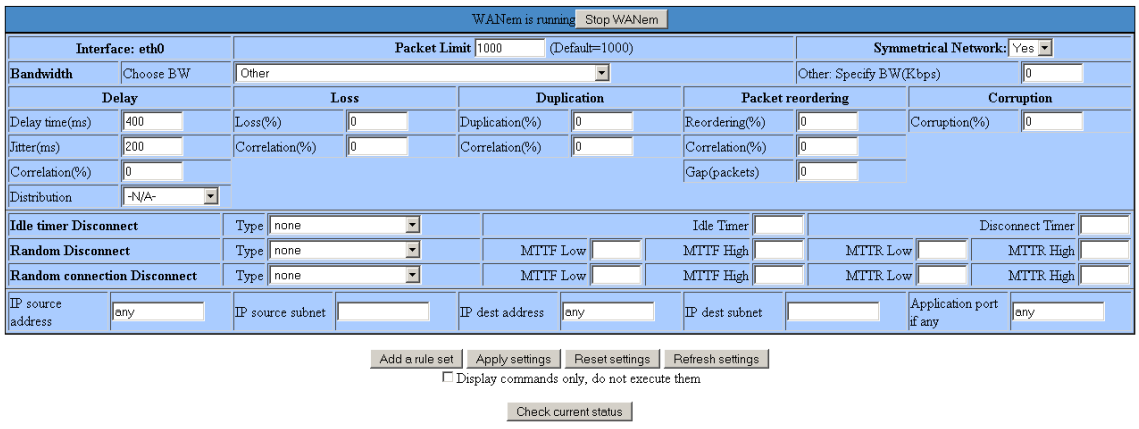
Následující tabulka uvádí naměřené hodnoty MOS bez zásahu do parametrů linky pomocí WANem emulátoru.

Tab. 4 Hodnoty MOS na lince bez konfiguračních změn

MOS:LQ	4,2
MOS:CQ	4,2

Hodnota 4,2 udává vynikající kvalitu spoje. Účastník by nezaznamenal žádné deformace hlasu či rozpady.

Dále jsme využili emulátoru WANem (Wide Area Network emulatoru), který umožňuje měnit parametry na spoji. WANem je volně šířený systém a operuje na linuxovém systému Knoppix. WANem lze lehce obsluhovat přes vzdálené webové rozhraní. Emulátor WANem je pak umístěn na síť mezi dva nebo více koncových uživatelů a veškerý provoz musí být směrován přes něj. V základním nastavení stačí pouze vybrat, z které IP adresy chceme přesměrovat provoz přes emulátor. Zde tedy z IP adresy ústředny – 192.168.20.9. V rozšířeném nastavení je poté umožněno měnit všemožné parametry. Zde však byli důležité zejména čtyři a to: šířka pásma, zpoždění, ztrátovost a jitter. Obr. 7 zobrazuje prostředí WANem emulátoru a možnosti nastavení jednotlivých parametrů.

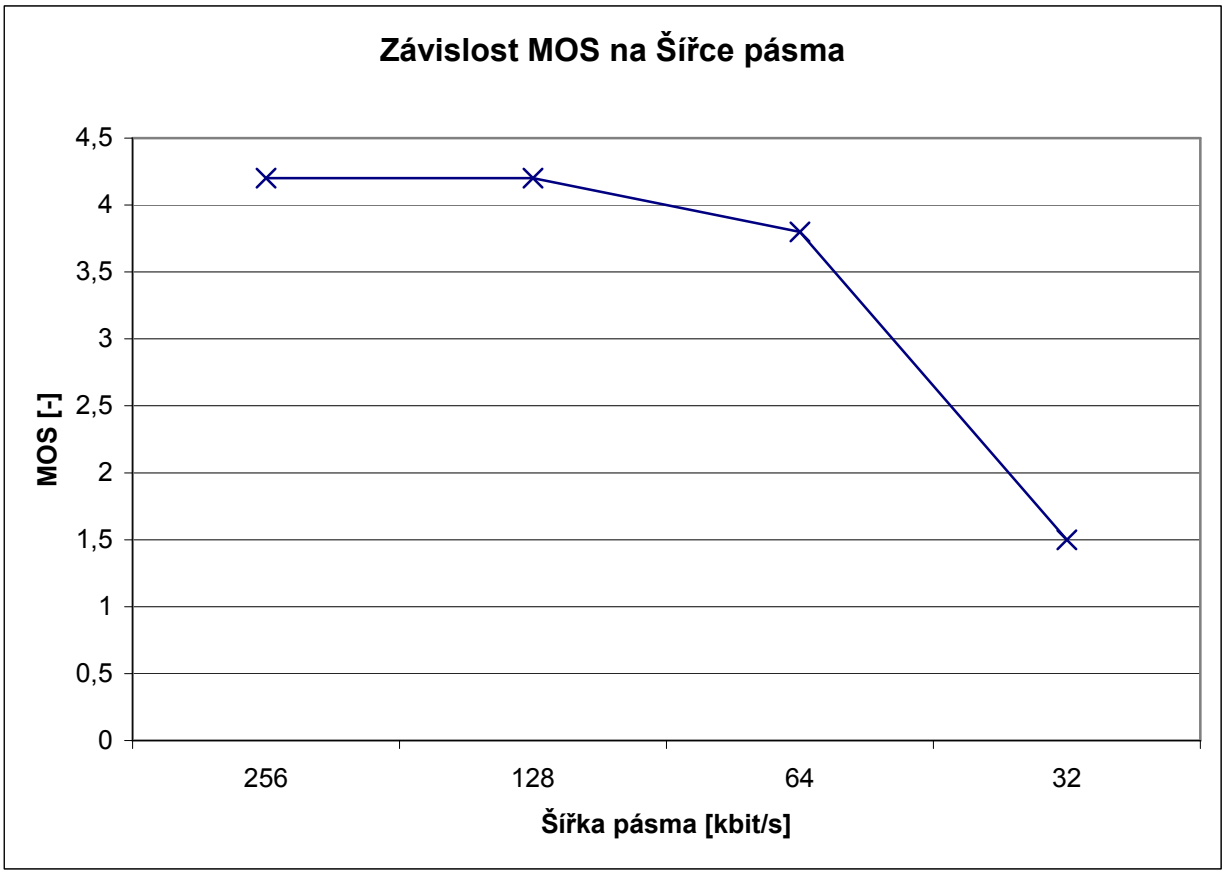


Obr. 7 Prostředí WANem

První měření bylo provedeno v závislosti na šířce pásma pro přenos hlasu po vytvořené síti při použití kodeku G.711. Výsledky jsou zaznamenány v tabulce č. 5.

Tab. 5 Parametry MOS v závislosti na šířce pásma

	Šířka pásma [kbit/s]			
	256	128	64	32
MOS:LQ	4,2	4,2	3,8	1,5
MOS:CQ	4,2	4,2	3,8	1,5



Graf č. 1 Závislost MOS na Šířce pásma

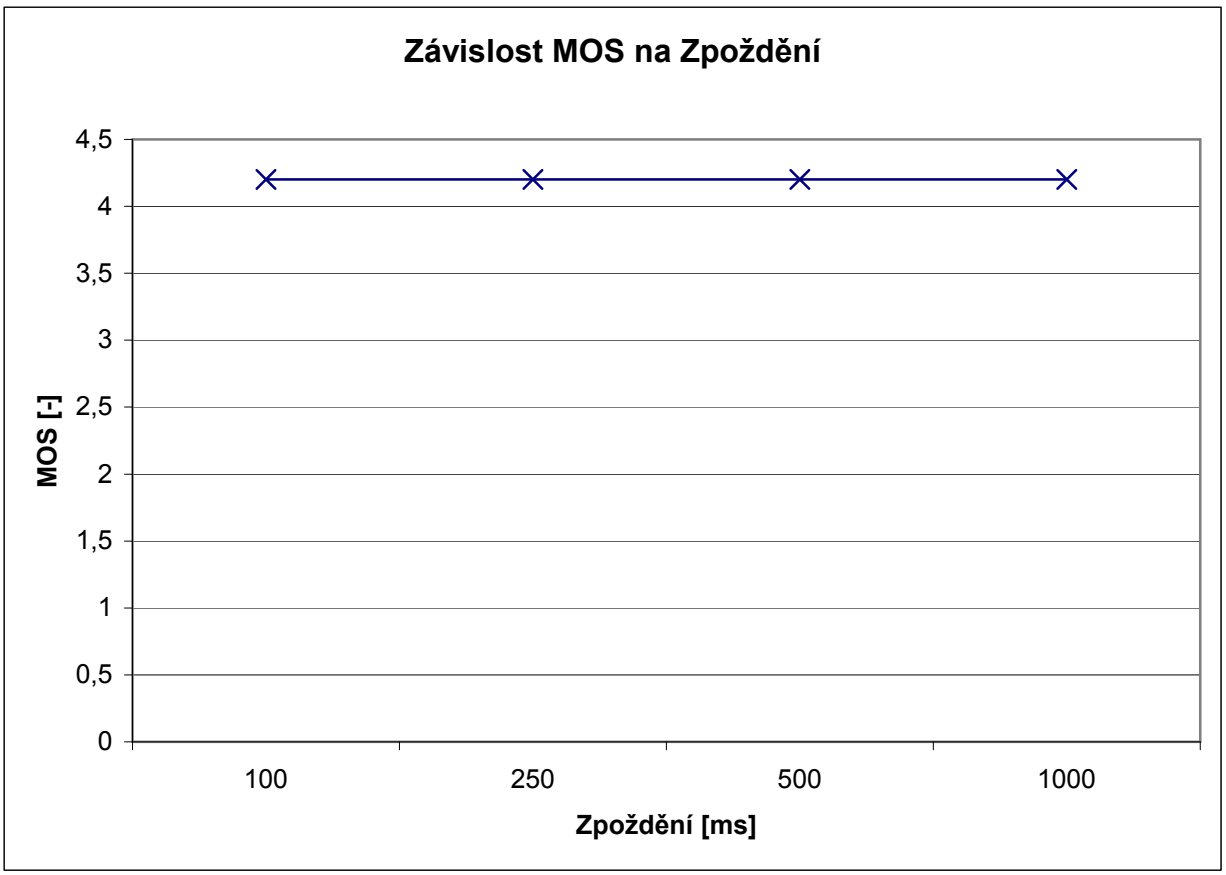
Z výsledků je patrné, že při použití kodeku G.711 pro kódování hlasu je potřebná šířka pásma alespoň 64 kbit/s. Při této hodnotě anebo vyšší byla kvalita hovoru výborná. Při nastavení šířky pásma 32 kbit/s byl změřený MOS faktor nízký a hovoru nešlo rozumět.

V dalším kroku byla proměřena linka v závislosti na zpoždění. Výsledky jsou zaznamenány do tabulky č. 6.

Tab. 6 Parametry MOS v závislosti na zpoždění

	Zpoždění [ms]			
	100	250	500	1000
MOS:LQ	4,2	4,2	4,2	4,2
MOS:CQ	4,2	4,2	4,2	4,2

Z výsledků je patrné tvrzení, které bylo již předesláno na začátku a tedy, že při jednosměrném provozu MOS parametry nejsou ovlivňovány zpožděním. Při využití takového systému totiž přijímači nevadí, pokud jsou data opožděna. V případě dvousměrné komunikace, která je naprosto normální v běžné praxi, by ale taková linka byla již nepoužitelná. Vysoké zpoždění by mělo za následky ozvěny v hovoru a



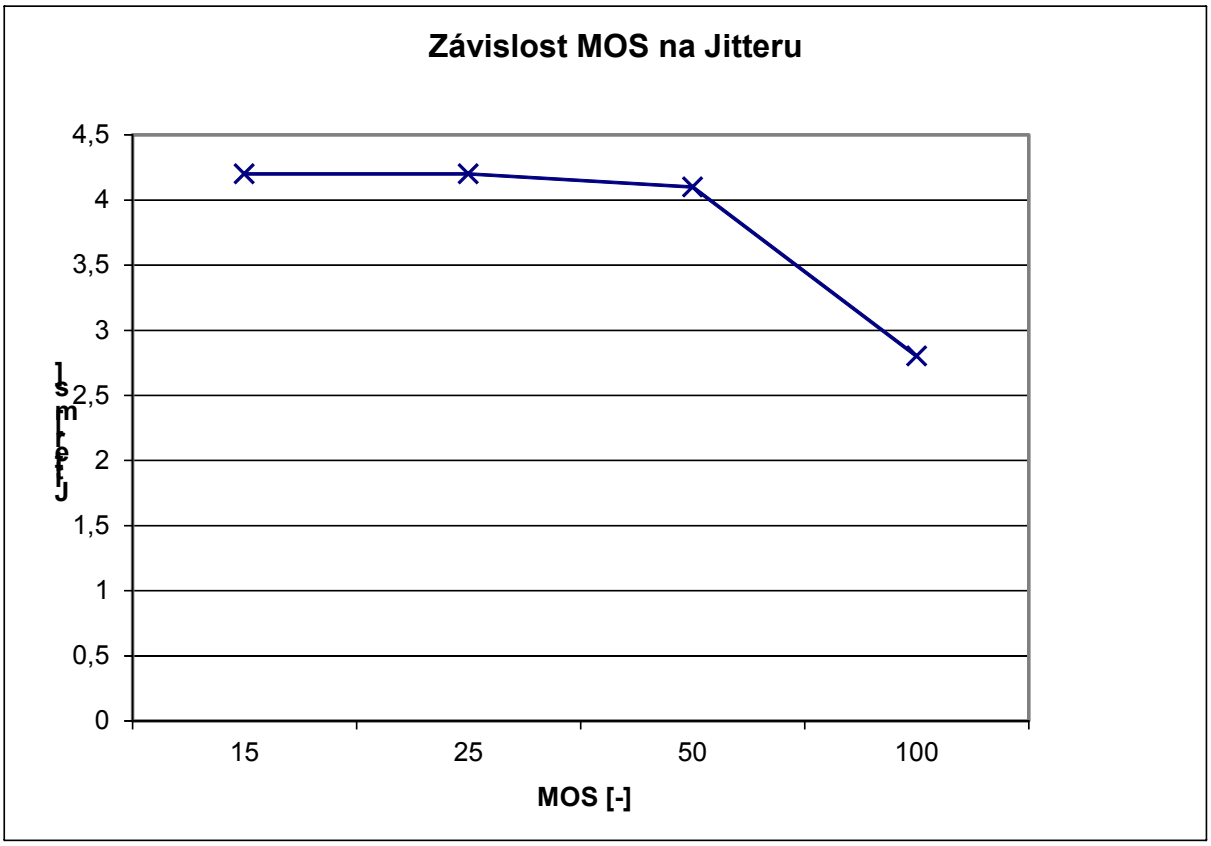
Graf č.2 Závislost MOS na Zpoždění

by si také skákali do řeči, což jsou dva velmi nežádoucí jevy. MOS:CQ by měl tyto parametry brát v potaz, ale jelikož byl na lince jen jednosměrný provoz, tak nebyl tento parametr ovlivněn.

Dále byly proměřeny závislosti kvality služeb na parametru Jitter při konstantním nastavení zpoždění 200ms. Jitter byl při tomto nastavění měněn a parametry byly zaznamenány do tabulky č. 7.

Tab. 7 Parametry MOS v závislosti na jitteru

	Jitter [ms]			
	15	25	50	100
MOS:LQ	4,2	4,2	4,1	2,8
MOS:CQ	4,2	4,2	4,1	2,7



Graf č.3 Závislost MOS na Jitteru

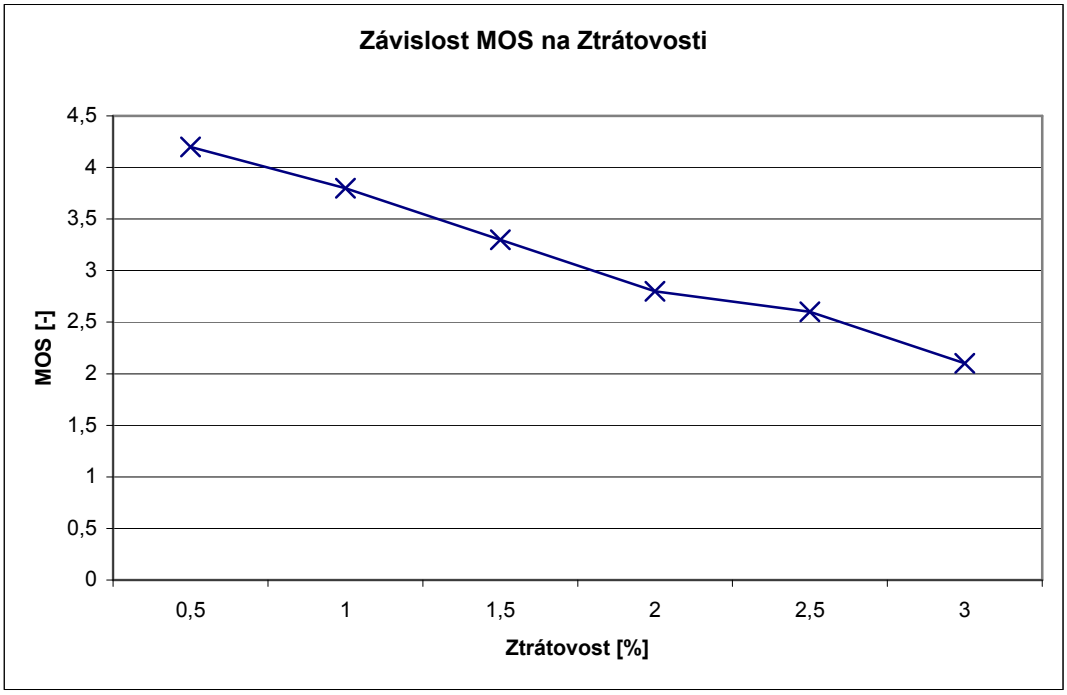
Z výsledku vyplývá, že opět při použití jednosměrného provozu není kvalita hovoru tak výrazně ovlivňována jak by tomu bylo při použití obousměrného provozu. Podle Tab. 3 by měla být kvalita služeb pro jitter nad 50 ms již nevyhovující, avšak zde se jen nepatrně zhoršila. Až při hodnotách jitteru nad 100 ms byl hovor dostatečně deformován a hodnota MOS faktoru klesla pod 3.

V poslední části měření byla pomocí WANem emulátoru postupně měněna ztrátovost na lince a výsledky byly zaznamenány do tabulky č. 8.

Tab. 8 Parametry MOS v závislosti na ztrátovosti

	Ztrátovost [%]					
	0,5	1,0	1,5	2,0	2,5	3,0
MOS: LQ	4,2	3,8	3,3	2,8	2,6	2,1
MOS:CQ	4,2	3,7	3,3	2,8	2,4	2,1

Z výsledků vyplývá, že při ztrátovosti do 0,5% se chová linka jako za běžných podmínek a tedy s vynikající kvalitou. V intervalu ztrátovosti od 1 do 2% se jedná ještě o přijatelné hodnoty a hovor je dobře slyšitelný. Při ztrátovosti nad 2,5% se hovor rozpadá a je již není možné vést normální konverzaci.



Graf č.4 Závislost MOS na Ztrátovosti

3 NÁVRH SÍTĚ V PROSTŘEDÍ OPNET MODELER

3.1 Program OPNET Modeler

Program OPNET Modeler je simulační program, který slouží pro návrhy, analýzy a simulace počítačových sítí. Usnadňuje tak práci techniků při vytváření takových sítí a jejich následném ladění, pokud už jsou sítě v provozu. Často bývá pro správce sítě složité odhadnout, jak bude síť v reálném prostředí vypadat a jestli bude mít dostatečnou kapacitu popř., jestli nebude docházet ke kolizím. Pomocí tohoto programu mají inženýři možnost si takové sítě nejdříve navrhnout a otestovat. Program byl vyvinut v roce 1987 americkou firmou OPNET Technologies a umožňuje simulovat sítě na jakékoliv úrovni díky použití velkému množství knihoven se síťovými prvky. OPNET Modeler také přináší možnost programovat si vlastní síťové protokoly.

Užitečnou vlastností tohoto softwaru je možnost vytváření velkého množství statistik z každé simulace. Je tak možné simulovat i situace, které by na reálné síti byly velmi těžko proveditelné ne-li nemožné, avšak z hlediska bezpečného a plynulého provozu je nutné tyto stavy vyloučit. Výsledky simulací je možné generovat ve formátech HTML nebo XML, nejčastěji se však využívá ukládání do tabulek.

Správa jednotlivých modelů je rozdělena do několika úrovní. OPNET Modeler totiž pracuje s třemi hierarchicky řazenými editory. S každým editorem je možné pracovat zvlášť a není závislý na ostatních editorech. Jedná se o následující editory:

- Editor Projektu
- Editor Uzlu
- Editor Procesu

Editor projektu umožňuje graficky znázorňovat topologii sítě pomocí komponent z široké palety. Řídí tak neomezeně velkou síť, která může být členěna podle států, měst, firem či kanceláří. Obsahuje také veškeré zeměpisné a fyzikální vlastnosti dané sítě. Na nižší úrovni se nachází editor uzlu, který zobrazuje informace o toku dat mezi

jednotlivými prvky sítě – tzv. moduly. Moduly jsou procesy, které posílají a přijímají pakety mezi sebou. Na nejnižší úrovni se nachází editor procesu, který popisuje chování jednotlivých modulů. Jedná se o stavový automat, který detailně popisuje všechny úrovně modelu. Jednotlivě stavy a jejich přechody jsou definovány v grafickém diagramovém editoru a jejich kód je kompilován pomocí programovacího jazyka C++.

3.2 Návrh bezdrátové sítě

Důležitým prvkem při práci s programem OPNET Modeler je nutnost používat stále stejnou verzi. Pro tuto práci byla zvolena aktuální verze 16.1. Bohužel není OPNET vůbec kompatibilní mezi verzemi a to ani zpětně. Takže programy vytvořené ve verzi 16.0 a nižší nejdou ve verzi 16.1 otevřít.

3.2.1 Vytvoření modelu

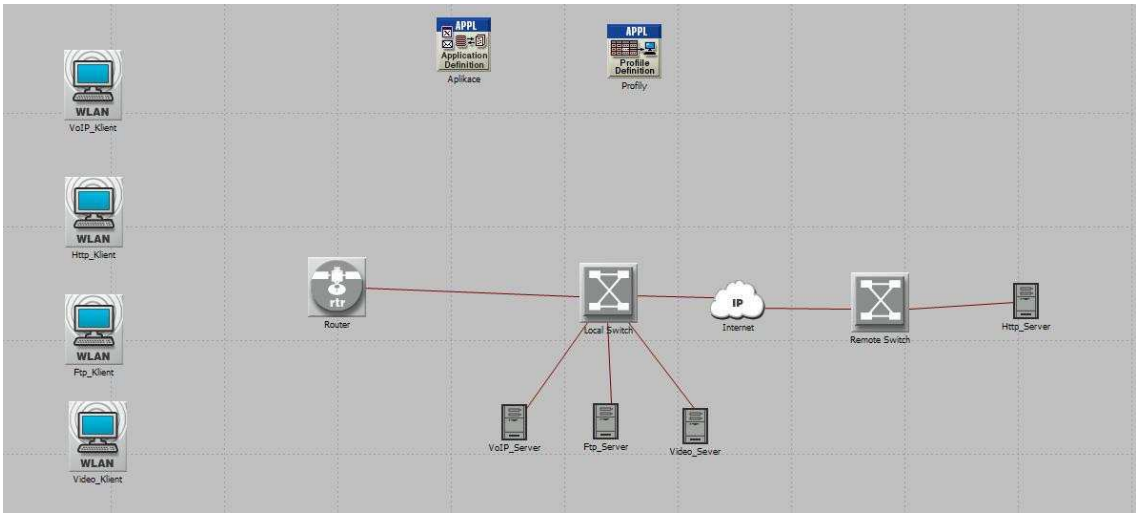
Nejdříve byl vytvořen nový model a pojmenován „DP_WiFi“ se scénářem „DP_WiFi_1“. Projekt byl založen s prázdným scénářem pomocí „Create empty scenario“. Jelikož se jedná o lokální síť, jako prostředí byla zvolena Kancelář o velikosti 25 x 25 m a dále byla jako použitá technologie vybrána položka wireless_lan_adv z modelové rodiny.

Do prázdného projektu z palety nástrojů byly vloženy následující prvky: wlan_ethernet_router_adv, který bude sloužit jako bezdrátový směrovač, 4x wlan_wkstn_adv, jako čtyři koncové stanice. Dále 4x ethernet_server_adv, který bude sloužit jako server pro aplikace. Dále dvakrát ethernet16_switch_adv a ethernet4_slip8_cloud_adv pro simulaci internetu a pro přístup na zvdálený Web_server pomocí Http aplikace. Důležité jsou také prvky pro nastavení jednotlivých aplikací, kterými jsou Application Config a Profile Config. Zapojení jednotlivých modelů je možné vidět na obr. 8.

Seznam použitých modelů:

- Router - wlan_ethernet_router_adv
- VoIP_Klient - wlan_wkstn_adv
- Video_Klient - wlan_wkstn_adv
- Http_Klient - wlan_wkstn_adv

- Ftp_Klient - wlan_wkstn_adv
- VoIP Server - ethernet_server_adv
- Video Server - ethernet_server_adv
- Http Server - ethernet_server_adv
- Ftp Server - ethernet_server_adv
- Local Switch - ethernet16_switch_adv
- Remote Switch - ethernet16_switch_adv
- Internet - ethernet4_slip8_cloud_adv
- Aplikace - Application Config
- Profily - Profile Config



Obr. 8 Schéma zapojení v OPNET Modeleru

3.2.2 Nastavení WLAN sítě

Nastavení se provádí po pravém kliknutí na daný prvek a výběrem položky Edit Attributes. Na směrovači s názvem Router byla nastavena bezdrátová síť. Jedná se o síť standardu 802.11g na 1. kanálu. Přenosová rychlost (Data rate) byla nastavena na hodnotu 54 Mb/s. BSS Identifier byl zvolen zcela náhodně na hodnotu 10 a slouží k tomu, aby určoval, ke kterým bezdrátovým sítím se budou stanice připojovat. Tato funkce je zejména důležitá v případě, kdy bude v modelu více jak jeden bezdrátový směrovač a aby tedy bylo jasné, ke kterému uzlu jsou koncové stanice připojeny. Stanice byly nastaveny velmi obdobně jako směrovač, jen byla vypnuta položka Access

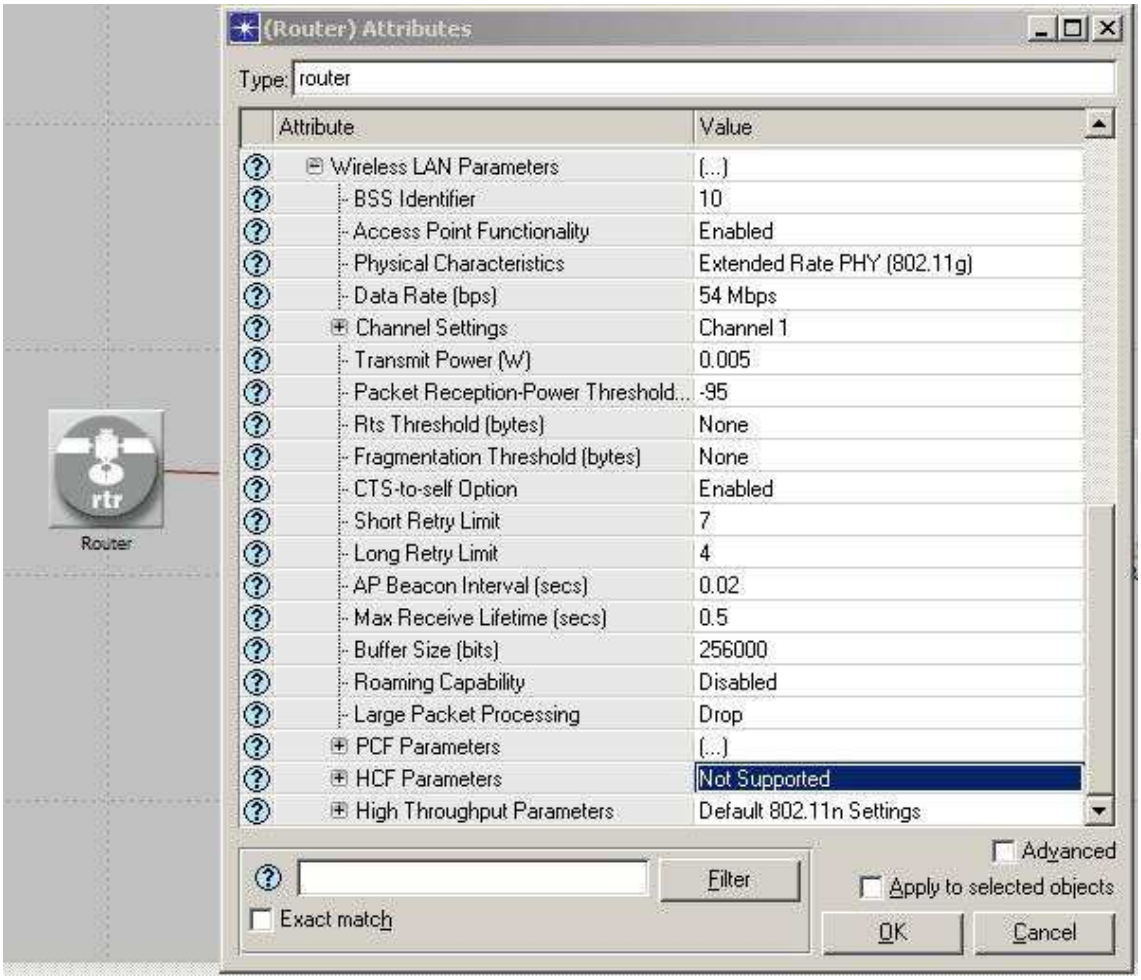
Point Functionality, není totiž žádoucí, aby samotné stanice sloužili jako přístupové body. Na začátek byla také vypnuta podpora QoS tím, že byla nastavena hodonta HFC Parametrs na Not Supported - tedy, že není podporována. Tento parametr se bude později měnit, až bude zprovozněna funkce pro QoS. Ostatní parametry nebyly měněny.

Router

- Wireless LAN Parameters
  - BSS Identifier: 10
  - Access Point Functionality: Enabled
  - Physical Characteristics: Extended Rate PHY (802.11g)
  - Data Rate (bps): 54 Mbps
  - Channel Settings: Channel 1
  - HFC Parametrs: Not Supported

Klienti

- Wireless LAN Parameters
  - BSS Identifier: 10
  - Access Point Functionality: Disabled
  - Physical Characteristics: Extended Rate PHY (802.11g)
  - Data Rate (bps): 54 Mbps
  - Channel Settings: Channel 1
  - HFC Parametrs: Not Supported



Obr. 9 Nastavení parametrů WiFi sítě

3.2.3 Nastavení Aplikací

Dále je nutné v Application configuration přidat jednotlivé aplikace, které na síti budou provozovány a následně je nadefinovat. Byly vytvořeny celkem čtyři aplikace pro čtyři různé služby. První s názvem „httpapp“ slouží ke generování HTTP provozu na lince a k jejímu drobnému zatěžování. HTTP bude jako jediná využívat IP cloud, tedy simulaci internetu. Ostatní aplikace poběží na lokální síti. Druhá aplikace s názvem „voiceapp“ generuje hlasový provoz na síti. Třetí aplikací je „videoapp“, která simuluje provoz streamovaného videa po síti. Poslední aplikace je „ftpapp“, která slouží ke generování FTP provozu na síti z klienta na server.

Aplikace se definuje opět pravým kliknutím na Application configuration, a zvolíme Edit Attributes. V záložce Application Definitions zvolíme počet řádků, podle toho

kolik aplikací je nutno nakonfigurovat. V našem případě se jedná o 4 aplikace a tak volíme Numer of Rows na 4. Dále v záložce Voice Encoder Schemes je možné vybrat schéma pro kódování zvuku, tedy jaký kodek je použit. Zvolíme jeden univerzální kodek, a proto počet řádků stanovíme na 1. Vybereme pulzní kódovou modulaci - PCM a jako kodek G.711 s přenosovou rychlostí 64 kb/s.

Nyní už je možné konfigurovat jednotlivé aplikace. Aplikace se pojmenuje v položce name a v záložce Description je možné vybrat jednu z devíti nabízených možností: Custom, Databáze, Email, Ftp, http, Print, Repote Login, Video Conferencing, Voice.

Nastavení aplikace HTTP:

- Name: httpapp
- Description: Http
    - HTTP: Specification: HTTP 1.1
    - Page Interval Time: exponential (5)
    - ToS: Backgroung (1)

Nastavení aplikace FTP:

- Name: ftpapp
- Description: Ftp
    - Command Mix: 50%
    - Inter-Request: exponential (1)
    - File Size: constant (50000)
    - ToS: Best Effort (0)

Nastavení aplikace VoIP:

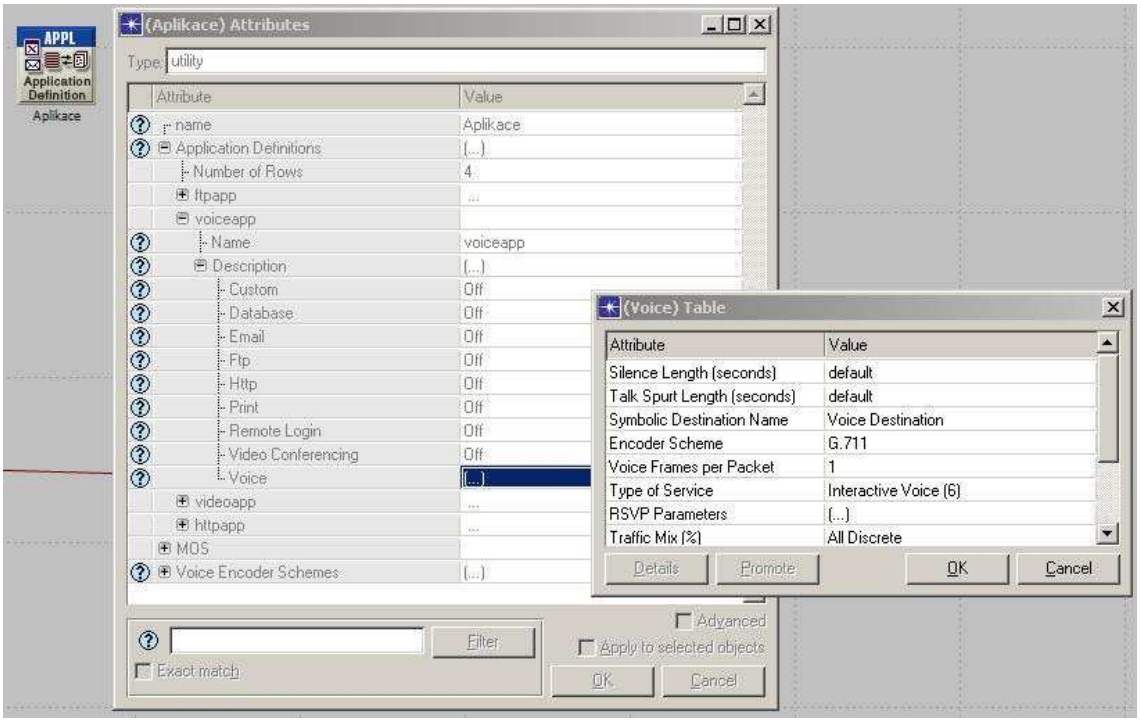
- Name: voiceapp

- Description: Voice
    - Encoder Schneme: G.711
    - ToS: Interactive Voice (6)
    - Signaling: H.323

Nastavení aplikace Video:

- Name: videoapp
- Description: Video Conferencing
    - Frame Interarrival Time: 30 frames/sec
    - Frame Size: 352x240 pixels
    - ToS: Interactive Multimedia (5)
    - Traffic Mix: 25%

Všechna nastavení mají uveden typ služby (ToS), ten je ale nepodstatný pokud není použita funkce HFC na routeru a na jednotlivých stanicích. Http aplikace má standardní nastavení na hodnotu 1, tedy background, čili aplikace běžící na pozadí. Ftp aplikace má hodnotu nastavenu na Best Effort, pro kterou je důležitější aby data byla doručena nehledě na jejich zpoždění. Video a hlas mají své vlastní třídy 5 – Interactive Multimedia a 6 – Interactive Voice, kdy je už v úvahu bráno i zpoždění a další parametry ovlivňující interaktivní komunikaci po internetu. Z výše uvedeného nastavení je vidět, že aplikace simulující http provoz bude jednat podobně jako by uživatel klikal na novou stránku průměrně každých 5 sekund a bude se jednat pouze o nenáročný provoz. Aplikace FTP bude stahovat data o velikosti 50 kb. Pro hlasovou aplikaci je použit již předem nastavený kodek G.711, pro řízení spojení zde byla použita protokolová sada H.323 a to zejména proto, že použití SIP protokolu v prostředí OPNET Modeler nefungovalo správně a i po nastavení SIP Proxy serveru, hlásila simulace chybu. Video bylo zvoleno nastavení takové, aby aplikace streamovala video o rozlišení 352x240 pixelů s frekvencí 30 snímků za sekundu.



Obr. 10 Nastavení Hlasové aplikace

3.2.4 Natavení profilů

V Profile Configu byly dále vytvořeny čtyři profily, které budou spouštět již vytvořené aplikace. Obecně může jeden profil spouštět i více aplikací, ale zde byla zvolena možnost vlastního profilu pro každou aplikaci. Hlasové aplikaci byl vytvořen profil s názvem „VoIP_Profil“, k FTP aplikaci profil pojmenovaný „FTP_Profil“, pro http aplikaci byl vytvořen profil s názvem „Http_Profil“ a nakonec pro video přenosy profil s názvem „Video_Profil“.

Profil se vytváří opět pravým kliknutím na Profile Config a vybráním možnosti Edit Attributes. Dále je nutné vybrat počet řádků: Numer of rows pro vytvoření profilů. V tomto případě opět 4. Položka Profile Name je nutná pro pojmenování jednotlivých profilů. Dále v záložce Application je nutné přiřadit profilu již existující aplikaci. Na výběr by měli být všechny již vytvořené aplikace z kapitoly 3.2.3. Další položky jsou následující:

- Start Time Offset – udává v sekundách čas, kdy se daná aplikace spustí po spuštění profilu

- Duration – udává dobu trvání dané aplikace
- Repeatability – nastavuje počet opakování dané aplikace a čas mezi jednotlivými opakováními
- Operation Mode – definuje, jak se budou dané aplikace spouštět
- Start Time – určuje čas od začátku, kdy bude daný profil spuštěný
- Duration – nastavuje délku trvání profilu, většinou do konce simulace
- Repeatability – opět udává počet opakování, tentokráte ale daného profilu, nikoliv aplikace

Http_Profil

- Profile Name: Http_Profil
- Applications:
    - Name: httpapp
    - Start Time Offset: uniform (1,5)
    - Duration: End of Profile
- Operational Mode: Serial (Ordered)
- Start Time: constant (10)
- Duration: End of Simulation

Ftp_Profil

- Profile Name: Ftp_Profil
- Applications:
    - Name: ftpapp
    - Start Time Offset: uniform (1,5)
    - Duration: End of Profile
- Operational Mode: Serial (Ordered)
- Start Time: constant (20)

- Duration: End of Simulation

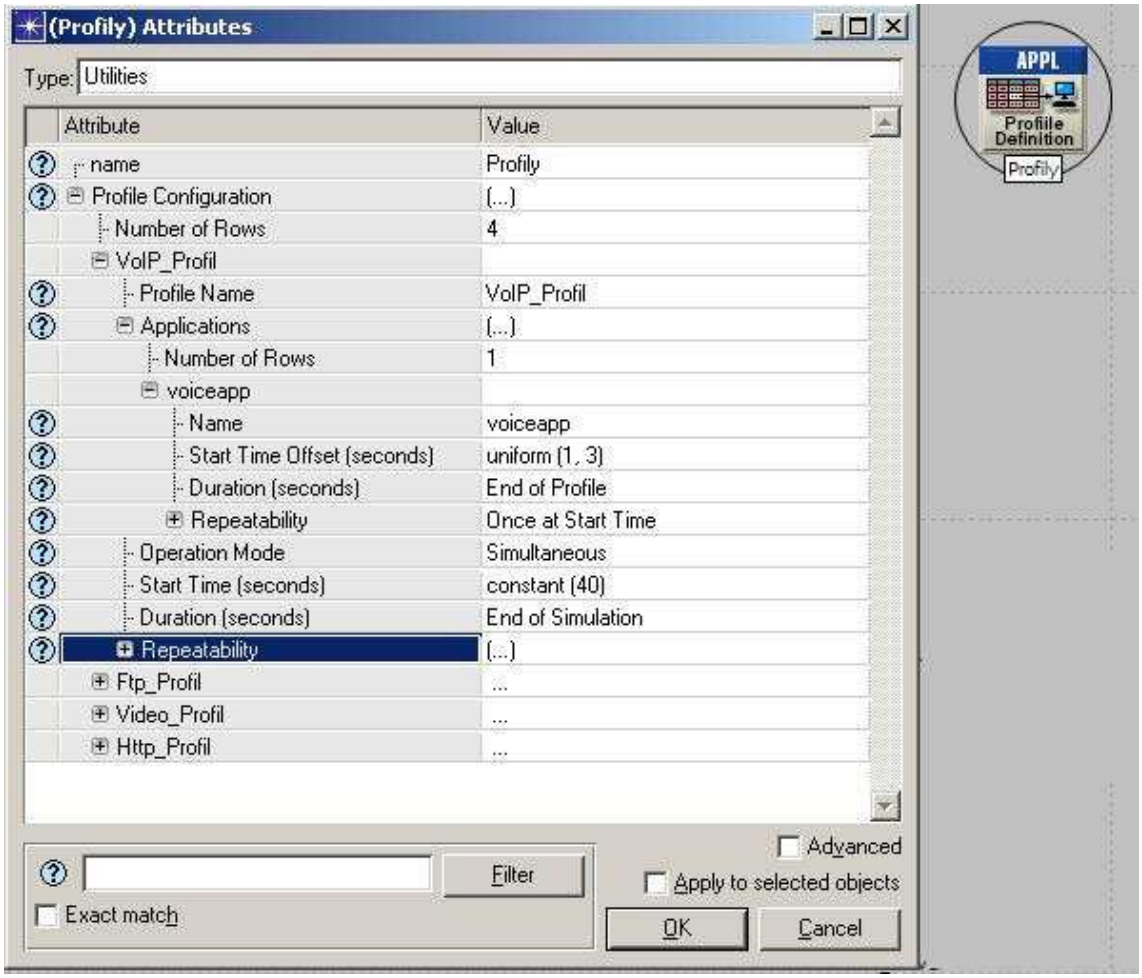
Hlasový_Profil

- Profile Name: VoIP_Profil
- Applications:
    - Name: voiceapp
    - Start Time Offset: uniform (1,3)
    - Duration: End of Profile
- Operational Mode: Serial (Ordered)
- Start Time: constant (40)
- Duration: End of Simulation

Video_Profil

- Profile Name: Video_Profil
- Applications:
    - Name: videoapp
    - Start Time Offset: uniform (1,5)
    - Duration: End of Profile
- Operational Mode: Serial (Ordered)
- Start Time: constant (50)
- Duration: End of Simulation

Z výše uvedeného nastavení je tedy možné vidět, že se budou od začátku simulace postupně spouštět aplikace tak, že 10 sekund od začátku se začne generovat Http provoz, dále 20 sekund od začátku Ftp provoz, poté v 40. sekundě začne hlasová komunikace a 50 sekund od začátku začne i provoz streamování Videa.



Obr. 11 Profil aplikace Hlasových služeb

3.2.5 Nastavení aplikací na stanicích a serverech

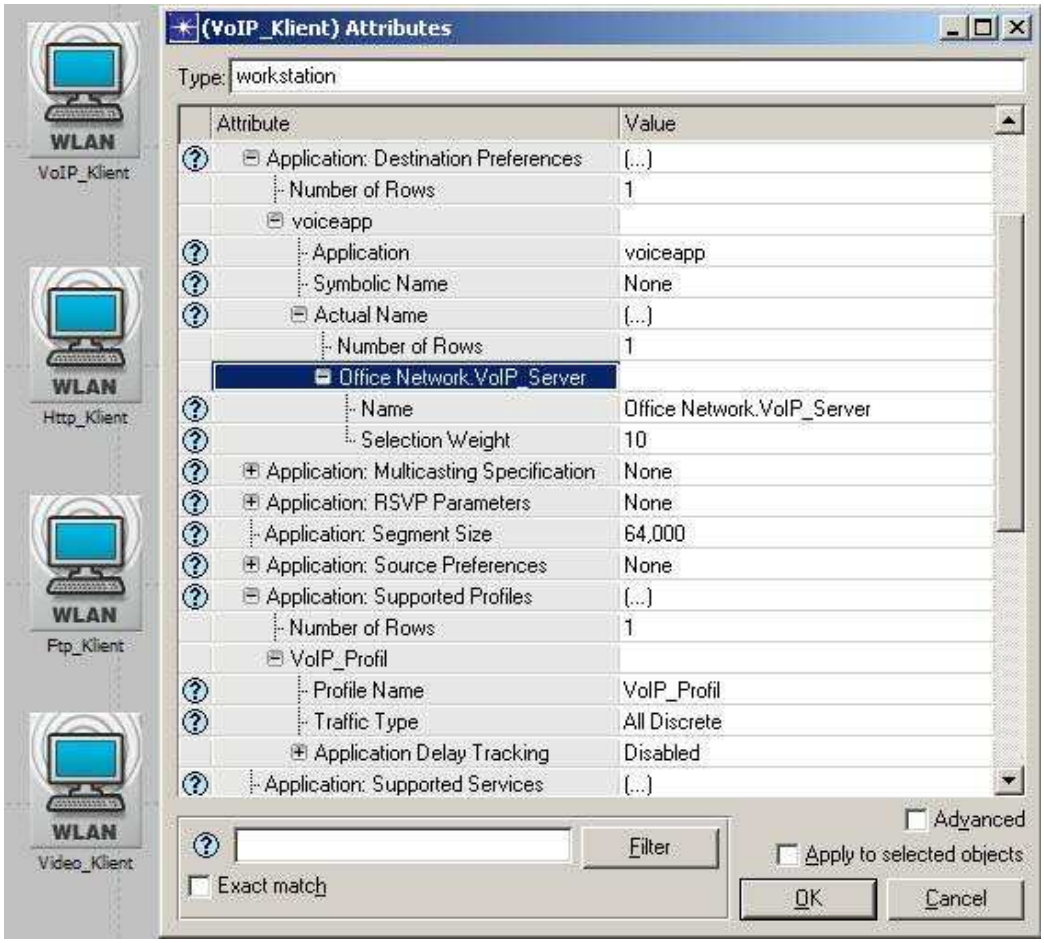
Pro správné fungování sítě je nutné nastavit na každém koncovém uzlu jaké aplikace, podle jakých profilů bude daná stanice používat. U počítačů je pak také nutné nastavit v Destination Preference protilehlou stranu spoje (tedy server). U serverů stačí pouze nastavit podporované aplikace. Konfigurace je vidět níže. Obdobně je nakonfigurována na všech ostatních koncových bodech. Konfigurují se následující prvky:

- Applications: Destination Preferences – natavuje spojení mezi reálným uzlem sítě a danou aplikací
- Applications: Supported Profiles – zde se vyberou profily, které bude stanice či server podporovat

- Applications: Supported Services – zde se vyberou přímo aplikace, kterou budou na stanici či serveru obsluhovány

VoIP_Klient

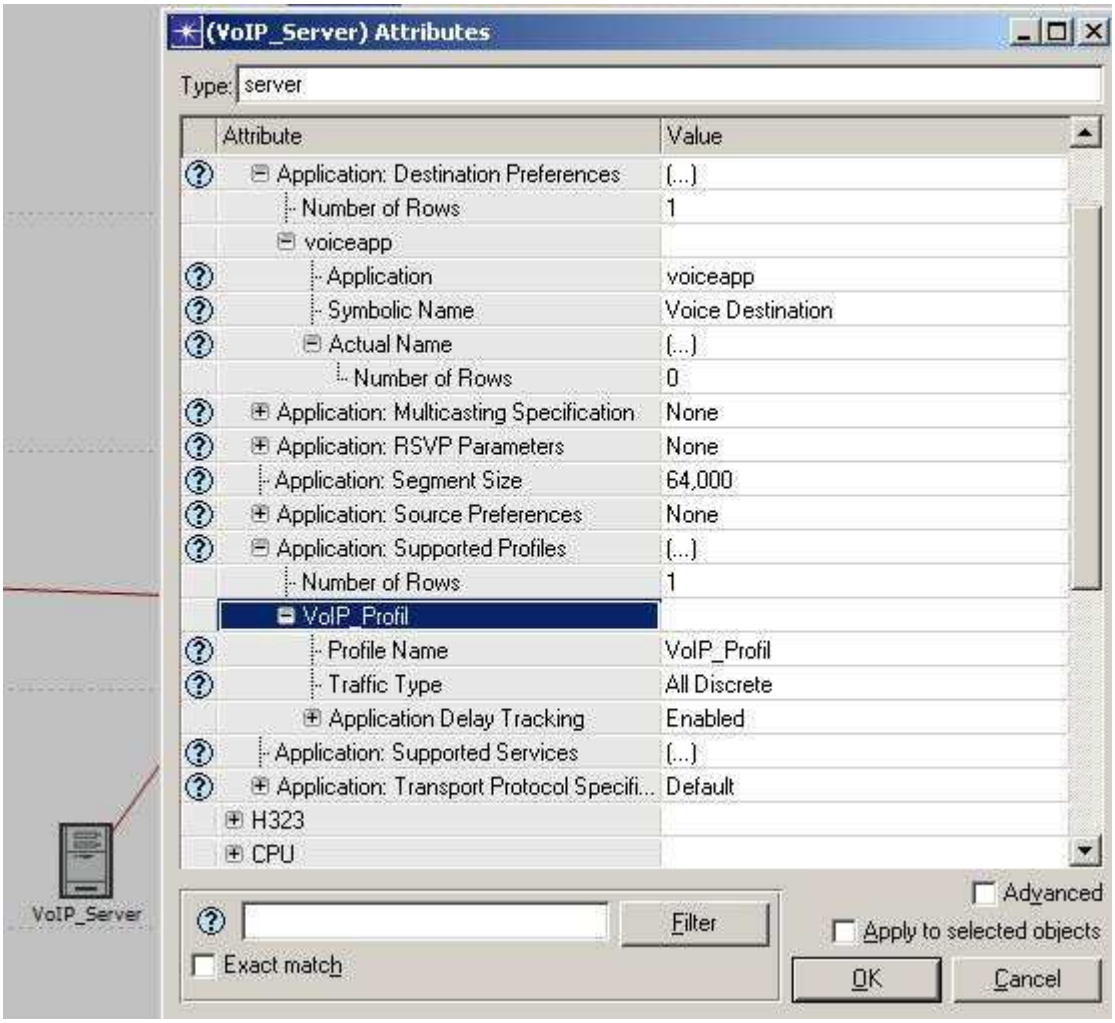
- Applications
  - Destination Preferences
    - Number of rows: 1
    - Appication: voiceapp
    - Actual Name: Office.Network.VoIP_Server
  - Supported Profiles
    - Profile Name: VoIP Profile
  - Supported Services
    - Name: voiceapp – Supported



Obr. 12 Nastavení aplikace na klientské stanici

VoIP_Server

- Applications
  - Destination Preferences
    - Number of rows: 1
    - Appication: voiceapp
    - Symbolic Name: Voice Destination
  - Supported Profiles
    - Profile Name: VoIP Profile
  - Supported Services
    - Name: voiceapp – Supported



Obr. 13 Nastavení aplikace na serveru

3.2.6 Nastavení připojení k Internetu

Nastavení přístupu do jiné sítě prostřednictví internetu je v prostředí OPNET Modeler velmi jednoduché. Pro tuto práci nebylo nutné nastavování jednotlivých směrovacích protokolů, a tak bylo pouze nastaveno několik základních údajů na přepínači na fyzické vrstvě. MAC adresy se navíc nemusí volit podle obvyklých pravidel, ale stačí zadat přirozená čísla. Nastavení se opět prování po kliknutí pravým tlačítkem na Switch a volbou Edit Attributes.

Local Switch

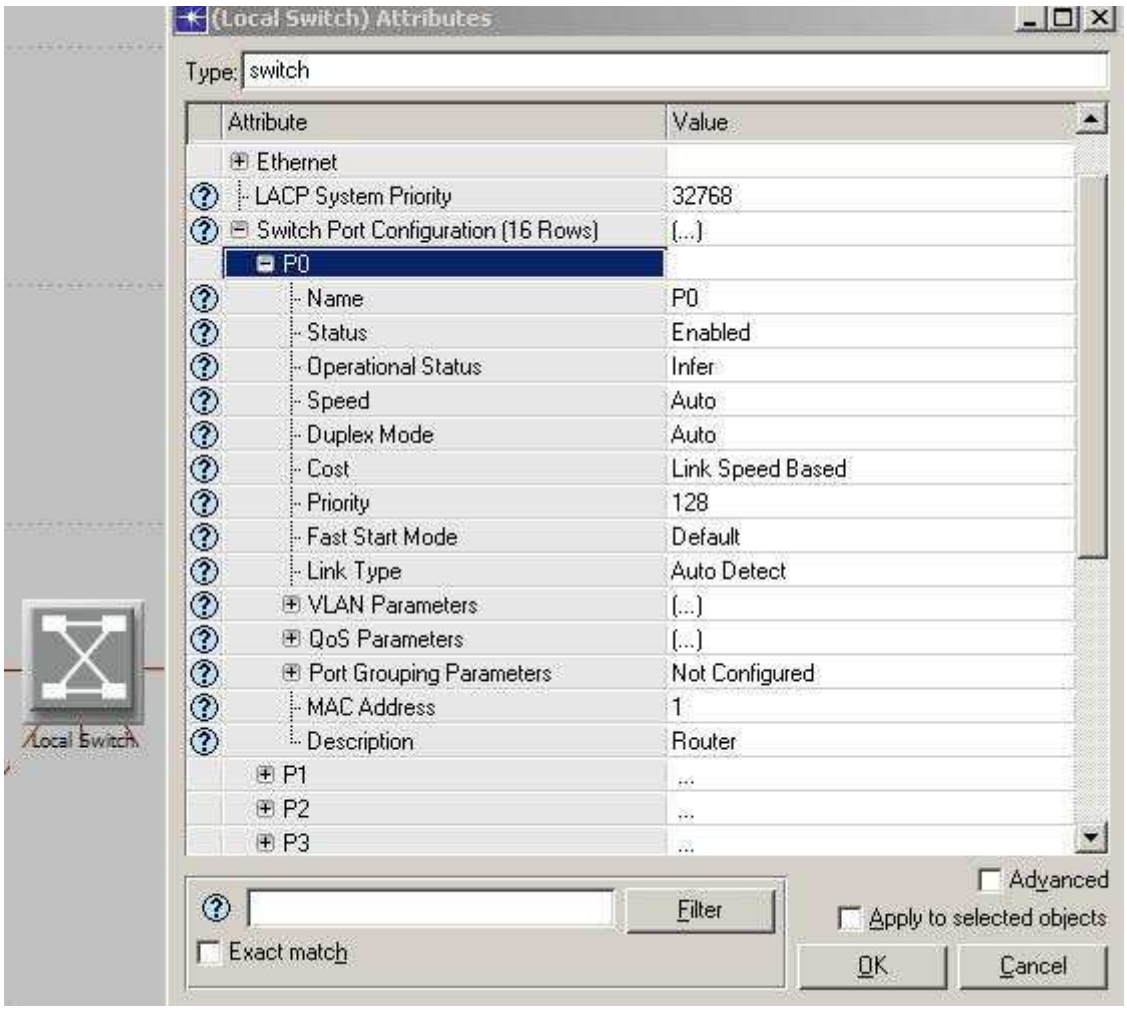
- Switch Port Configuation
    - P0
        - MAC Address: 1
        - Descrtiption: Router
    - P1
        - MAC Address: 2
        - Descrtiption: VoIP_Server
    - P2
        - MAC Address: 3
        - Descrtiption: Ftp_Server
    - P3
        - MAC Address: 4
        - Descrtiption: Video_Server
    - P4
        - MAC Address: 5
        - Descrtiption: Internet

Na prvku IP Cloud není nutné nic nastavovat. Local Switch byl spojen se servery pomocí kabelu 100BaseT, stejně tak jako Remote Switch s Http_Serverem. Spojení mezi Switchi a Internetem (IP Cloud) bylo provedeno pomocí kabelů 1000BaseX.

Remote Switch

- Switch Port Configuation
    - P0
        - MAC Address: 6
        - Descrtiption: Internet

- P1
  - MAC Address: 7
  - Descrtiption: Http_Server



Obr. 14 Nastavení přepínače

3.2.7 Nastavení simulace

V závěru nastavení vybereme, které statistiky mají být v simulaci brány v potaz. Z globálních statistik byly vybrány statistiky pro FTP, HTTP, hlasové služby (Voice),video služby a WLAN provoz. Na uzlech pak byly zobrazeny statistiky pro FTP klienty a servery, http klienty a servery. Dále statistiky pro obě strany VoIP provozu a Video provozu a dále statistiky bezdrátové sítě (WLAN). Nakonec byla nastavena dálka simulace na 10 minut.

3.2.8 Duplikování scénáře

Než bude možné se pustit do sběru statistik, bylo nutné vytvořit k aktuálnímu scénáři nový scénář, kde bude užito již QoS. V OPNET Modeleru je velmi jednoduché scénář duplikovat a to v menu Scenarios -> Duplicate Scenario. Nový scénář byl pojmenován jako „DP_WiFi_2“ a zdědil všechna nastavení od původního scénáře. V novém scénáři byla změněna jen jedno velmi zásadní nastavení a to povolení HCF Parametrs.

Router + Stanice
- Wireless LAN Parameters
  - HCF Parametrs: Default

Dále by scénář duplikován ještě dvakrát. Nově vytvořený scénář s názvem „DP_WiFi_3“ obsahuje stejné nastavení jako scénář 2, tedy již s použitím algoritmů zajišťující QoS, avšak tentokrát byla změněna síť na standard 802.11a

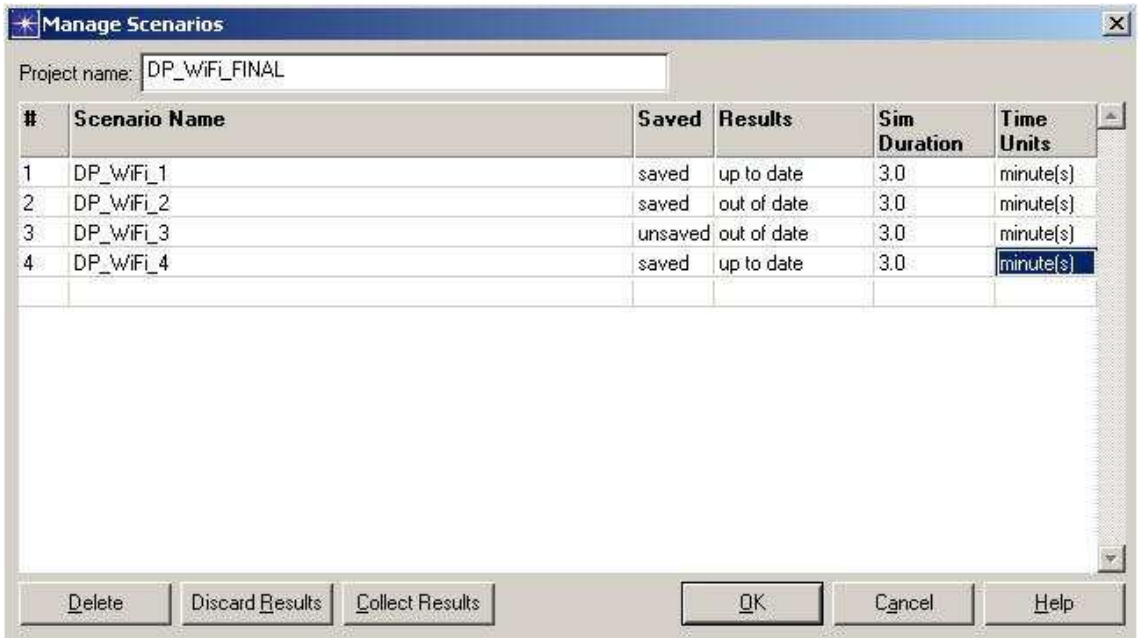
Router + Stanice
- Wireless LAN Parameters
  - Physical Characteristics: OFDM (802.11a)

Čtvrtý scénář s názvem „DP_WiFi_4“ byl opět vytvořen na základě druhého scénáře a opět byla změněna vlastnost určující standard sítě, tentokrát však ještě i rychlost přenosu.

Router + Stanice
- Wireless LAN Parameters
  - Physical Characteristics: HT PHZ 2.4 GHz (802.11n)
  - Data Rate (bps): 65 Mbps (base) / 288.9 Mbps (max)

Tím se zpřístupní možnost využívání tříd v aplikačním nastavení pro všechny druhy dostupných Wi-Fi standardů. Bohužel standard 802.11b nebyl na výběr, pravděpodobně proto, že se jedná o starší standard a je velmi podobný 802.11g, jen pomalejší.. Nyní už nezbývá, než spustit simulaci se všema scénáři. To je možné v menu Scenarios -> Manage Scenarios, kde je nutné v kolonce Results u obou scénářů vybrat položku collect (sběr dat) a potvrdit OK. Tím se simulace spustí. V položce status je možné sledovat aktuální stav simulace jednotlivých scénářů, čas, který již uběhl a odhadovaný

čas do konce dané simulace. Simulace bude probíhat celkem dlouho, záleží na výpočetním výkonu daného PC.

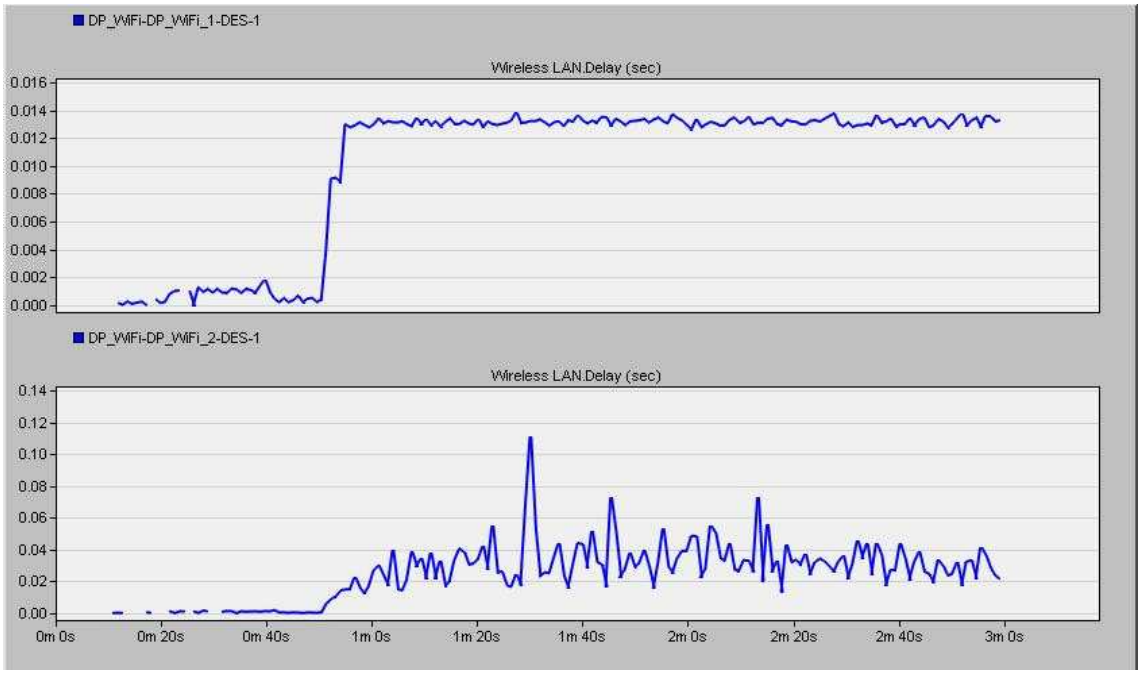


Obr. 15 Nastavení simulace scénářů

3.3 Výsledky simulace

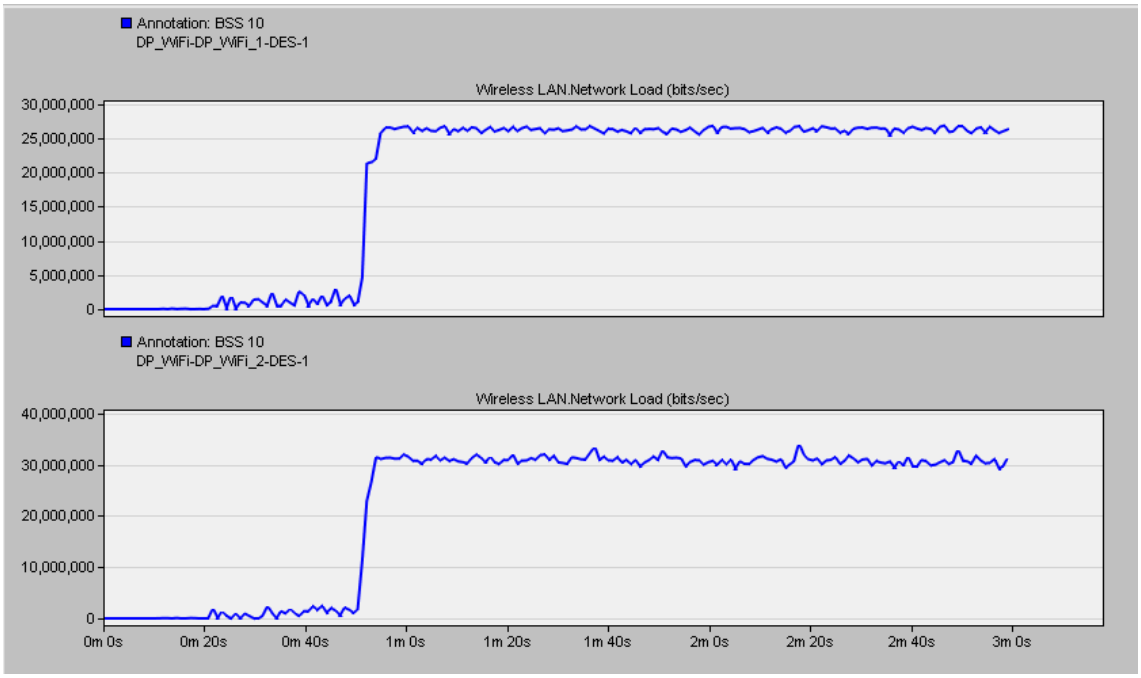
Po proběhnutí simulace je možné zobrazit výsledky pomocí pravého kliknutí na pracovní plochu a zvolením „View Results“. Důležité je také zvolit, které scénáře mají být zobrazeny, nebo bude zobrazen jen aktuální scénář. Výsledky všech scénářů se zobrazí tak, že se v menu Results for: zvolí položka Current Project místo položky Current Scenario. Nyní by již měli být vidět všechny scénáře a budou potřeba zobrazit, zaškrtneme. Nejdříve bylo pracováno pouze se scénáři DP_WiFi_1 a DP_WiFi_2, tedy pouze se sítí dle standardu 802.11g. Srovnání s ostatními standardy je shrnuto v kapitole 3.3.5.

3.3.1 Statistiky WLAN



Obr. 16 Zpoždění na Routeru

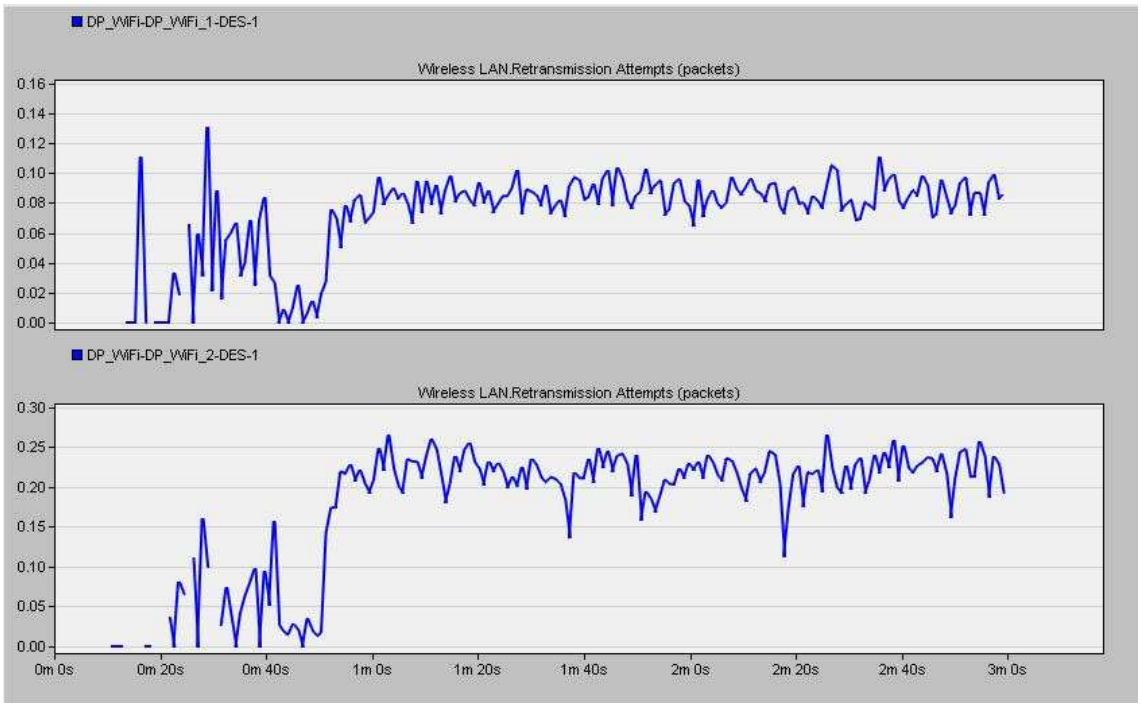
Jelikož datová část generovala velký provoz, který se postupně zvedal s narůstajícím časem, je možné pozorovat na obrázku 16 statistiku zpoždění dat na routeru. Zde je vidět i nastavení simulace, kdy se nejprve začal generovat Ftp a Http provoz a od 40 sekundy hlasový provoz a dále od 50 sekundy provoz streamovaného videa, který linku výrazně zatížil. V horní části obrázku jsou vidět výsledky scénáře WiFI_1 tedy bez podpory QoS a v dolní polovině pak zpoždění s použití algoritmů QoS ve scénáři WiFi_2. Zde je vidět, že s podporou QoS je celkové zpoždění nižší i když kolísá, což není žádný velký problém.



Obr. 17 Data přeposílaná směrovačem

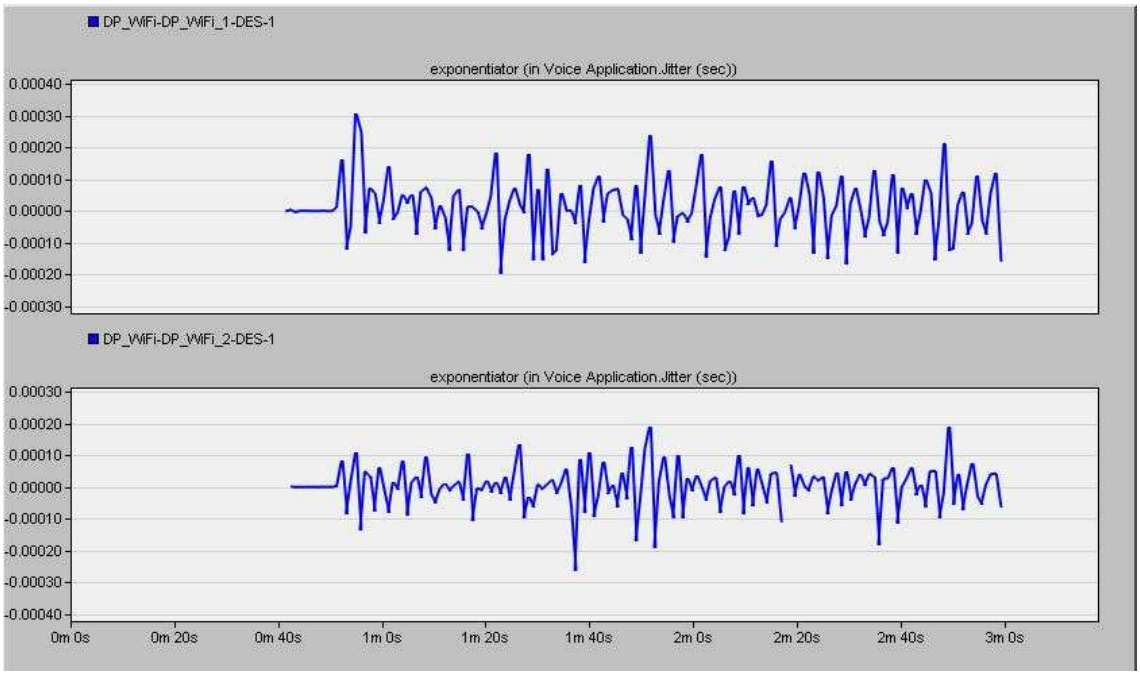
Na obrázku 17 je také vidět jaké bylo postupně zatížení dat procházejících Routerem. V horní polovině je opět vidět síť bez podpory QoS a v dolní s QoS. Padesát sekund od začátku simulace je vidět výrazný nárůst v přenášených datech, kdy se spustila video aplikace. Celkově má síť s podporou QoS větší propustnost, jelikož umožňuje lepší režii procházejících dat a nedochází tak k jejich zahazování.

Obrázek 18 níže zobrazuje graf požadavků na opětovné posílaní dat v rámci bezdrátové sítě. Jak je vidět v dolní polovině, kde je sít s podporou QoS, tak došlo k nárůstu takovýchto žádostí. To je způsobeno především díky fungování QoS, která se snaží o bezchybný přenos dat od Klienta k Serveru nebo obráceně. Znehodnocená data jsou tak opětovně zasílána popř. přerušené FTP a HTTP spojení musí být znovu navázáno, aby nenarušilo chod aplikace.



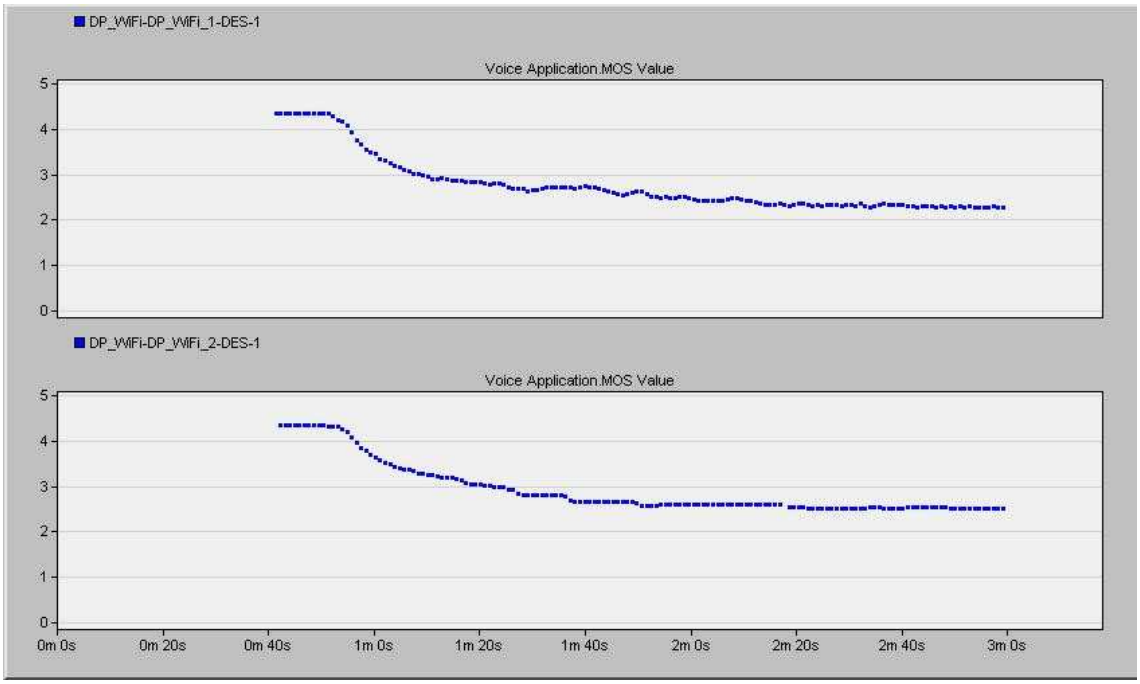
Obr. 18 Znovu zasílaná data

3.3.2 Statistiky Hlasových služeb



Obr. 19 Statistika jitteru

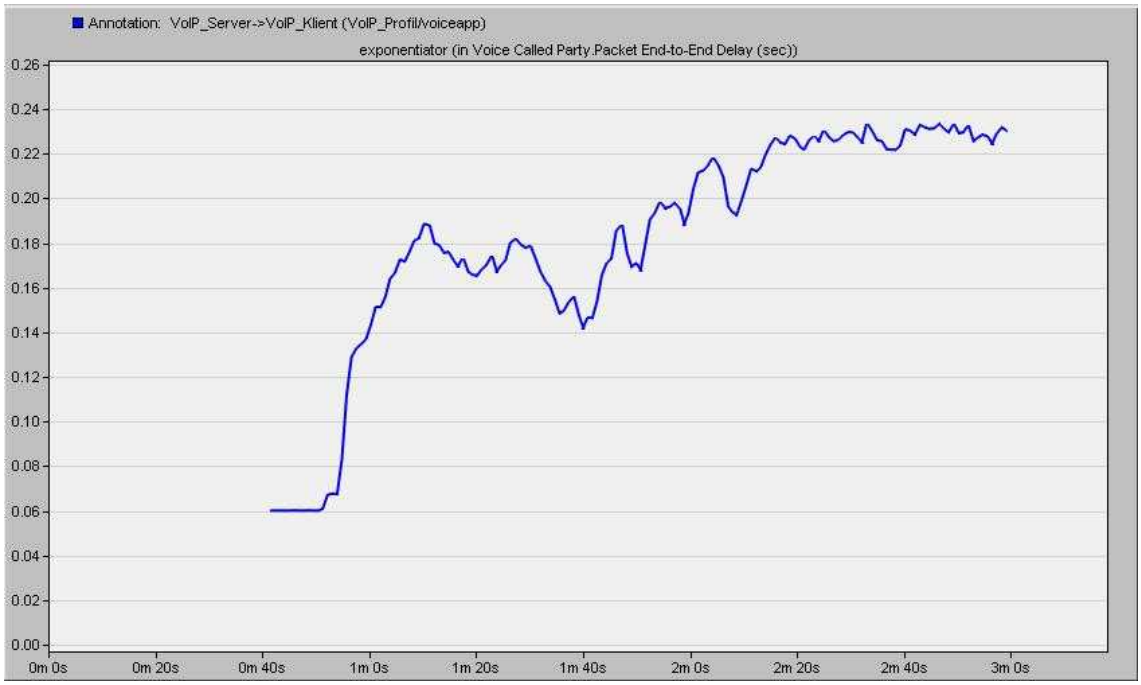
OPNET Modeler umožňuje také sledovat statistiky Jitter a MOS, důležité pro zhodnocení interaktivní hlasové komunikace v síti. Na obrázku 19 jsou zachyceny statistiky Jitteru na síti. V horní polovině je opět hlasová aplikace bez podpory QoS a v dolní polovině druhý scénář s podporou QoS. Na první pohled je zřejmé, že síť s podporou QoS dosahuje nižších špičkových hodnot jitteru a je tedy spolehlivější.



Obr. 20 Statistika MOS

Z hodnot vyčtených ze statistiky v obrázku 20 je možné vidět, jak klesá parametr MOS Na síti s podporou QoS je vidět jeho pozvolnější klesání, avšak na konci simulace jsou již obě sítě tak zatíženy, že parametr MOS klesá k hodnotě 2, tedy již velmi špatnému zhodnocení hlasové komunikace. Ve druhém scénáři s podporou kvality služeb, je ale přeci jen vidět, že dosahuje lepších hodnot.

Hodnoty zpoždění linky jsou zobrazeny v obrázku 21 níže. Hodnota zpoždění hlasové aplikace postupně roste až do hodnoty přibližně 240ms. Tato hodnota je dle Tab. 3 již na hranici mezi přijatelnou a znehodnocenou komunikací, i proto tedy v závěru simulace klesá MOS faktor k hodnotě 2.

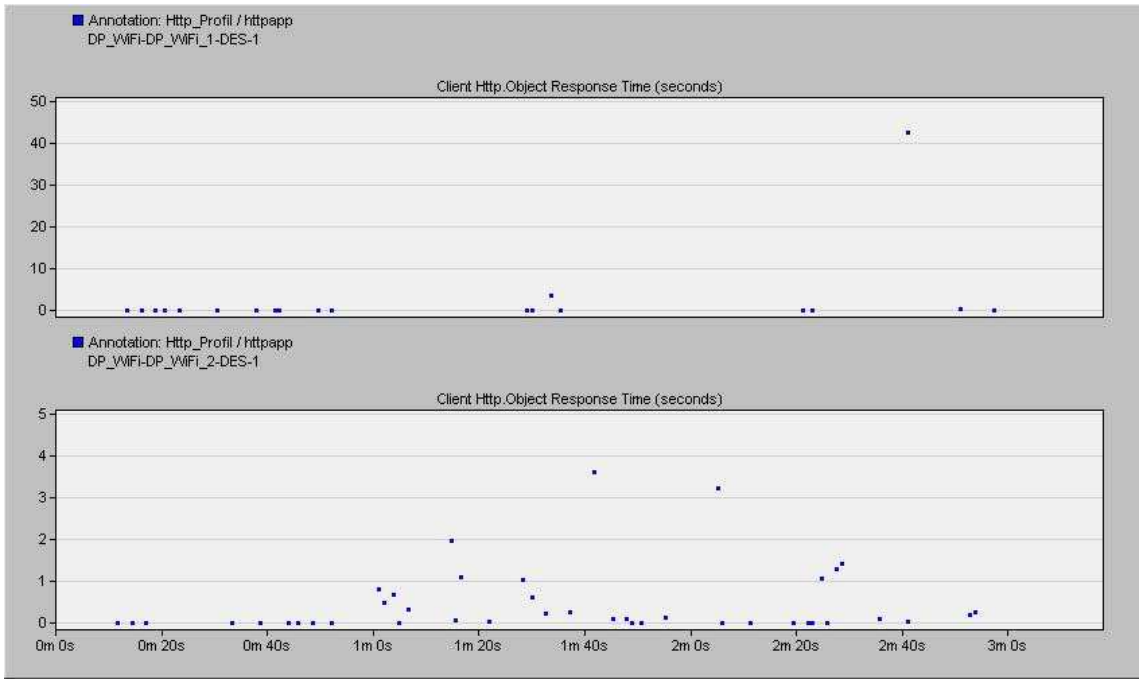


Obr. 21 Statistika zpoždění

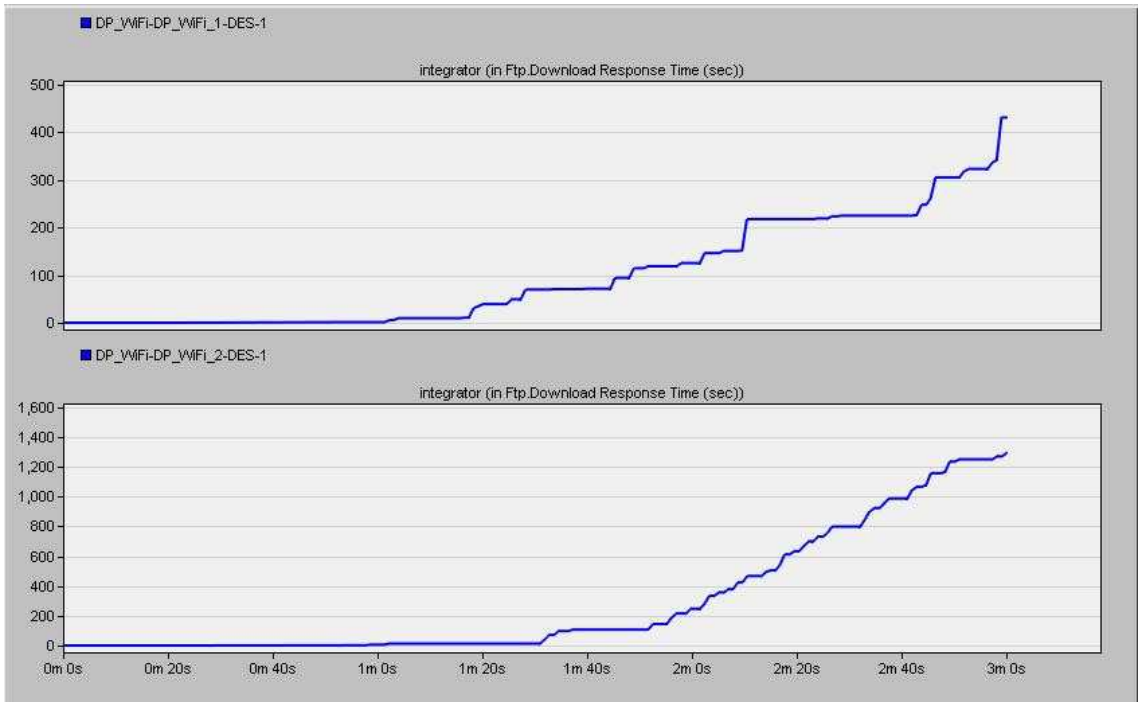
3.3.3 Statistika datových služeb

Služby FTP a HTTP byly také vysokým provozem na síti ovlivněny. Jelikož interaktivní přenosy mají před těmito aplikacemi podle nastavení v QoS přednost, tak se dalo předpokládat, že při použití algoritmů zajišťujících kvalitu služeb, dojde k zhoršení přenosových statistik právě na těchto službách, na úkor zvuku a videa.

Na obrázku 22 je patrné pozorovat jen drobný rozdíl v odpovědí Http_Serveru na požadavky Http_Klienta. V horní části je opět scénář bez QoS a v dolní s použití kvality služeb. Výrazné zhoršení parametrů je ale možné pozorovat u aplikace FTP na obrázku 23. Při výrazném vytížené po druhé minutě simulace došlo k výraznému nárůstu v času odpovědí v průměru až 2,5 krát oproti síti bez použití QoS. V reálném prostředí FTP klientovi ale vůbec nevadí, stáhne-li si soubor ze serveru o jednu sekundu později. Zde je důležité především to, aby byl soubor správně doručen. I proto se pro aplikace FTP volí třída Best Effort. Data jsou tak doručena za „každou cenu“ i za cenu vytvoření dodatečného zpoždění.



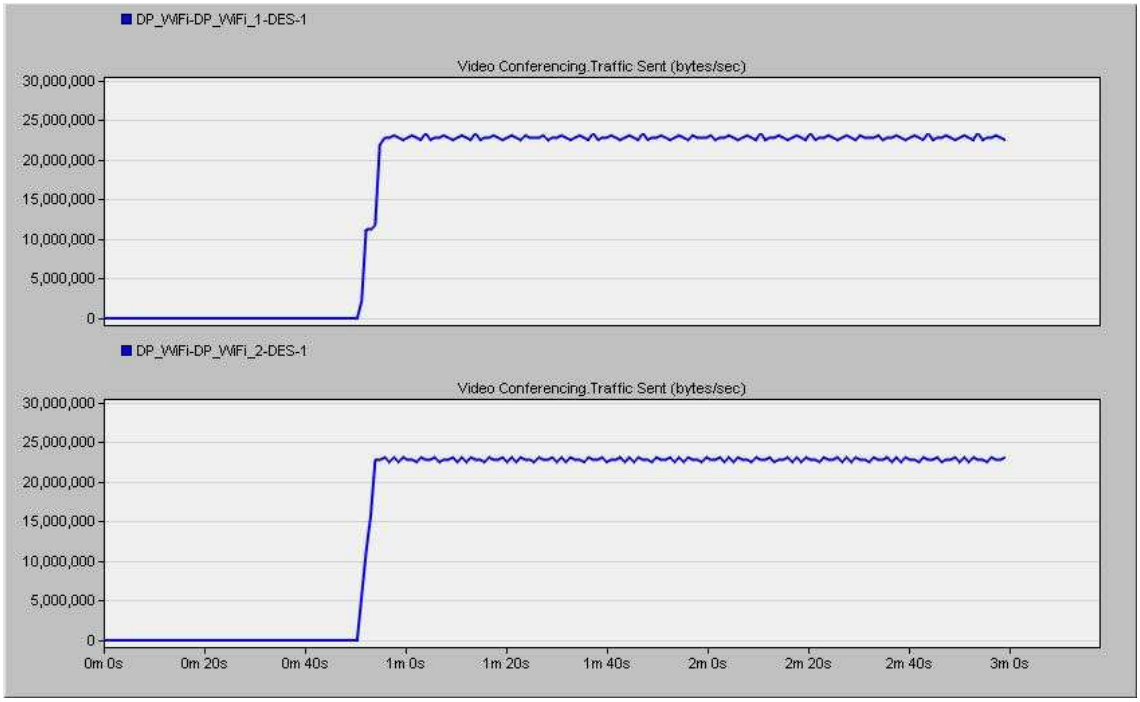
Obr. 22 Odpovědi Web Serveru



Obr. 23 Odpovědi FTP Serveru

3.3.4 Statistika Video přenosu

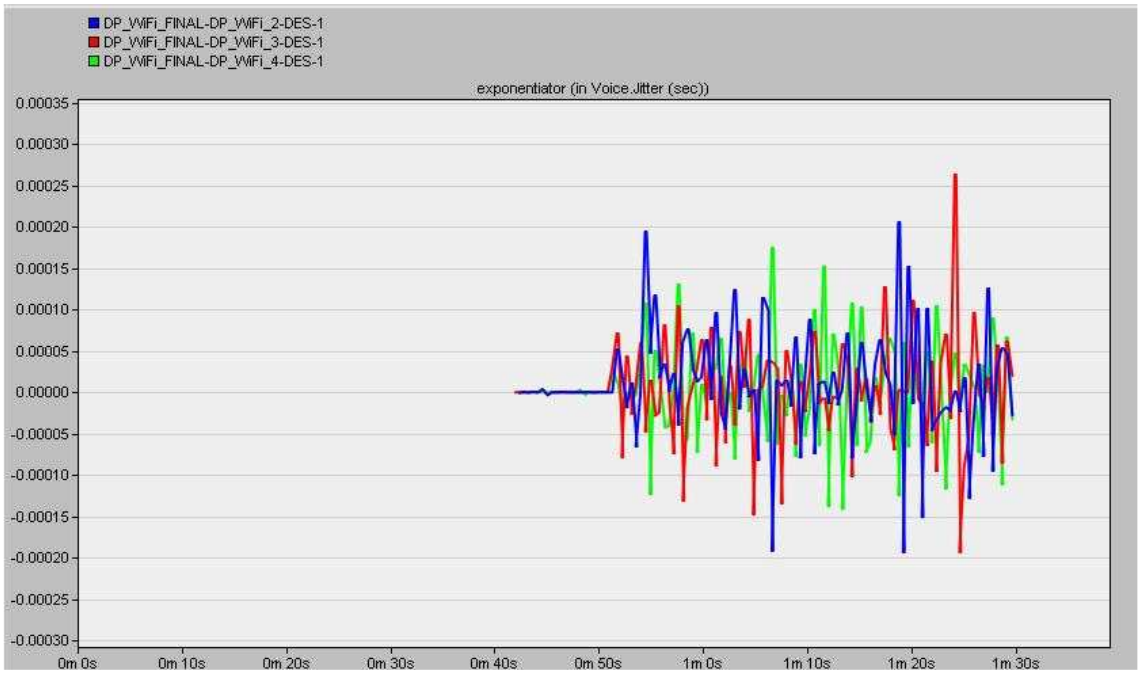
OPNET Modeler neumožňoval sběr velmi relevantních dat pro Video přenosy. Proto je zde uvedeno jen na obrázku 24, jak vypadala zátěž posílaná přes Video aplikaci. V obou scénářích se jedná o masivní tok dat, který právě způsoboval na síti zpoždění a ztrátovost a ovlivnil tak ostatní aplikace popsané v kapitolách 3.3.2 s 3.3.3.



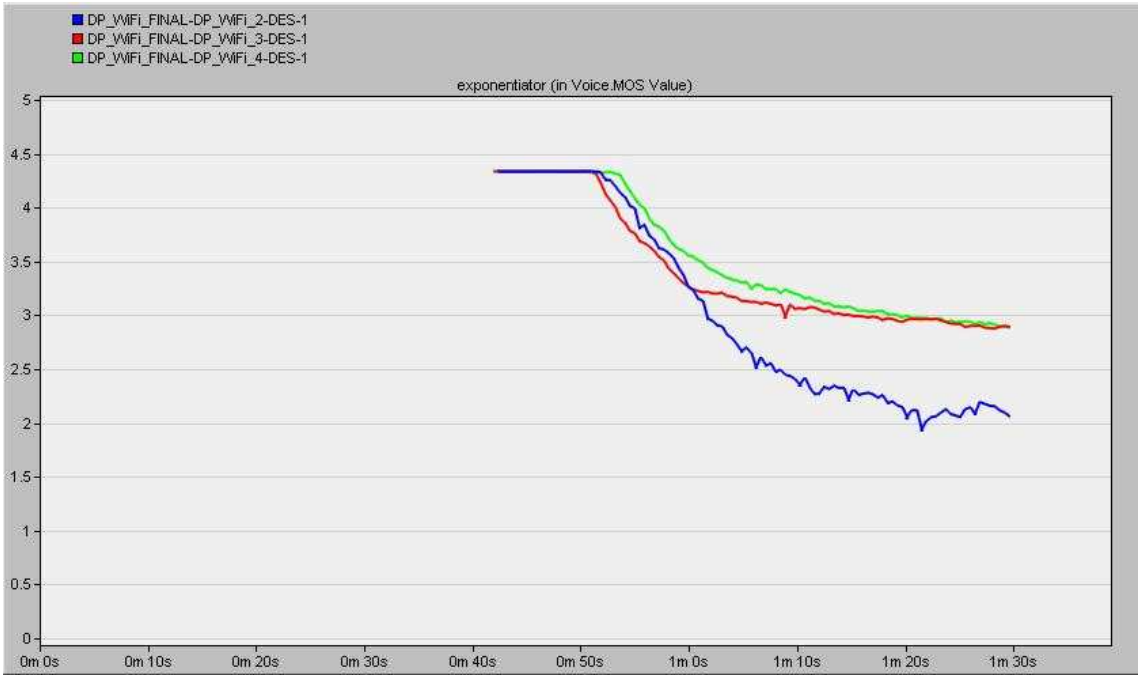
Obr. 24 Video posílané po síti

3.3.5 Srovnání výsledků simulace standardů 802.11

Na závěr jsou srovnány výsledky měření standardů sítě využívající 802.11a v 5 GHz licenčním pásu a 802.11n jako rozšíření 2,4 GHz pásma se standardem 802.11g. Ve všech měřeních, ke kterým docházelo v kapitolách 3.3.1 - 3.3.4 dosahovali standardy 802.11a a 802.11n lepších výsledků. Celkově nejlépe obstál standard 802.11n, který prokázal nejnižší míru zpoždění a MOS faktor při měření neklesl pod hodnotu 3. Jitter byl u všech třech typů bezdrátových sítí přibližně stejný. Na obrázku 25 je srovnání všech standardů z hlediska Jitteru a na obrázku 26 poté z hlediska MOS.



Obr. 25 Srovnání Jitteru mezi standardy



Obr. 26 Srovnání MOS mezi standardy

ZÁVĚR

V diplomové práci byly popsány principy bezdrátové sítě na standardu IEEE 802.11 se zaměřením na kvalitu služeb popisovanou ve standardu 802.11e. Dále byly prezentovány protokoly transportní a aplikační vrstvy sloužící k přenosu dat v reálném čase a další relevantní síťové komponenty k popsání přenosu interaktivních dat po internetu.

V druhé kapitole byla vytvořena testovací síť v laboratoři VUT za účelem proměření objektivní parametrů sítě, ovlivňujících kvalitu služeb v multimediálních přenosech. Nejdříve byl analyzován provoz na SIP protokolu zajišťujícím řízení VoIP hovorů. Dále byl pomocí měřicího přístroje VePal BX100V+ změřen MOS faktor, který popisuje právě kvalitu hovoru na VoIP službách. Pomocí emulátoru WANem byly postupně měněny parametry ovlivňující kvalitu služeb – šířka pásma, ztrátovost, zpoždění a jitter. Následně byly zaznamenány výsledky měření do přehledných tabulek a grafů. Měření bylo ovlivněno použitý přístrojem a zvolenou metodou, ale v určitých oblastech dosahovalo předpokládaných výsledků. S rostoucími hodnotami zpoždění, jitteru a ztrátovosti klesal MOS faktor. Při snížení šířky pásma pod mez používanou daným audio kodekem došlo také k výraznému zhoršení faktoru MOS.

Poslední část byla věnována vytvoření komplexního modelu sítě v prostředí OPNET Modeler verze 16.1. Toto simulační prostředí umožňuje otestovat parametry bezdrátových sítí. Byla vytvořena síť s bezdrátovým přístupovým bodem, čtyřmi bezdrátovými stanicemi a čtyřmi servery, na které se bezdrátové stanice připojují prostřednictvím přístupového bodu. Síť byla navrhnuta podle zjednodušeného modelu tak, aby připomínala strukturu malé kanceláře, kde se používají aplikace FTP, HTTP, VoIP a přenos Videa. HTTP server byl v modelu umístěn tak aby simuloval vzdálený Web Server.

Výsledné simulace dokázaly předpoklady, že použití algoritmů zajišťujících kvalitu služeb v bezdrátových sítích výrazně pozitivně ovlivní přenos dat po dané síti. Byl vytvořen srovnávací scénář DP_WiFi_1 bez použití algoritmů zajišťujících QoS a dále scénář DP_WiFi_2, kde bylo užito HCF, hybridní koordinační funkce a rozdělení

jednotlivých aplikací do tříd. Pro FTP přenos byla dle doporučení použita třída Best Effort, pro HTTP přenosy třída Background, pro hlasové služby třída Interactive Voice a pro video přenos třída Interactive Video.

Zavedení QoS mělo za následek snížení celkového zpoždění na síti a zejména zlepšení parametrů kvality služeb pro VoIP. Jitter dosahoval nižších špičkových hodnot a MOS faktor s rostoucí zátěží klesal pomaleji. Přenosy aplikacemi využívajícími FTP a HTTP byli ovlivněny negativně, dle předpokladu byli totiž upřednostněni přenosy s vyšší prioritou. Klienti využívající FTP a HTTP však nebyli nějak výrazně omezeni. Video přenos v prostředí OPNET Modeler nenabízel mnoho statistik k porovnání, avšak jeho velký objem přenesených dat způsoboval na síti právě zhoršení parametrů, především zpoždění.

Na závěr byly srovnány standardy 802.11a a 802.11n se standardem 802.11g. OPNET Modeler nepodporoval na směrovačích nastavení standardu 802.11b. Ve všech měřeních dosahovali standardy 802.11a a 802.11n lepších výsledků. Nejlepší QoS prokázal standard 802.11n, který měl nejnižší míru zpoždění, kdy MOS faktor při měření neklesl pod hodnotu 3.

LITERATURA

[1] Bigelow, S. J. *Mistrovství v počítačových sítích*. Nakladatelství CPRESS, 2004. ISBN 80-251-0178-9.

[2] Matas, J. *Linux jako brána do sítě Internet*. [Bakalářská práce]. Ústav Telekomunikací FEKT VUT v Brně. 2007.

[3] BARKEN, Lee. *Wi-Fi : jak zabezpečit bezdrátovou síť*. 1. vyd. Brno : Computer Press, 2004. 174 s. ISBN 80-251-0346-3.

[4] ZANDL, Patrick. *Bezdrátové sítě WiFi*. 2003. 204 s. ISBN 80-722-6632.

[5] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS.* 3. vyd. Praha: Computer Press, 2002. 542 s. ISBN 80-7226-675-6.

[6] KOVÁŘ Petr, MOLNÁR Karol, NOVOTNÝ Vít. *Současnost a budoucnost VoIP sítí*. Elektrorevue - časopis pro elektrotechniku. 1999- . roč. 8, č. 10, ISSN 1213-1539

[7] GAST, M. 2005. *802.11® Wireless Networks The Definitive Guide.* New York: O'Reilly, 2005. ISBN 0-596-10052-3.

[8] PRASAD R. Anand, PRASAD R. Neeli, *802.11 WLANs and IP Networking: Security, QOS, and Mobility*, 2005, ISBN 1-58053-789-8

[9] OPNET Technologies, *OPNET Modeler, General Tutorials*, součást instalace simulačního prostředí OPNET Modeler, 2009

[10] PUŽMANOVÁ, R. 2006. *Moderní komunikační sítě od A do Z.* 2 aktualizované vydání. Brno: Computer Press a.s, 2006. ISBN 80-251-1278-0.

SEZNAM ZKRATEK

AIFS – Arbitration Inter Frame Sparing
CAP - Controlled Access Phase
DCF - Distributed coordination function
EDCA - Enhanced distributed channel access
HCCA - HCF Controlled Channel Access
HCF – Hybrid Coordination Function
IEEE - Institute of Electrical and Electronics Engineers
IP – Internet Protocol
ISO/OSI - Internation Standard Organization/Open System Interconnection
MAC - Media Access Kontrol
MIMO – Multiple Input Multiple Output
MOS - Mean opinion score
MSS - Maximum Segment Size
MTU - Maximum transmission unit
PCF - Point coordination function
QoS – Quality of Service
RTP - Real-time Transport Protocol
RTPC – RTP Control Protocol
RTSP - Real Time Streaming Protocol
SIP - Session Initiation Protocol
TCP - Transmission Control Protocol
TKIP - Temporal Key Integrity Protocol
UDP - User Datagram Protocol
WAN – Wide Area Network
WiFi - Wireless Fidelity
WLAN - Wireless Local Area Network
WME - Wireless Media Extension

PŘÍLOHY

Projekt DP-WiFi, návrh sítě v programu OPNET Modeler.

Kompatibilní pouze s verzí 16.1.

Na přiloženém CD/DVD.