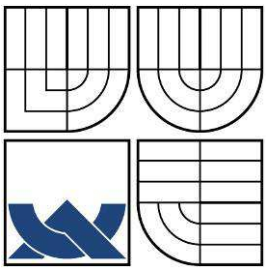
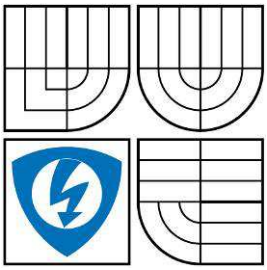


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATION

OPTIMALIZACE A ANALÝZA ZÁVISLOSTÍ KOMUNIKAČNÍCH SLUŽEB NA ZPOŽDĚNÍ

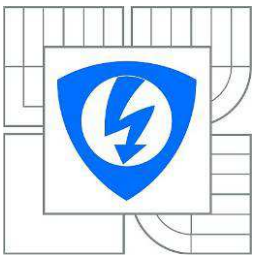
OPTIMALIZATION AND ANALYSIS OF COMMUNICATION SERVICES LATENCY DEPENDENCIES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — BC. LUKÁŠ ZIKMUND
AUTHOR

VEDOUCÍ PRÁCE — ING. PAVEL ENDRLE
SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor

Telekomunikační a informační technika

Student: Bc. Lukáš Zikmund ***ID:*** 71986

Ročník: 2 ***Akademický rok:*** 2013/2014

NÁZEV TÉMATU:

Optimalizace a analýza závislostí komunikačních služeb na zpoždění

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. Seznamte se simulačním prostředím Opnet Modeler. V tomto prostředí vytvořte bezdrátovou lokální síť, ve které nakonfigurujete mechanismy pro zajištění kvality služeb daných standardů. Vytvořte simulaci porovnávající technologie 802.11a/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.

Termín zadání: 10. 2. 2014 ***Termín odevzdání:*** 28. 5. 2014

Vedoucí práce: Ing. Pavel Endrle

Konzultanti diplomové práce:

doc. Ing. Jiří Mišurec, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

ANOTACE

Tato diplomová práce je zaměřena na zajištění kvality služeb (QoS) v bezdrátových sítích pro standardy IEEE 802.11 a/b/g/n. První část práce je zaměřena na teoretické pozadí této problematiky. Jsou zde popsány způsoby přenosu dat počítačovou sítí a jednotlivé parametry přenosu, především na parametry nutné pro zajištění kvality služeb (QoS). Dále jsou zde popsány jednotlivé standardy pro přenos dat bezdrátovou sítí a nakonec pak protokoly zajišťující přenos dat v reálném čase. Druhá část práce se pak věnuje simulačnímu prostředí OPNET modeler a simulacím vytvořených v tomto prostředí. Simulace jsou zaměřeny na přenos dat v reálném čase a porovnávají jednotlivé standardy z hlediska zpoždění a jeho kolísání.

Klíčová slova: Kvalita služeb, zpoždění, kolísání zpoždění, ztrátovost, IEEE 802.11 a/b/g/n,

ABSTRACT

This master's thesis is focused on ensuring of Quality of Service (QoS) in wireless network for standards IEEE 802.11 a/b/g/n. First part of this thesis is focused on the theory of this issue. It covers methods of data transfer in computer networks and individual transfer parameters especially on parameters needed to ensure quality of service. It also describes standards for wireless data transmission and protocols for real time data transmission. The second part is devoted to OPNET modeler and to simulations created on this program. Simulations are focused on real-time data transfer and compare the standards in terms of delay and jitter.

Keywords: Quality of Service, latency, jitter, packet loss, IEEE 802.11 a/b/g/n

BIBLIOGRAFICKÁ CITACE:

ZIKMUND, L. *Optimalizace a analýza závislostí komunikačních služeb na zpoždění*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2014. 56 s. Vedoucí diplomové práce Ing. Pavel Endrle.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma Optimalizace a analýza závislostí komunikačních služeb na zpoždění 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 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 následku porušení ustanovení $ 11 a následujících autorského 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 IV. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....
podpis autora

Poděkování

Děkuji vedoucímu práce Ing. Pavlu Endrlemu za velmi užitečnou metodickou a odbornou pomoc a další cenné rady při zpracování diplomové práce

V Brně dne ....
podpis autora

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.

V Brně dne . . . .

podpis autora

Obsah:

Úvod

V dnešní době si život bez komunikačních služeb již nedovedeme představit. Kdo není permanentně připojen k internetu, jako by snad ani neexistoval. Není to přitom ještě tak dávno, kdy byl internet v domácnosti poměrně vzácnou věcí, připojení bylo realizováno pomocí vytáčeného připojení, rychlosti dosahovaly maximálně několik desítek Kbit/s a cena se odvíjela od doby připojení.

Postupem času vznikaly další technologie umožňující trvalé připojení s mnohem vyššími rychlostmi, poplatky se paušalizovaly a poskytovatelé se začali předhánět s garantovanou rychlostí připojení. Mimo města, kde nebyla tak vyvinutá komunikační infrastruktura, se začalo prosazovat bezdrátové připojení pomocí WiFi. S rostoucími rychlostmi a vyšší stabilitou připojení se začaly zavádět i nové komunikační služby jako například streamování hudby a videa, internetová telefonie atd.

S nárůstem těchto služeb a s neustále rostoucími objemy dat, které proudily sítí, bylo třeba tento provoz nějakým způsobem řídit tak, aby nedocházelo k výpadkům právě během například přehrávání videa či hovoru přes počítačovou síť, kde je kladen mnohem větší důraz na zpoždění než u obyčejného stahování. Bylo třeba zajistit, aby provoz právě pro tyto služby byl upřednostňován před ostatním provozem, který není tak náchylný na čas doručení.

Vznikly tak nové mechanizmy na řízení provozu v počítačových sítích, kde je veškerý provoz zařazen do několika kategorií a každá kategorie vyžaduje určité parametry, které jsou pro ni více či méně důležité. Jednotlivé kategorie jsou pak v závislosti na důležitosti jednotlivých parametrů upřednostňovány před ostatním provozem, který by jinak dosažení těchto parametrů bránil.

V bezdrátových sítích jsou komplikace se zajištěním kvality služby o to horší, že přenosovým médiem není metalický či optický kabel, ale vzduch, který vykazuje mnohem horší přenosové vlastnosti. Přenos vzduchem je silně závislý na síle a kvalitě signálu, které se mohou během přenosu velmi měnit, umožňuje nižší přenosovou rychlost, přenos má větší problémy se zpožděním i s jeho kolísáním. Umožňuje však větší mobilitu a tím i větší pohodlí pro uživatele, a je tak stále oblíbenější. Úkolem tak je zajistit požadovanou kvalitu služeb podobnou kvalitě dosahované při použití kabelových rozvodů.

1 Přenos dat

Pro přenos dat mezi jejich zdrojem a cílem existuje několik způsobů přenosu. Každý způsob přenosu má své specifické vlastnosti, které se hodí pro přenos různých typů dat. Pro přenos hovorového signálu je potřeba zajistit trvalé spojení, aby byl řečový signál plynule odesílán a do svého cíle dorazil přesně v tom pořadí, v jakém byl odeslán. Drobné výpadky signálu během spojení nevytváří až takový problém. Při přenosu dat mezi počítači, kde komunikace probíhá v určitých dávkách, není naopak zpoždění signálu tak kriticky důležité, vzniká zde tak prostor pro kontrolu správnosti doručení, neboť vyžadujeme naprostou spolehlivost přenosu. Z těchto důvodů existuje několik způsobů komunikace.[6]

1.1 Způsoby přenosu informace

Spojování okruhů

Tento způsob komunikace je vhodný především pro přenos informací v reálném čase nebo u telefonních hovorů. Vykazuje totiž minimální a téměř stejné zpoždění přenosu informací.

Pro každé spojení je před vlastním přenosem dat vytvořen okruh (obousměrný komunikační kanál), který slouží pro přenos dat pouze daného spojení a je vyhrazen po celou dobu komunikace. Nezáleží tak, jestli dochází k přenosu informací, ale okruh je rezervován, dokud není spojení ukončeno. Tento způsob přenášení informací je poměrně neefektivní, protože parametry spojení, dohodnuté při jeho vzniku, jsou během celého spojení neměnné a síť tak není schopna pružně reagovat na změny v síti. Okamžiky, kdy žádné informace kanálem neprobíhají, by tak mohly být využity pro jiný přenos dat. [6][10]

Spojování zpráv

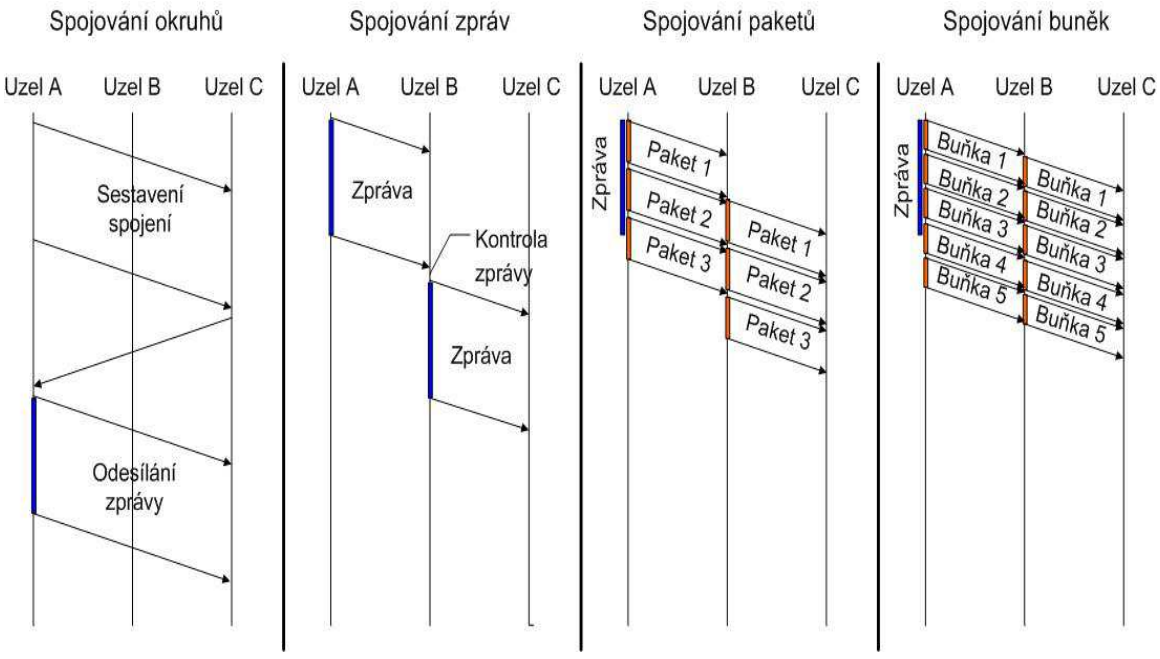
U tohoto typu komunikace se nevytváří pevné spojení mezi odesílatelem a příjemcem zpráv, ale jednotlivé zprávy jsou jedna po druhé odesílány na mezilehlé uzly, kde jsou zprávy přijaty, zkontrolovány a poté odeslány dalšímu uzlu směrem k příjemci dat. Tento způsob komunikace mnohem efektivněji využívá přenosový kanál a využívá pouze tu část sítě, kterou se daná zpráva přenáší. Klade však velké nároky na mezilehlé uzly, které musejí uchovávat a zpracovávat velké množství informací. Musí být schopny provést kontrolu jednotlivých zpráv, zda přišly v pořádku, a znovu je odeslat.

Spojování paketů

Tento způsob přenosu informací je v současné době nejpoužívanějším typem přenosu v datových sítích. Pracuje na podobném principu jako spojování zpráv, avšak s tím rozdílem, že jednotlivé zprávy jsou rozděleny na menší datové jednotky – pakety, které mají přesně definovanou délku. Ty jsou pak přenášeny stejným způsobem jako v případě spojování zpráv. Nevýhodou tohoto řešení je, že jednotlivé pakety mohou být doručeny v nesprávném pořadí, a je tak třeba využívat další mechanizmy, které jsou schopny zajistit správné pořadí jednotlivých paketů.

Spojování buněk

Při přenosu dat, které využívá spojování buněk, jsou jednotlivé datové zprávy rozděleny na buňky s pevně danou velikostí. Přenos probíhá podobně jako v případě spojování zpráv či paketů s tím rozdílem, že na každém uzlu nejsou kontrolovány celé zprávy, ale pouze jejich hlavičky a kontrola zprávy závisí na konkrétním uživateli. Dochází tím k výraznému urychlení kontroly jednotlivých buněk a tím i k rychlejšímu přenosu zpráv danou sítí. [6][10]



Obr. 1: Porovnání jednotlivých typů přenosu dat

Na obr. 1 je znázorněno porovnání jednotlivých typů přenosu dat. Komunikace probíhá z Uzlu A do uzlu C. Uzel B představuje mezilehlý uzel, přes který musí data projít a je zde vidět zpoždění při jednotlivých způsobech předávání dat. Z obrázku je

patrné větší zpoždění při komunikaci pomocí spojování okruhů, kdy je na počátku přenosu nutné sestavit spojení. Jako nejrychlejší způsob komunikace se jeví spojování buněk, kdy jsou na mezilehlém Uzlu B kontrolovány pouze hlavičky jednotlivých buněk.

1.2 Parametry přenosu dat

Mezi základní parametry přenosu dat, s jejichž pomocí lze porovnávat přenosové vlastnosti jednotlivých sítí a sledovat kvalitu služeb, kterou je síť schopna poskytnout, patří zpoždění, kolísání zpoždění, ztrátovost a šířka pásma (propustnost). Jednotlivé parametry jsou více či méně důležité pro různé typy přenášených dat. Pro aplikace pracující v reálném čase, jejichž typickým zástupcem je IP telefonie, je velmi důležité zpoždění a jeho kolísání. Naopak pro aplikace vyžadující pouze velké datové přesuny je mnohem důležitější vysoká propustnost sítě a malá ztrátovost paketů. Zpoždění několik stovek milisekund zde tedy nehraje tak důležitou roli. [9]

Zpoždění

Zpoždění (latency) udává celkový čas potřebný k přenosu informace z jednoho koncového zařízení na druhé. Je závislé na mnoha parametrech, zejména na délce trasy (rychlost šíření signálu prostředím je limitována), na velikosti dané zprávy, šířce pásma přenosového kanálu a také na zatížení trasy.

Vliv těchto parametrů se liší v závislosti na velikosti zprávy. Budeme-li přenášet pouze krátkou zprávu (několik bitů), hraje největší roli délka trasy. Šířka pásma v tomto případě není tak důležité, protože doba vysílání zprávy je velmi krátká. Naopak při přenosu většího množství dat, je třeba se zaměřit hlavně na šířku pásma, protože zpoždění po trase již nehraje takovou roli

Dalším důležitým faktorem při posuzování přenosu dat, který je třeba zohlednit, je rovněž výkon aktivních prvků v síti. Čím je prvek výkonnější, tím se zmenšuje zpoždění ve frontě na odbavení i zpoždění při přepínání v síti. [2][6]

Kolísání zpoždění

Kolísání zpoždění (změny ve zpoždění) udává rozdíly ve zpoždění příchodu jednotlivých zpráv. Vzniká díky rozdílům v délkách front u jednotlivých zařízení v síti. Dalším důvodem ke vzniku zpoždění je fakt, že jednotlivé zprávy se nemusejí sítí šířit stejnou trasou, ale mohou být směrovány různými směry skrz celou síť. Dochází tak

k tomu, že vzdálenost, kterou musí jednotlivé zprávy urazit, je různá. Díky tomu je odlišné i trvání přenosu jednotlivých zpráv. Může se tak stát, že zprávy dojdou do síle zpřeházené, a jsou potom zapotřebí mechanizmy k jejich správnému seřazení. I tento proces může zvětšovat rozdíly v čase doručení informací, tedy ke zvětšení kolísání zpoždění. [3][6][8][10]

Šířka pásma

Šířka pásma je v souvislosti s počítačovými sítěmi poněkud zavádějící označení, které vychází z teorie radiového přenosu. Tento termín označuje maximální teoreticky dosažitelnou přenosovou rychlost uváděnou v bitech za sekundu. Udává tedy, kolik bitů (v dnešní době se pohybujeme většinou v řádu megabitů či gigabitů) je možné daným kanálem přenést za jednu sekundu. Tato hodnota je pouze teoretická a v praktickém světě ji nelze dosáhnout. Reálná hodnota je obvykle označována jako propustnost. Ta v sobě již zahrnuje naměřenou skutečnost v reálném provozu. Z reálné propustnosti pak vyplývá i charakter komunikace, formát zpráv nebo konstrukce a vytížení prvků po trase přenosu. [6]

Ztrátovost

Ztrátovost udává, kolik procent zpráv z celkového vyslaného množství je nedorazilo do cíle. Ke ztrátě zpráv může dojít jak z důvodu přetížení linek, zahlcení směrovačů a tím jejich neschopnost obsloužit v jeden okamžik velké množství zpráv, tak i z důvodu vzniku chyb během přenosu. U aplikací využívajících spolehlivou službu dojde při ztrátě zpráv k jejich opakovanému přenosu a zvyšuje se tak pouze zpoždění. Avšak u aplikací využívajících nespolehlivou službu, kde chybí mechanizmus pro kontrolu správnosti doručení, dochází k nenávratné ztrátě zpráv. U aplikací pracujících v reálném čase je však určitá ztrátovost tolerována, na rozdíl od zpoždění, na které jsou kladeny přísné nároky. [3][6]

2 Bezdrátové sítě

Bezdrátové sítě, označované jako WiFi, vznikly jako alternativa k běžným drátovým sítím. Signál se volně šíří vzduchem a ke svému šíření využívá bezlicenční frekvenční pásmo, čímž odpadá jakákoli starost s umístěním kabelů i s případnou licencí k vysílání signálu. Další výhodou této možnosti je jednoduchá instalace a velká mobilita koncových stanic. Naproti tomu hlavní nevýhodou je nižší přenosová rychlost, delší doba odezvy, vyšší rušení přenosovým médiem (vzduch) a nižší bezpečnost přenosu dat.

Přesto, že je tato technologie alternativou k běžným sítím, nejsou zde aplikovatelné všechny metody zajišťující přenos dat. Klasický ethernet používá jako přístup k médiu protokol CSMA/CD (Carrier Sense Multiple Access with Collision Detection), kdy stanice během svého vysílání současně kontroluje i přenosové médium, zda nezachytí jiné vysílání, které by kolidovalo s jejím. Pokud stanice zjistí kolizi, zastaví vysílání, počká náhodnou dobu a opakuje svůj pokus znovu.

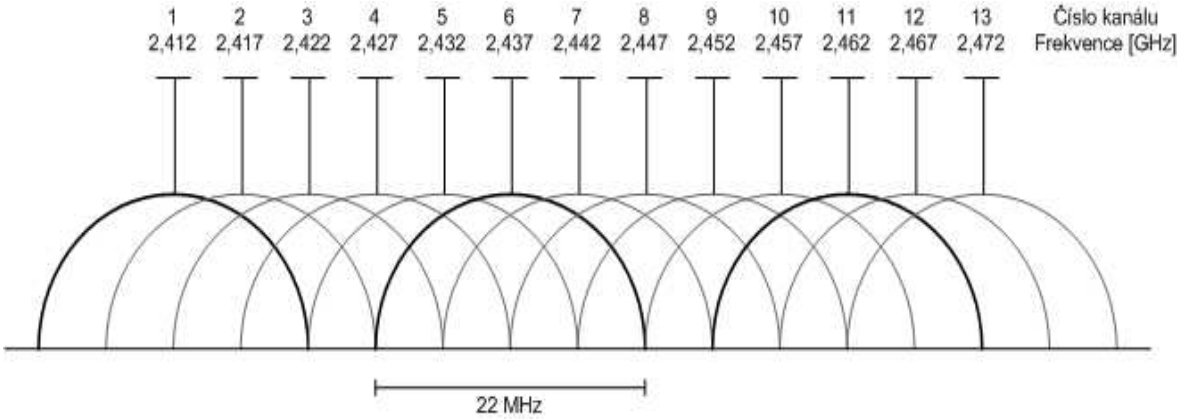
V bezdrátových sítích však nelze kontrolovat přístupové médium. Byla proto zvolena metoda CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), která má za úkol kolizím předcházet. Proces komunikace je tak zahájen vysláním rámce z přístupového bodu. Ten se postupně dotazuje stanic, jestli mají data k vysílání. V případě, že dotázaná stanice má data k vysílání, pošle datový rámec jako odpověď. V opačném případě odpoví prázdným rámcem. [8]

2.1 Standard 802.11

V roce 1997 byl mezinárodní organizací IEEE definován základní standard 802.11, který používal bezlicenční pásmo 2,4 GHz. Používal modulační techniky FHSS a DSSS a přenosová rychlost byla 1 a 2 Mbit/s. Pro všechny WLAN totiž platí, že se přenosová rychlost na fyzické vrstvě podle situace mění: snižuje se s růstem chybovosti nebo zvyšuje při zlepšení podmínek prostředí, takže maximální rychlost jednotlivých WLAN lze předpokládat pouze na krátkou vzdálenost a v prostředí bez rušivých vlivů na přenos.

Pro techniku FHSS (Frequency hopping spread spectrum) je pásmo rozděleno na 79 kanálů o šířce 1 MHz. Pro tuto techniku je charakteristické přeskakování mezi několika frekvencemi při přenosu bitu nebo bitů. Obě komunikující strany se tedy domluví na sekvenci přeskakování. V závislosti na síle signálu, je použita modulace 2-GFSK, která dosahuje maximální přenosové rychlosti 1Mbit/s, nebo 4-GFSK. Ta dosahuje maximální přenosové rychlosti 2Mbit/s.

Pokud je použita technika DSSS (Direct sequence spread spektrum), je signál rozprostřen do větší části radiového spektra. Výhodou je, že je méně citlivý vůči rušení. Pásmo je rozděleno do 14 kanálů, které se vzájemně částečně překrývají. Jejich šířka je 22 MHz. Používá se buď modulace DBPSK, dosahující maximální přenosové rychlosti 1Mbit/s nebo DQPSK, která dosahuje rychlosti 2Mbit/s. [8][13]



Obr. 2: Rozdělení kanálů WiFi v pásmu 2,4 GHz

2.2 Standard 802.11b

Tento standard byl schválen v roce 1999 jako doplněk předchozího standardu 802.11 a maximální přenosová rychlost byla navýšena na 11 Mbit/s. Využívá stejně jako původní 802.11 frekvenční pásmo 2,4 GHz i stejné modulační techniky FHSS a DSSS. Pro FHSS se využívá dvou- a čtyřstavová modulace GFSK a přenosové rychlosti dosahují 1,6 Mbit/s (dvoustavová) a 3,2 Mbit/s (čtyřstavová GFSK).

Pro DSSS se opět využívá modulace DBPSK a DQPSK a dosahují maximální teoretické přenosové rychlosti 1, 2, 5,5 a 11 Mbit/s. Tyto rychlosti jsou dosaženy i díky použití doplňkového klíčového kódování (CCK – Complementary code keying). CCK mapuje čtyři bity na symbol (na 8 Mbit/s) a současně mírně zvyšuje symbolovou rychlost, čímž se dosáhne na fyzické vrstvě maximální rychlosti 11 Mbit/s. [8][10]

2.3 Standard 802.11a

Tento standard byl schválen rovněž v roce 1999, stejně jako standard 902.11b, má však řadu odlišností. Frekvenční pásmo bylo změněno z 2,4 GHz na 5 GHz, čímž se vyřešil problém s vysokým zarušením právě pásma kolem 2,4 GHz, které využívá mnoho jiných bezdrátových technologií jako například Bluetooth nebo Zigbee. Velké problémy mohou vznikat i díky mikrovlným troubám, které rovněž vysílají na frekvenci 2,4 GHz. Jako modulační technika se využívá OFDM (Orthogonal frequency division multiplex). Pásmo je rozděleno na 52 kanálů s šířkou pásma 20 MHz, ve kterých mohou být přenášeny zprávy. To umožňuje vytvořit až 13 vzájemně se nepřekrývajících kanálů (802.11b umožňuje pouze 3 vzájemně se nepřekrývající kanály). Maximální přenosová rychlost dosahuje 54 Mbit/s.

V Evropě je navíc povolena úprava 802.11h pro vnější použití. Jedná se o doplněk pro 8802.11a, který je navržen s ohledem na evropské podmínky, aby bylo možné sítě využívat mimo budovy a zároveň nebyly problémy s rušením od ostatních zařízení, pracujících na frekvenci 5 GHz. Na tomto pásmu pracují například radary nebo některé satelitní systémy. V podstatě mají bezdrátová zařízení, pokud detekovala rušení, omezit vysílací výkon nebo uvolnit kanál, na kterém toto rušení rozpoznaly. Kvůli svým specifickým nárokům však nebyla implemetována v žádném z běžně dostupných zařízení na trhu (bráno Cisco, Ubiquity, Mikrotik, Ovislink 2011) a dnes je i pro vnější podmínky využíváno zařízení 802.11a s omezeními proti rušení meteorologických radarů. [10][14]

2.4 Standard 802.11g

Tento standard vznikl v roce 2003 a vychází ze staršího standardu 802.11b. Pracuje na stejném frekvenčním pásmu 2,4 GHz, změněno však bylo kanálové kódování na OFDM. Maximální teoretická přenosová rychlost tak dosahuje 54Mbits. Velikou výhodou tohoto standardu je zachování zpětné kompatibility se starším standardem 802.11b.

Pro dosažení vyšší rychlosti se u 802.11g používá OFDM, kdy se data k vysílání nejprve rozdělí do několika paralelních toků bitů o mnohem nižší bitové rychlosti. Každý z toků se používá pro modulaci jiné nosné frekvence. Zatímco tradiční kmitočtový multiplex dělí kmitočtové pásmo do několika nepřekrývajících se kmitočtových kanálů vzájemně oddělených ochranným kmitočtovým pásmem, OFDM používá překrývající se kanály, takže kmitočtové pásmo se využívá účinněji.

Způsobem paralelního vysílání se OFDM účinně brání zkreslení při přenosu signálu různými cestami (multipath distortion). Každý přenášený symbol trvá na dílčí nosné déle, takže se prakticky vyloučí nepříznivý dopad zpoždění signálu delší cestou. Navíc se používá více úzkopásmových nosných a jejich vzájemné rušení ovlivní jen velmi malou část signálu.

Podporovaných rychlostí u 802.11g je víc než u 802.11b. Rychlosti podporované pomocí OFDM jsou, v závislosti na modulaci, 54, 48, 36 a 24 Mbit/s při použití 16-QAM, 18 a 12 Mbit/s při využití QPSK, 9 a 6 Mbit/s (BPSK). Další rychlosti jsou v souladu s 802.11b a vyžadují použití DSSS a CCK. [10][12][14]

2.5 Standard 802.11n

Tento WiFi standard byl navržen tak, aby dosahoval přenosové rychlosti větší než 100 Mbit/s. Zároveň se měl prodloužit dosah signálu pomocí zvýšení zisku zpracování.

Při vývoji 802.11n vznikly 2 konkurenční návrhy, které bylo třeba buď sjednotit, nebo rozhodnout, který z nich bude platit. Během procesu rozhodování se však objevila na trhu poptávka po zařízeních s vyšší kapacitou a výrobci potřebovali jistotu kompatibility s novým standardem. V rámci urychlení procesu bylo založeno bezdrátové konsorcium EWC (Enhanced Wireless Consortium), které prosazovalo vzájemnou kompatibilitu zařízení.

Aby se předešlo znejistění trhu, bylo zvoleno vícestupňové zavádění nového standardu a přijat tzv. Draft 1.0 – předstandard. Zařízení splňující tuto normu měla zaručeno, že budou schopna komunikace se stanicemi výsledné normy. Do dokončení standardizace byla vydána v roce 2007 ještě norma 802.11n Draft 2.0. K pevnému ustavení 802.11n došlo až v září 2009.

Norma zavádí nové rozšíření při přenosu dat a to technologii MIMO (Multiple Input – Multiple Output), která umožňuje navýšení rychlosti pomocí fázového posunu vysílání. MIMO totiž využívá fenoménu vícecestného šíření ke zvýšení propustnosti a dosahu nebo ke snížení počtu přenosových bitových chyb, místo snahy o eliminaci efektu vícecestné propagace, o kterou se snaží tradiční SISO (Single Input – Single Output). Odrazů, které předchozím standardům působilo problémy, je využito ke zvýšení přenosové rychlosti. [14]

3 Kvalita služeb (QoS)

V normální jednoduché síti se všichni její členové dělí o prostředky sítě stejným dílem. Jednoduchý příklad: Pokud bychom měli linku s kapacitou 100Mbit/s a po této lince by přenášelo 100 lidí data, každý by přenášel data rychlostí 1Mbit/s. To při obyčejném surfování na internetu, případně stahování emailů, není žádný problém. Tyto aplikace totiž pracují s jakoukoli šířkou pásma a uživateli stačí počkat, než se požadovaný objem dat stáhne. [11]

Existují však aplikace, které pro své fungování potřebují určitou šířku pásma, jinak jejich správné fungování není možné. Typickým příkladem jsou multimediální služby pracující v reálném čase, či o IP telefonii. Tyto služby mohou normálně fungovat, dokud není síť zatížená tak, že již pro datové přenosy nedostačuje šířka pásma

(více uživatelů začne stahovat). V tomto případě nebude daná aplikace dostávat dostatečné množství dat v čas a začne docházet k zasekávání nebo výpadkům obrazu či zvuku.

Aby k těmto problémům nedocházelo, vznikly mechanizmy, které jsou schopny datový provoz určitým způsobem rozeznat a určit, u kterých dat je důležité včasné doručení a u kterých doba doručení tolik důležitá není. Následně dochází k upřednostňování určitého datového toku před jiným například vyčleněním větší šířky pásma pro tento datový tok tak, aby byla zajištěna bezchybná funkčnost dané aplikace. Dojte tak k zajištění kvality služeb (Quality of service). [1]

Quality of Service (QoS) je tedy souhrnné označení pro řadu technologií a mechanizmů, které mají zajistit řízení síťového provozu a umožnit tak nastavení určité kvality přenosu pro data přenášená sítí. Dále umožňuje rozlišovat jednotlivé datové přenosy a každému nastavit jinou kvalitu služby, tedy rozlišit o jak moc důležitý provoz se jedná a následně určit, jak moc bude upřednostňován vůči ostatnímu provozu.

QoS se poslední dobou stává čím dál víc populární a to i díky čím dál rozšířenějšímu používání IP telefonie i online multimediálních služeb (IPTV, youtube apod.). Je tak třeba dbát na zajištění určitých vlastností provozu po síti.

QoS nástroje nejčastěji ovlivňují tyto kvalitativní parametry přenosu (v závorce jsou doporučené hodnoty pro VoIP, kterých by se mělo v praxi dosáhnout pro optimální nasazení IP telefonie):

- Šířka pásma – propustnost (12 – 106 Kbit/s v závislosti na vzorkování, kodeku a režii na druhé vrstvě ISO/OSI modelu)
- Zpoždění – doba mezi vysláním paketu a jeho doručením (< 150 ms)
- Kolísání zpoždění – rozdíl v intervalech mezi přijímanými pakety (< 30 ms)
- Ztrátovost paketů – podíl přijatých a vyslaných paketů za časovou jednotku (< 1%)

QoS však není jeden jednolitý nástroj pro řešení problémů se zajišťováním kvalitativních parametrů přenosu. Používá se celá řada QoS nástrojů a jejich názvy se mohou podle dodavatele lišit. Používají se nejen nad protokolem IP, ale i nad protokoly vyšších vrstev a je možné je rozdělit přibližně do následujících kategorií:

- Classification and marking - klasifikace resp. rozlišení a označení provozu
- Congestion management (Queuing) - správa zahlcení pomocí front
- Shaping and Policing - správa datového toku, omezování a vyhrazování

- Congestion avoidance - nástroje pro zabránění zahlcení, např. selektivním zahozením TCP paketu
- Link-efficiency - správa efektivního využití linky, obvykle se týká pomalých linek, komprese nebo fragmentace paketů
- Signaling (RSVP, QPPB)
- Ostatní

Je tedy zřejmé, že pokud potřebujeme zajistit určitou šířku pásma pro určitou aplikaci, případně preferovat některé datové toky před jinými, je vhodné použít nástroje QoS. Pokud se hovoří o QoS, je třeba si mimo jiné uvědomit, že se nástroje QoS používají pro rezervaci a řízení datových toků tak, aby nedošlo ke snížení kvality síťových služeb ve stavu zahlcení sítě nebo v situacích, kdy zahlcení sítě hrozí, ale ještě nenastalo. QoS se tedy uplatňuje ve chvíli, kdy je síť zahlcena, nebo téměř zahlcena. Jinak se QoS neuplatňuje a pakety plynule procházejí zařízením.

Další skutečností, kterou je nezbytné si uvědomit, pokud budeme chtít řešit problémy v síti pomocí QoS, je fakt, že mechanizmy QoS nejsou všespásné. Nastavení QoS nebude schopno vyřešit obecný nedostatek přenosové kapacity v síti nebo problémy v přenosové trase. Je pochopitelné, že nelze připojit společnost s tisíci zaměstnanci na linku o kapacitě 64 kb/s a je celkem lhostejné, zda s nasazeným QoS nebo bez QoS. Stejně tak ztrátovost paketů na lince, např. způsobená radiovým rušením Wi-Fi spoje, není možné vyřešit pomocí nástrojů QoS. [5]

Při implementaci QoS rozlišujeme tři třídy služeb:

- Garantované služby – jedná se o služby, které jsou dostupné v každý časový okamžik a zaručují doručení veškerých vyslaných dat.
- Služby s řízením zátěže – služby garantující průměrné zpoždění a doručení vysokého procenta přenášených dat. Nejedná se však o stoprocentní doručení, jak je tomu u služeb garantovaných
- Služby Best-effort – služby, které neposkytují žádnou garanci doručených dat

V sítích se v dnešní době používají především tři modely mechanizmů QoS. Jedná se o modely označované jako Best-effort services, Integrated services a Differential services. [3]

3.1 Best-effort services

Best-effort services, tedy metodu největší snahy, nelze tak úplně zařadit mezi metody zajišťující kvalitu služby. V tomto případě má každý datový tok nastavenu stejnou prioritu, tedy jinými slovy lze říct, že prioritizace provozu je vypnuta a není zde žádná garance dodržení kvality služby.

Jedná se o základní model přenosu dat a síť se tak snaží doručit všechny pakety v co nejkratším čase. Aplikace vysílají data kdykoliv se jim zachce, kolik chtějí, a bez vyžádání si jakéhokoli povolení. Síť se snaží přenést data co nejlépe, s co nejmenším zpožděním a snaží se o co nejmenší rozdíl v čase doručení. Snaží se o to i tehdy, když není možné data doručit, aniž by byl informován odesílatel nebo příjemce.

Pokud není zajištěn dostatek prostředků sítě, a dojde tak k jejímu přetížení, postupně se prodlužují vstupní a výstupní fronty a následně může dojít až k zahození paketů. Nerozlišuje přitom, jestli jde o přenos multimediálního toku nebo se jedná o obyčejné datové soubory. [3][7][8]

3.2 Integrated services

Integrated services (IntServ), česky integrované služby, se již snaží datový provoz nějakým způsobem řídit a zajistit tak určitou kvalitu požadovaných služeb v závislosti na právě dané službě.

Tento model pracuje tak, že aplikace oznámí síti své požadavky na přenos dat sítí. Počítačová síť zkontroluje, jestli jsou potřebné požadavky k dispozici a rozhodne, jestli je schopna jim vyhovět a jestli vytvoření nové rezervace neovlivní již dříve rezervované datové toky. Tato funkce je označována jako řízení přístupu (admission kontrol) a je jednou ze čtyř částí nutných k implementaci integrovaných služeb.

V případě, že síť požadavkům nevyhoví, není spojení povoleno a aplikace musí snížit své požadavky a znovu požádat síť o povolení přenosu dat. Tento proces se opakuje, dokud síť není schopna požadavkům vyhovět a nedojde k povolení přenosu dat.

V případě, že je požadavek k přenosu přijat, musí počítačová síť informovat všechny komponenty, přes které bude probíhat přenos, aby rezervovaly odpovídající objem prostředků, především šířku pásma mezi jednotlivými komponentami a kapacitu fronty paketů uvnitř jednotlivých zařízení. To zajišťují rezervační protokoly, v tomto

případě nejrozšířenější z nich – protokol RSVP (Ressource reSerVation Protokol), který tvoří další ze čtyř částí nutných k implementaci integrovaných služeb. Je však poměrně složitý a představuje poměrně významnou režii při řízení sítě. Proto se v poslední době objevují jednodušší rezervační protokoly jako např. YESSIR.

Třetí částí nutnou k implementaci integrovaných služeb je plánovač paketů (Packet Scheduler), který řídí zasílání různých proudů dat. Ke své funkci využívá soubory front a další mechanizmy, např. časovač. Plánovač paketů musí být k dispozici na všech místech, kde jsou pakety řazeny do front, aby mohl tyto fronty řídit. Většinou je každý tok řešen svou samostatnou frontou a plánovač pak řeší, jak s jednotlivými frontami zacházet.

Poslední částí, která je zapotřebí při použití integrovaných služeb, je klasifikátor. Ten slouží k identifikaci a směrování paketů. Každý příchozí paket je pomocí klasifikátoru přiřazen do určité třídy QoS. S pakety zařazenými do stejné třídy se pak zachází podle stejných pravidel. [3][7]

3.3 Differentiated services

Differentiated services (DiffServ), česky označované jako rozlišované služby, představují další způsob, jak řídit provoz v síti a zajistit určitou kvalitu služby. Od integrovaných služeb se liší tím, že aplikace neoznamuje předem potřebné požadavky na kvalitu přenosu. Odpadá tak i použití rezervačních protokolů, nutnost uchovávat stavové informace o jednotlivých spojeních. U rozlišovaných služeb směšovače udržují pouze stavovou informaci přidruženou ke každé třídě přenosu a zajišťují určitý vztah mezi jednotlivými třídami.

Implementace rozlišovaných služeb do sítě spočívá v tom, že každý paket vstupující do sítě je opatřen značkou, která určuje třídu přenosu, která bude paketu poskytnuta. S každou třídou pak směrovač zachází rozdílně, ale s pakety v jedné třídě zachází stejně. Označování paketů probíhá pouze při vstupu do sítě a během přenosu sítí směšovače pouze přečtou značku a podle ní pak řídí způsob zpracování paketu. Rozlišované služby se používají spíše na páteřních sítích.

Data jsou na hranici sítě klasifikována a rozdělena do jednotlivých skupin s určitou agregací. Označení chování je zakódováno do kódu DSCP (DiffServ Code Point), který zkoumá klasifikátor. Ten pak provede pro označený paket danou úpravu provozu. Uvnitř sítě mají tedy jednotlivé toky dat jednotné chování, označované jako PHB (Per Hop Behavior), které je přidruženo k DSCP.

Rozlehlé počítačové sítě lze rozdělit na menší sítě, které jsou řízeny místním správcem. V těchto sítích mohou být použity různé protokoly pro zajištění kvality služeb. Je tedy poměrně obtížné zajistit jednotné chování paketů v rámci QoS. Z hlediska rozlišovaných služeb je tedy celá síť rozdělena na oblasti se samostatnou správou rozlišovaných služeb. Tyto oblasti jsou označovány jako DiffServ domény.

Každá doména obsahuje dva druhy směšovačů – vnitřní a hraniční. Vnitřní směšovače zajišťují spojení uvnitř domény a hraniční směšovače zajišťují kromě spojování i klasifikaci paketů do jednotlivých typů tříd. Hraniční směšovače lze ještě rozdělit na ingress směšovače, které provádějí značkování při vstupu do dané DiffServ domény a egress směšovače, které naopak provádějí jejich odznačení při výstupu z dané DiffServ domény. Jsou-li propojeny dvě DiffServ domény, pracuje hraniční směrovač současně jako ingress jedné domény i egress domény druhé, a to v obou směrech.

Jak už bylo řečeno, značkování se provádí v ingress směrovači. Značka může být přidělena na základě zdrojové nebo cílové IP adresy, podle čísel portů označujících určitou službu, podle výsledků měření dynamických vlastností přicházejících dat atd. Uvnitř DiffServ domény je značka neměnná, ale při přechodu do jiné domény může být změněna na jinou značku se stejným významem nebo na stejnou značku s jiným významem. Značka může samozřejmě zůstat stejná, jako v předchozí doméně.

Způsob značení paketu závisí na použité technologii nebo protokolu. Pokud je na značku místo uvnitř hlavičky protokolu, může být obsažena tam, ale může být přidána i vně paketu. V případě použití DiffServ pro přenosy protokolem IPv4 je značka obsažena v poli TOS (Type Of Services) v záhlaví IP.

V případě použití protokolu IPv6 je značka umístěna do pole Traffic Class záhlaví. Pole, do kterého je značka uložena, se označuje DS (Differentiated Services) a má délku osm bitů. Šest bitů je určeno pro vlastní značku, označovanou jako DSCP (differentiated services codepoint), dva zbývající bity jsou ponechány volné a jsou rezervovány pro budoucí použití.

Zpracování paketů v rámci DiffServ domény je možné rozdělit na tři různé úrovně. Charakteristický, znakem nejvyšší úrovně je služba mezi koncovými body komunikace. Jako příklad může sloužit komunikační kanál, který má shodné chování jako pronajatý okruh, a který poskytuje předem dohodnutou propustnost s nízkým zpožděním a malou ztrátovostí paketů, ale ve skutečnosti je realizován pomocí sdílených prostředků sítě.

Střední úroveň zpracování paketů je dána způsobem zacházení paketů v jednotlivých směrovačích bez ohledu na to, jak je s pakety zacházeno v ostatních směrovačích. Jedná se o tzv. per-hop-behaviour (PHB). Každý směrovač se tak stará o pakety tak, aby chování odpovídalo značkám paketů, ale zpracovává je nezávisle na ostatních směrovačích. Uvnitř domény pak nejsou udržovány žádné virtuální spoje.

Specifikace PHB je jednou ze základních částí DiffServ a v současné době jsou standardizovány dvě verze. Urychlené posílání (Expited forvarding) zajišťuje, že každý směrovač v diffserv doméně odesílá pakety průměrnou rychlostí alespoň rovné stanovené rychlosti. Průměrná rychlost se měří v jakémkoliv časovém intervalu delším nebo rovném době potřebné pro odesílání paketu maximální délky stanovenou rychlostí. Urychlené posílání je vhodné pro implementaci virtuálního pronajatého okruhu.

Druhou verzí je zajištěné posílání. To umožňuje zařadit pakety do jedné ze čtyř tříd. Každé třídě je ve směrovačích přidělen určitý objem prostředků jako například velikost vyrovnávací paměti nebo kapacita výstupní linky. V rámci každé třídy je každému paketu přiřazena jedna ze tří priorit zahození paketu (drop precedence), ke kterému může dojít v případě zahlcení. Směrovač musí odeslat paket mající nižší hodnotu priority se stejnou nebo vyšší pravděpodobností než paket mající vyšší hodnotu priority. Zajištěné posílání se používá pro implementaci služeb, u kterých je třeba volitelná úroveň kvality přenosu.

Nejnižší úroveň zpracování paketů je pak definována jako služba best-effort a síť se tedy snaží o maximální využití svých prostředků. V poli DS se jedná o implicitní nastavení a je označena hodnotou 0.

Při větším zatížení počítačové sítě se může stát, že objem dat, která přicházejí na určitý směrovač, přesahuje okamžitou kapacitu linky výstupního portu. Pakety jsou v tomto případě ukládány do fronty ve směrovači. Je tedy třeba řešit situaci, kdy dojde k přeplnění fronty případně přeplnění fronty předejít, a upravovat objem dat, která přicházejí do DiffServ domény.

Úprava objemu dat se obvykle provádí jen na ingress směrovači. K tomuto účelu se používají techniky označované jako kontrolování či hlídání a úprava přenosu. Kontrolování je charakterizováno jako jednoduché zahazování paketů, které se začne provádět po splnění nějaké podmínky. Metoda označovaná jako úprava přenosu spočívá v pozdržování paketů přicházejících do směrovače ve shlucích a odesílání rovnoměrně rychlostí odpovídající kapacitě linky.

Při správné funkci řízení provozu na ingress směrovači by nemělo na vnitřních směrovačích docházet k vyčerpání kapacity front. Vnitřní směrovače včetně ingress směšovače, implementují požadovaná PHB (per-hop-behaviour). Jednotlivá PHB jsou typicky realizována použitím více front s určitým algoritmem pro zařazování paketů do front, výběrem paketů z front a jejich odesílání. Mezi nejpoužívanější metody patří priority queueing – PQ, class-based queueing – CBQ a weighted fair queueing – WFQ. Ve všech případech je paket vložen do jedné z front podle své značky. Metody se liší způsobem obsluhy front.

Priority queueing pracuje tak, že každá fronta má přiřazenu určitou prioritu. Fronty jsou obsluhovány podle priorit tak, že fronta s nejvyšší prioritou je obsloužena jako první a fronta s nejnižší prioritou jako poslední. Nevýhodou této metody je možnost uvíznutí dat ve frontě s nižší prioritou, kdy mohou být data pozdržena natolik, že vysílací stanice je považuje za ztracená a opakuje jejich vysílání, čímž ještě zvýší zatížení sítě.

Class-based queueing je metoda řízení front, kde jsou jednotlivé fronty obsluhovány cyklicky, jedna po druhé. Když přijde fronta na řadu, je z ní odesláno určité množství dat nebo je fronta vyprázdněna úplně. Tato metoda je spravedlivá ke všem frontám stejně, neumožňuje tedy upřednostnění jedné fronty před druhou.

Weighted fair queueing je poslední metoda řízení front. U této metody mají všechny fronty stejnou prioritu a jednotlivým frontám je přidělována část kapacity výstupní linky, která odpovídá váze přiřazené ke každé frontě. Pro přicházející pakety je vypočten čas, kdy nejpozději má být paket odeslán. [7]

4 802.11e

Standard 802.11e je doplněk k původnímu standardu 802.11. Byl schválen koncem roku 2005 a jeho cílem je rozšíření MAC podvrstvy linkové vrstvy původního standardu 802.11 o podporu kvality služeb (QoS). Bez tohoto doplňku by byly bezdrátové sítě značně znevýhodněny v případě jejich využití pro přenos síťového provozu pracujícího v reálném čase. Vznikl tak poměrně silný tlak na to, aby byla kvalita služeb podporována i u bezdrátových sítí. Následkem toho postupně vznikl i standard 802.11e. Ten rozšiřuje původní přístupové metody WiFi o další mechanizmy s propracovanější podporou zajištění QoS. Tyto mechanizmy byly přitom navrženy tak, aby byly přístupové body schopny komunikovat i se staršími komponentami, které tyto nové techniky nemají implementovány.

Základní MAC podvrstva používá ke sdílení média mezi více komunikujícími stranami funkci DCF (Distributed Coordination function). To znamená, že jakmile jedna strana získá přístup k médiu, může ho využívat, jak dlouho chce a ostatní strany se tak nemusejí k médiu na dlouhou dobu dostat. Není zde jakýkoli náznak priority provozu.

Další funkcí, kterou je možné použít, avšak používá se velmi zřídka, je PCF (Point Coordination Function). Tu je však možné použít pouze v infrastrukturním módu, kdy spolu komunikuje jeden přístupový bod a více klientů. PCF funguje tak, že přístupové body vysílají tzv. beacon rámce v pevně stanovených intervalech a PCF je dělí na dva časové úseky. V jednom se používá DCF a ve druhém pak přístupový bod posílá klientům signál, který z nich má právo vysílat.

Standard 802.11e vylepšuje DCF a PCF a přidává novou funkci označovanou jako HCF (Hybrid Coordination Function), někdy označovanou i jako EPCF (Enhanced Point Coordination Function). Dále definuje i rozšíření pro funkci DCF označovanou jako EDCF (Enhanced Distributed Coordination Function). U obou těchto funkcí jsou definovány třídy provozu podle jeho priority a je tak možné rozlišovat zatížení přenosového kanálu podle typu použití (aplikace). Emailová služba tak bude mít nižší třídu priority než například VoWIP (Voice over Wireless IP), u kterého jsou kladeny vyšší nároky na výpadky nebo zpoždění. [4][8][15]

4.1 EDCF

EDCF rozděluje provoz do osmi kategorií přenosu, které odpovídají požadavkům daného typu zátěže. Kategorie jsou rozvrženy v rozsahu od nejnižší priority pro přenos typu best-effort až po nejvyšší prioritu, která se využívá pro přenos dat extrémně závislých na zpoždění, nejčastěji přenos hlasu. Prioritní úrovně používané ve standardu 802.11e jsou identické s prioritami definovanými ve standardu IEEE 802.11d, což zajišťuje vhodnou spolupráci s mechanizmy řízení přístupu v pevných lokálních sítích.

Každá kategorie definuje určitou dobu (AIFS - Arbitration Inter-Frame Space), po kterou žadatel o přenos dat musí čekat, než vlastní přenos zahájí. Zátěž s vyšší prioritou má tuto dobu menší a umožňuje tak rychlejší přístup ke sdílenému médiu, než je tomu u kategorií s nižší prioritou. Tato doba se připočítává k náhodnému intervalu, který stanice generuje při detekci kolize při pokusu o přístupu k médiu. Docílí se tak omezení kolizí s jinými stanicemi, které provozují EDCF ve stejné kategorii.

Tab. 1: Rozdělení priorit podle 802e11d/802.11e

	prioritní úroveň	předpokládané využití (dle 802.11d)	předpokládané využití (dle 802.11e)
nejnižší	1	přenos na pozadí	přenos na pozadí
	2	nedefinované	přenos na pozadí
	0	best-effort	best-effort
	3	excellent-effort	best-effort
	4	řízená zátěž	video
	5	video (zpoždění do 100ms)	video
	6	hlas (zpoždění do 10ms)	hlas
nejvyšší	7	správa sítě	hlas

EDCF tedy poskytuje velmi vysokou pravděpodobnost přidělení vyšších hodnot šířky pásma pro kategorie s vyšší prioritou při soutěžení o sdílené médium. Tato metoda je jednoduše implementovatelná a často používaná.

4.2 HCF

Mechanizmus HCF vychází z centralizované koordinační funkce PCF, ale navíc nabízí propracovanější podporu pro zajištění kvality služeb. Řízení přístupu řeší centrální prvek, nejčastěji přístupový bod podporující 802.11e. Jeho hlavní funkcí je přidělování příležitostí k přenosu v síti. Narozdíl od EHCP, kde je přístup k médiu řízen na základě priority, u HCF může přístupový bod zaručit absolutní garanci doby přenosu a zpoždění. To je dáno díky vyšší prioritě HCF a možností pracovat jak během intervalu bez soutěžení, tak i během intervalu soutěžení.

K plné funkci tohoto mechanizmu nestačí pouhá registrace stanice u přístupového bodu s podporou 802.11e. Stanice musí navíc konkrétně specifikovat své požadavky na síťové prostředky. Tyto požadavky pak musí přístupový bod vyhodnotit a schválit nebo odmítnout, pokud je nemůže zaručit. Na základě těchto parametrů pak přiděluje stanicím potřebné příležitosti k přenosu dat a informuje je vysláním příslušného rámce. Tento rámec je vygenerován vždy na začátku intervalu bez soutěžení a podle potřeby může být generován i během intervalu soutěžení. Stanice může vyzvat k vysílání i více stanic s tím, že pro každou stanici specifikuje, kdy má vysílání zahájit. Na základě těchto informací si pak ostatní stanice zapamatují, jak dlouho musí čekat na uvolnění sdíleného média.

HCF je nejpokročilejší (a také komplexní) koordinační metoda. Při použití HCF lze požadovanou kvalitu přenosu nakonfigurovat s velkou precizností. [4][8][15]

5 Protokoly pracující v reálném čase

Jak už z názvu vyplývá, tyto protokoly jsou určeny pro přenos dat v reálném čase. Nejčastěji se jedná o IP telefonii, videokonference nebo obecně pro přenos multimediálního obsahu přes IP síť. Přestože je pro přenos dat častěji používán transportní protokol TCP, v případě potřeby přenášení dat v reálném čase je vhodnější použít protokol UDP.

TCP je totiž využíván pro spojení bod – bod a před vlastním spojením musí vytvořit mezi koncovými body spojení. Teprve potom je možné data přenést. Není proto vhodný pro multicastové vysílání. Navíc využívá mechanizmy pro opakované vysílání ztracených paketů. To vše je sice potřebné pro správné přenesení dat, dochází tím však ke značnému zpoždění, které je při přenosu multimediálních dat kritičtější než ztráta několika paketů. Z těchto důvodů se tedy používá protokol UDP, který tyto kontrolní mechanizmy nenabízí. UDP prostě vyšle data a co se s nimi dále děje, ho již více nezajímá.

5.1 Real-time Transport Protocol (RTP)

Real-time transport protocol je určen pouze k přenosu uživatelských dat v reálném čase. To může probíhat buď mezi dvěma účastníky (unicast) nebo mezi více učastníky (multicast). Pro každé spojení je třeba znát zdrojovou a cílovou IP adresu, číslo portu pro RTP a číslo portu pro RTCP (real-time transport control protocol), který je používán pro kontrolu a řízení spojení.

Real-time transport protocol obsahuje dva druhy vysílačů (translátor a mixer), které slouží pro optimalizaci datového toku. Vysílačem se rozumí mezilehlé zařízení mezi zdrojem a příjemcem vysílání datového toku.

Mixer je RTP vysílač, který přijímá RTP pakety z jednoho či více zdrojů, které může následně přeskládat a vyslat k jednomu nebo více příjemcům, kteří jsou identifikováni svým jednoznačným identifikačním číslem. Příkladem použití tohoto vysílače může být videokonference mezi několika účastníky. Pokud se stane, že hovoří více účastníků najednou, jsou v mixeru všechny přicházející proudy sloučeny do jednoho proudu, který je potom vysílán k ostatním. Tím jsou sníženy požadavky na šířku pásma.

Translátor je RTP vysílač, který může změnit formát dat nebo použít jakýkoli protokol nižší vrstvy k přenosu z jedné domény do druhé. Příkladem použití translátoru

může být případ, kdy potenciální příjemce není schopen přijímat video signál ve vysokém rozlišení. Translátor tedy konvertuje video do nižší kvality, čímž sníží bitovou rychlost a tím i potřebnou šířku pásma. Video je pak přijímáno bez větších problémů.

5.2 Real-time Transport Control Protocol (RTCP)

Jak již bylo uvedeno, RTP je používán pouze pro přenos uživatelských dat. Pro kontrolu a řízení celého spojení se stará Real-time transport control protocol (RTCP). Stejně jako RTP i RTCP používá pro přenos dat protokol UDP, používá ale jiné číslo portu.

Mezi hlavní funkce RTCP patří kontrola kvality služeb a zahlcení. Mechanizmus poskytuje informace o stavu vysílačů i přijímačů. Zprávy vysílačů (Sender report) umožňují přijímačům odhadovat datovou rychlost a kvalitu přenosu. Přijímače naproti tomu vysílají informace o svých problémech, například problémy se zahlcením. Mohou vysílat i informace o ztrátě paketů nebo o zpoždění. Pomocí těchto informací může aplikace upravit datový tok například snížením kvality poskytovaného obsahu.

Další funkcí RTCP je odhad velikosti relace. Každý účastník spojení periodicky zasílá informace sám o sobě. Při malém počtu účastníků se zprávy zasílají co nejčastěji (přibližně každých 5 vteřin). Čím více je v relaci účastníků, tím je interval mezi zasíláním jednotlivých zpráv větší. Tyto zprávy by neměly linku zatížit více jak z 5% celkové přenosové rychlosti relace.

5.3 Real Time Streaming Protocol (RTSP)

RTSP stejně jako RTCP není určen k vlastním přenosu dat, slouží pouze k řízení doručování dat v reálném čase. Podporuje ovládací funkce přehrávače jako například zastavení, převíjení apod. V podstatě se tedy jedná o jakýsi síťový dálkový ovladač. Využívá se především u služby video na požádání (video on demand – VoD).

5.4 Session Descrition Protocol (SDP)

SDP je textově orientovaný síťový protokol, který má za úkol přenášet detaily o spojení při realizaci multimediálních spojení. Příkladem takového spojení může být uskutečněný hovor pomocí VoIP nebo obecně nějaká multimediální konference. U multicastových spojení má SDP za úkol informovat o výskytu právě běžících relací a

zprostředkovat informace potřebné k tomu, aby bylo možné se k dané relaci připojit. Obsahuje tak informace o názvu a účelu relace, o době trvání relace, seznamu médií v relaci, šířce pásma potřebného k běhu relace nebo kontaktní informace o uživateli odpovídajícího na relaci.

Relace je popsána řadou dvojic „atribut – hodnota“. Atribut je vždy jeden znak, hodnota pak může obsahovat několik řetězců znaků oddělených mezerou

5.5 Session Announcement Protocol (SAP)

Jak již z názvu vyplývá, SAP je protokol sloužící k oznamování multicastových relací. Princip spočívá v tom, že vysílač v periodických intervalech odesílá své informace na známé multicastové adresy a porty. Na těchto portech odposlouchávají potenciální účastníci multimediální relace. Zprávy pouze oznamují, že relace existuje.

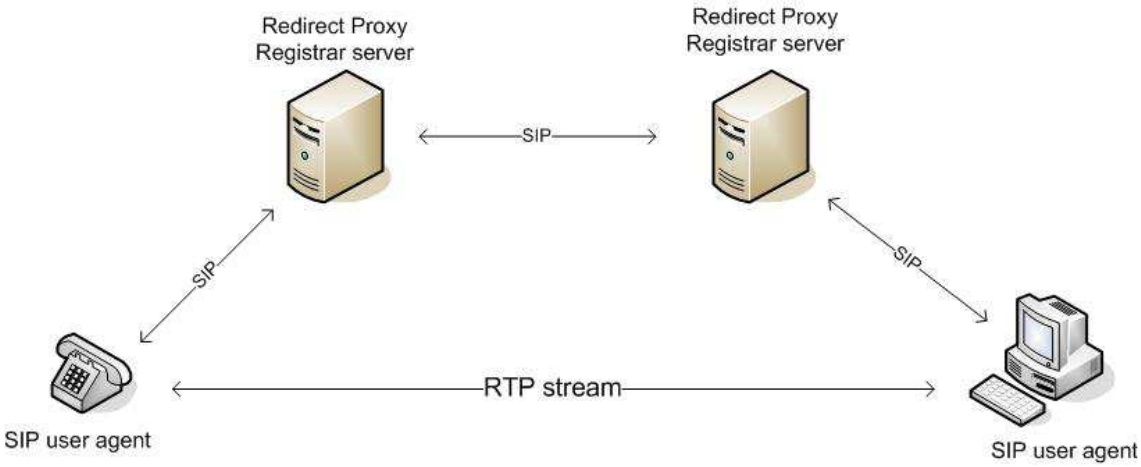
5.6 Session Initiation Protocol (SIP)

SIP je další protokol, který se využívá pro přenos multimediálních informací v reálném čase, nejčastěji pro internetovou telefonii. Opět neslouží k přenosu vlastních informací, ale pouze k signalizaci pro navázání, modifikaci a ukončení spojení. Pro vlastní přenos dat je opět použit RTP. SIP se používá pro spojení bod – bod a je stejně jako SDP textově orientovaný. To napomáhá nejen jednoduchému ladění, ale především snadné rozšiřitelnosti. Protokol SIP je typu klient-server, takže komunikace probíhá výměnou dvou typů zpráv, požadavků a odpovědí.

Základními dvěma komponentami v architektuře SIP jsou User agent a Server. User agent představuje koncové zařízení, jímž je ve většině případů telefon, ať už hardwarový nebo softwarový. Jako user agent se může tvářit i brána do jiných sítí. User agent je pak dále rozdělen na user agent client, který obstarává inicializaci spojení a na user agent server, který reaguje na příchozí události a posílá odpovědi. User agent server i user agent client jsou pouze logickým rozdělením jednoho koncového zařízení.

Druhou základní komponentou architektury SIP je server, přičemž SIP rozlišuje tři typy serverů. Proxy server přijímá žádosti od koncových uživatelů nebo jiných serverů a tyto žádosti pak posílá dál dalšímu proxy serveru nebo volanému koncovému zařízení. Druhým typem je Redirect server. Ten také přijímá žádosti od koncových zařízení, avšak žádosti nepřeposílá dál a tázajícímu pošle zpět informaci o tom, kam má danou žádost poslat, aby se dostala k volanému. Třetím typem serveru je Registrar

server, který pouze přijímá registrační žádosti od koncových zařízení a aktualizuje si tak svojí databázi koncových zařízení v dané doméně. [2][3]



Obr. 3: SIP architektura

6 OPNET modeler

OPNET Modeler je simulační program vyvinutý firmou OPNET Technologies Inc., a slouží k návrhu simulací a analýze různých síťových technologií a mechanizmů. Podrobně a efektivně dokáže modelovat chování rozsáhlých sítí a protokolů pracujících na různých vrstvách síťového modelu.

Díky grafickému prostředí je práce s modelerem rychlejší a přehlednější. Další jeho výhodou je široká možnost tvorby různých statistik z dané simulace. OPNET Modeler tak lze využít jako testovací nástroj pro ověření chování sítě v extrémních podmínkách. Jeho pomocí můžeme tak nasimulovat stav, který ani nemusí nastat a ověřit tak, jak se v dané situaci daný objekt zachová. Díky výsledku takové situace pak můžeme odvodit a vyzkoušet, jak těmto nežádoucím stavům předcházet.

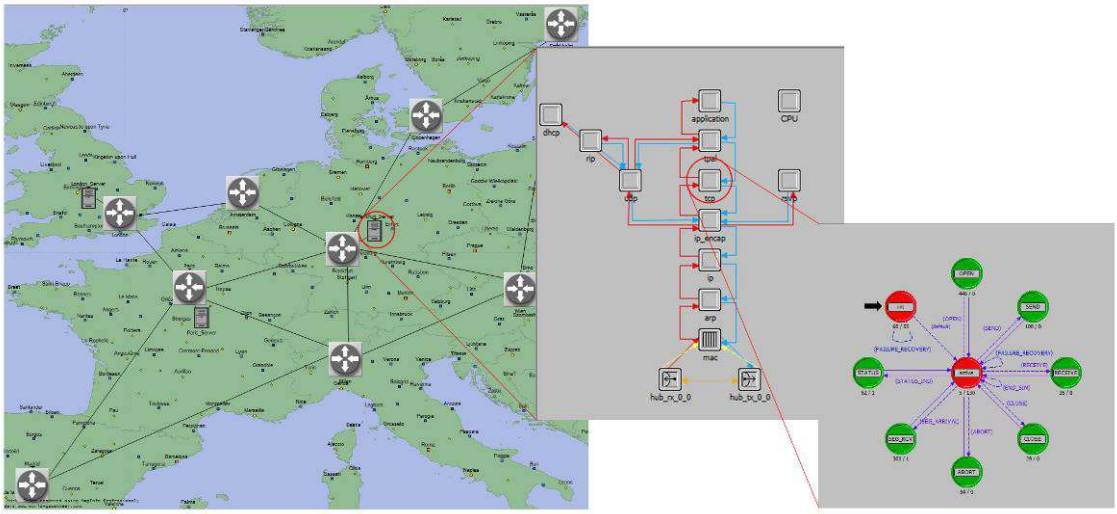
Výsledné statistiky je možné generovat do zprávy ve formátech XML nebo HTML, případně data uložit do tabulek. Program dokáže pak data z těchto tabulek zpět načíst.

Simulace probíhá rychleji než v reálném čase, takže je možné nasimulovat chování sítě v delším časovém období (měsíc) během několika hodin.

OPNET Modeler je multiplatformní program, lze jej tak spustit pod více operačnímy systémy (Windows, Linux). Jeho knihovny mají dostupný zdrojový kód, z čehož plyne, že jej lze dále upravovat.

6.1 Základní části prostředí OPNET Modeleru

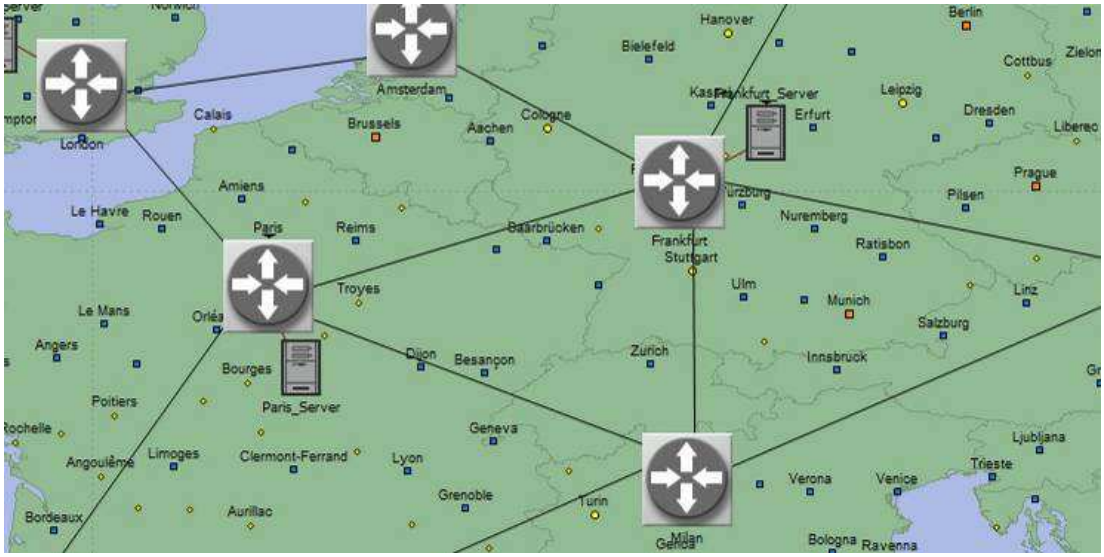
OPNET modeler má tři základní části (editory). Jedná se o editor projektu, editor uzlu a editor procesu.



Obr. 4: Základní struktura OPNET Modeleru

Editor projektu

Editor projektu je grafický editor, který modeluje topologii sítě a způsob komunikace použitý v síti. Topologie se sestavuje pomocí jednotlivých uzlů, které představují jednotlivé stanice, aktivní síťové prvky a komunikační linky. Dále je možné si vytvořit vlastní uzly. Editor projektu může mít v sobě mapu, na které je možné znázornit fyzické rozmístění jednotlivých prvků.

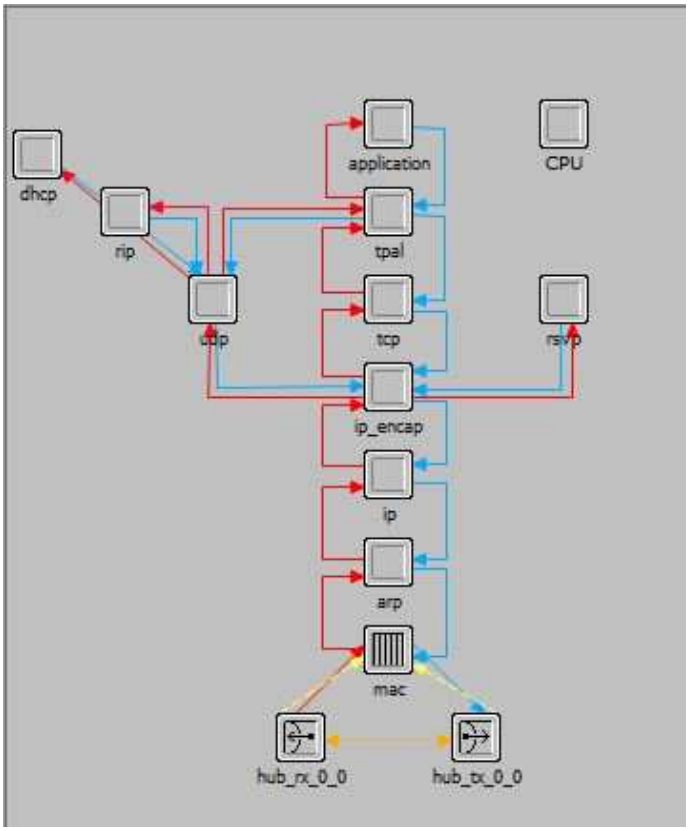


Obr. 5: Síťový model v editoru projektu

Editor uzlu

Editor uzlu představuje rozhraní nižší úrovně, než editor projektu. Je v něm znázorněna vnitřní architektura síťového zařízení nebo systému a vzájemné vztahy mezi funkčními bloky a volanými funkcemi. Uzel se skládá z modulů (bloků), které většinou představují aplikace protokolové vrstvy, algoritmy a fyzické prostředky jako jsou buffery, porty či sběrnice.

Další důležitou vlastností je předávání hodnot atributů do vyšších úrovní. Díky této vlastnosti lze klíčové parametry simulace zobrazit u objektů nejvyšší úrovně a není nutné se složitě "proklikávat" k objektu, kterého se daný parametr konkrétně týká (např. IP adresy definované na procesním modelu popisujícím proces vrstvy IP).

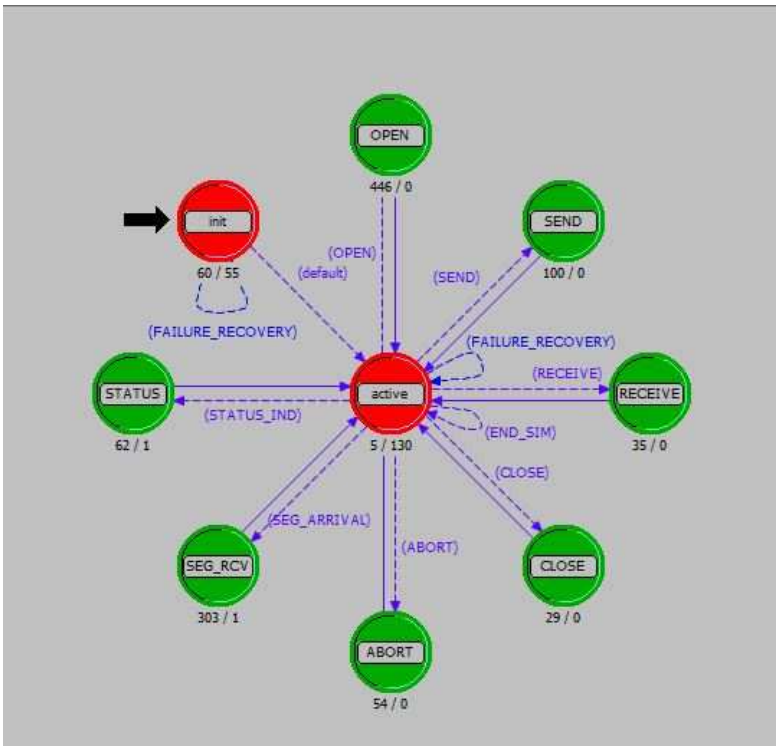


Obr. 6: Pracovní stanice v editoru uzlu

Editor procesu

Editor procesu je editor nejnižší úrovně. Slouží pro tvorbu konečného stavového automatu, který je přizpůsoben snaze specifikovat všechny úrovně modelu do detailu. Stavy a přechody jsou definovány v grafickém diagramu. Každý stav a proces modelu

obsahuje kód v C/C++ podporovaný rozsáhlou knihovnou s funkcemi vytvořenými pro protokolové programování.



Obr. 7: TCP v editoru procesu

7 Simulace QoS v bezdrátových sítích

V programu OPNET Modeler budou nyní nasimulovány dvě identické sítě, které budou obsahovat několik klientských stanic. Ty budou bezdrátově připojeny k přístupovému bodu pomocí standardu 802.11b s maximální přenosovou rychlostí 11Mbps. K tomuto bodu bude připojeno pomocí linky 100BaseT několik serverů, které budou mít na starosti jednotlivé síťové služby. Tyto sítě se budou lišit pouze tím, že jedna bude podporovat QoS a druhá ne. Oba scénáře pak porovnáme s hlediska síťových parametrů důležitých pro provoz multimediálních dat (zpoždění, ztrátovost atd.), které by měly být upřednostňovány.

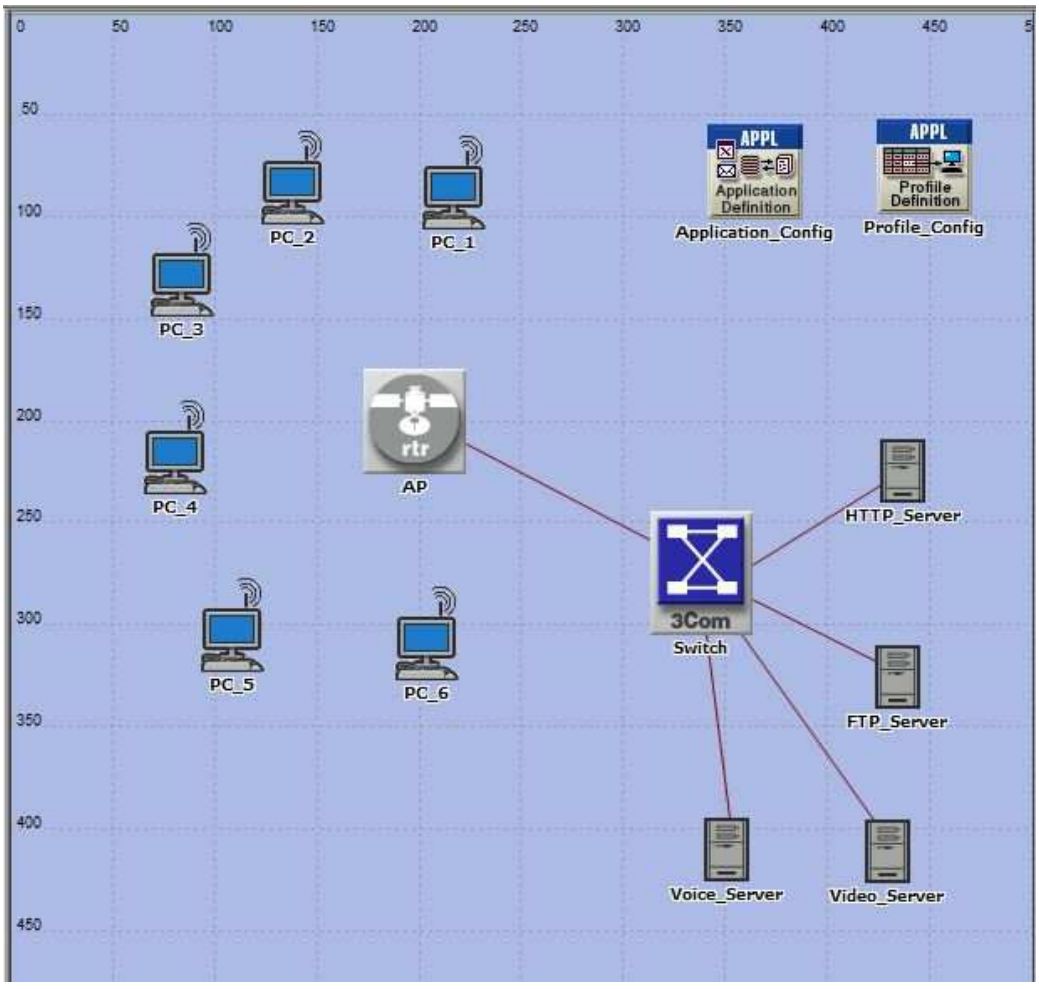
Síť ještě musí obsahovat, kromě standardních síťových prvků, komponenty Application Config a Profile Config, pomocí nichž je v síti nadefinován síťový provoz a jeho parametry.

V Application config jsou nadefinovány 4 aplikace, které zajišťují přenos dat (HTTP, FTP, VoIP a přenos videa). Ve scénáři s podporou QoS je zde ještě definována třída provozu (priorita) jednotlivých aplikací:

- HTTP – Background – prioritní úroveň 1
- FTP – Best Effort – prioritní úroveň 0
- Video – Video – prioritní úroveň 4 (Streaming Multimedia)
- Voice – Voice – prioritní úroveň 6 (Interactive Voice)

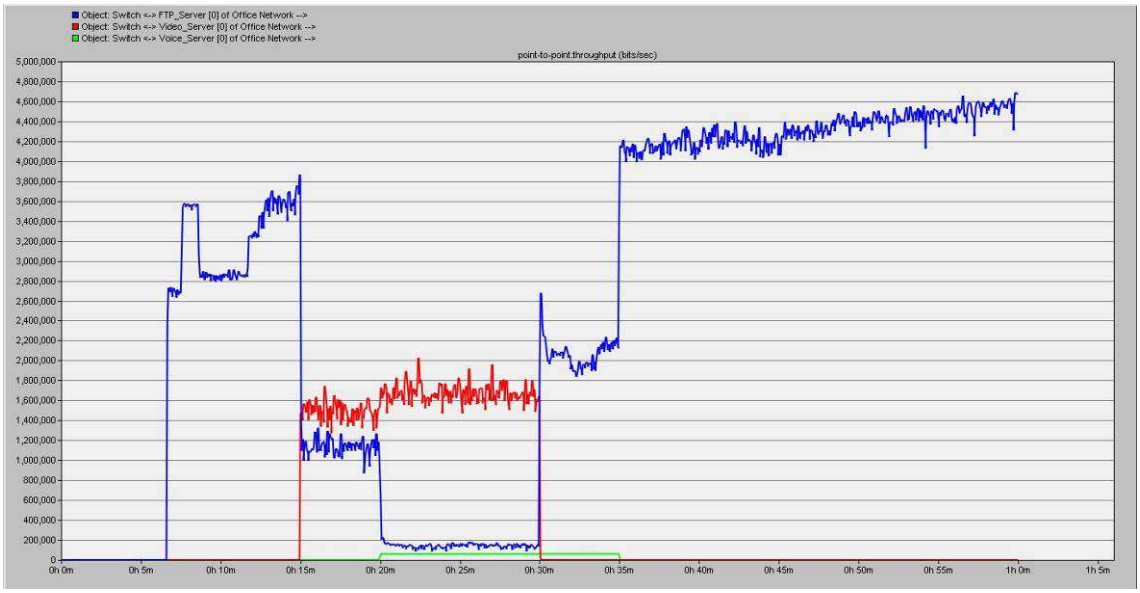
U scénáře s podporou QoS je ještě nutné zapnout podporu QoS u všech klientských stanic a u přístupového bodu. Nastavení ponecháme nastaveny v defaultním stavu, podle standartu 802.11e.

Profile Config pak obsahuje profily jednotlivých aplikací jako čas spuštění, délka trvání, počet opakování apod. Provoz v síti byl nastaven tak, že HTTP běží celou dobu simulace, přenos pomocí FTP začne v 6. minutě a trvá až do konce simulace. Přenos videa začne 15 minut od začátku simulace a délka trvání je nastavena na 15 minut. Ve 20. minutě se pak ještě na 15 minut spustí VoIP. Celková doba simulace je nastavena na 1 hodinu.

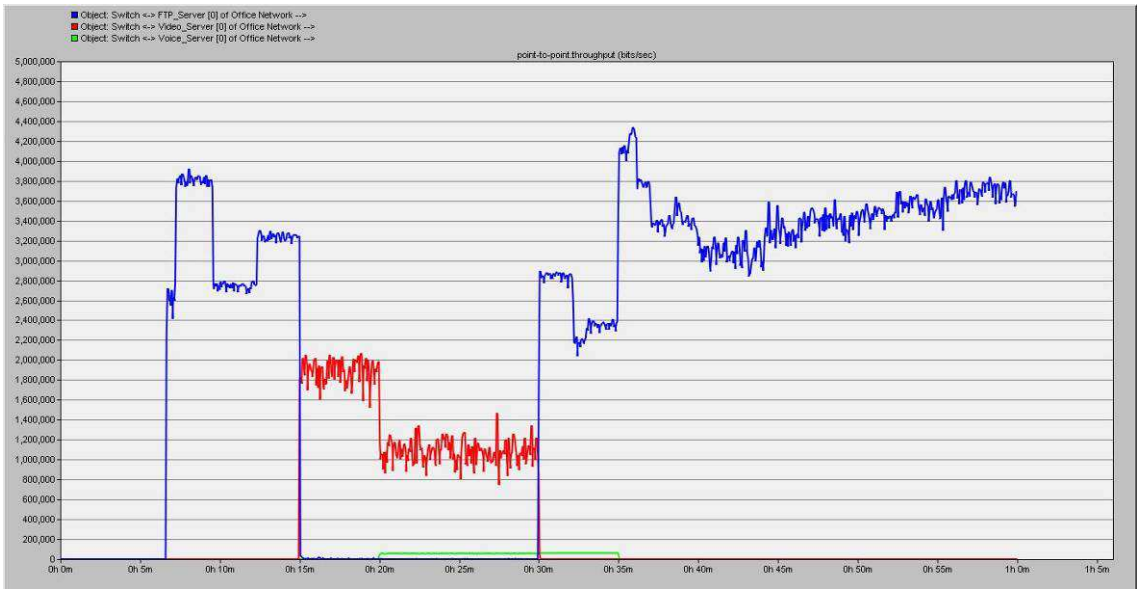


Obr. 8: Topologie sítě

Na následujících grafech je znázorněna propustnost jednotlivých datových toků. Modrá představuje přenos dat z FTP serveru, červená znázorňuje přenos videa a zelená ukazuje přenos pomocí VoIP. Horní graf pak ukazuje výsledek simulace scénáře bez podpory QoS a spodní graf je výsledkem simulace stejné sítě s podporou QoS.



Obr. 9: graf propustnosti sítě bez podpory QoS



Obr. 10: Graf propustnosti sítě s podporou QoS

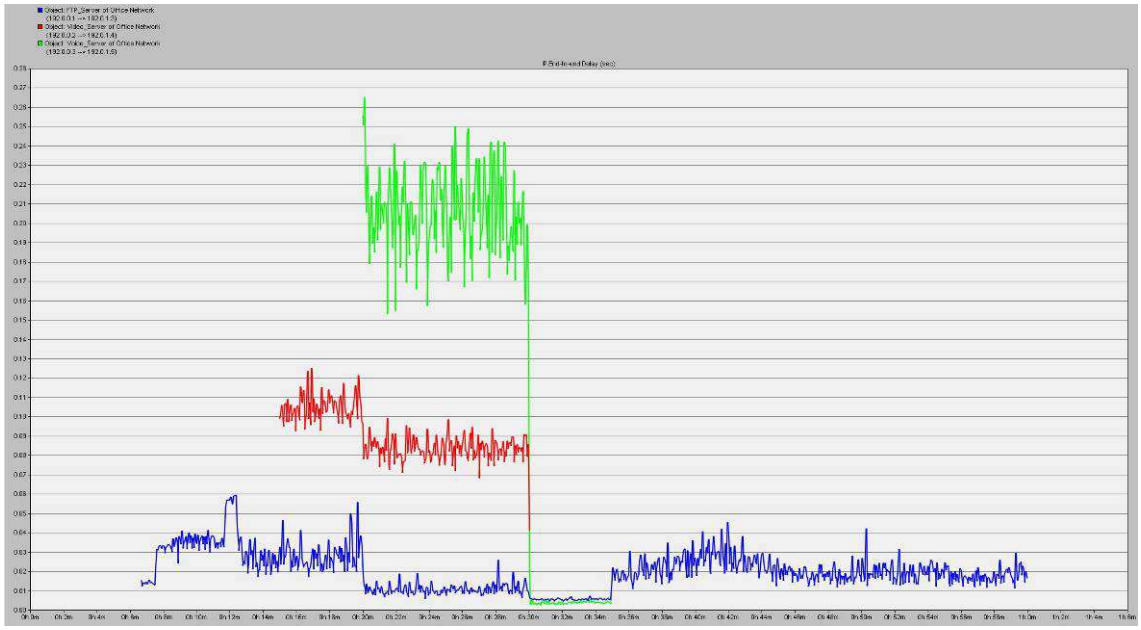
Jak je z výsledků patrné, při zahájení přenosu videa ustupuje přenos dat z FTP serveru do pozadí a využívá pouze nevyužitou část přenosové kapacity. Když se k přenosu videa ještě přidá videotelefonie, přenos dat z FTP serveru se ještě o něco zpomalí. Když se postupně ukončuje přenos videa a hovoru, přenos z FTP opět narůstá a využívá dostupnou přenosovou kapacitu.

Pokud QoS aktivujeme, je při zahájení přenosu videa přenos dat z FTP serveru téměř zastaven a celá přenosová kapacita je využita pro přenos videa. Po zahájení videohovoru klesá i přenosová rychlost videa na úkor hovoru, který má vyšší prioritu. Celková propustnost sítě je tedy nižší, zpoždění se zmenší a přenos videa a hlasu je kvalitnější. Po postupném ukončení přenosu videa a hovoru se opět zbylá přenosová kapacita využije pro přenos dat z FTP serveru.

Když se podíváme na zpoždění, zjistíme, že u sítě bez podpory QoS je zpoždění u FTP přenosu (modrá) mnohem lepší, než u přenosu videa (červená). Zpoždění při přenosu hlasu (zelená) je největší a nejčastěji dosahuje hodnot od 160 do 240 ms. To je však již na hranici tolerance pro ještě vyhovující kvalitu hlasu (viz Tab. 2)

Tab. 2: Kvalita hovoru v závislosti na parametrech sítě

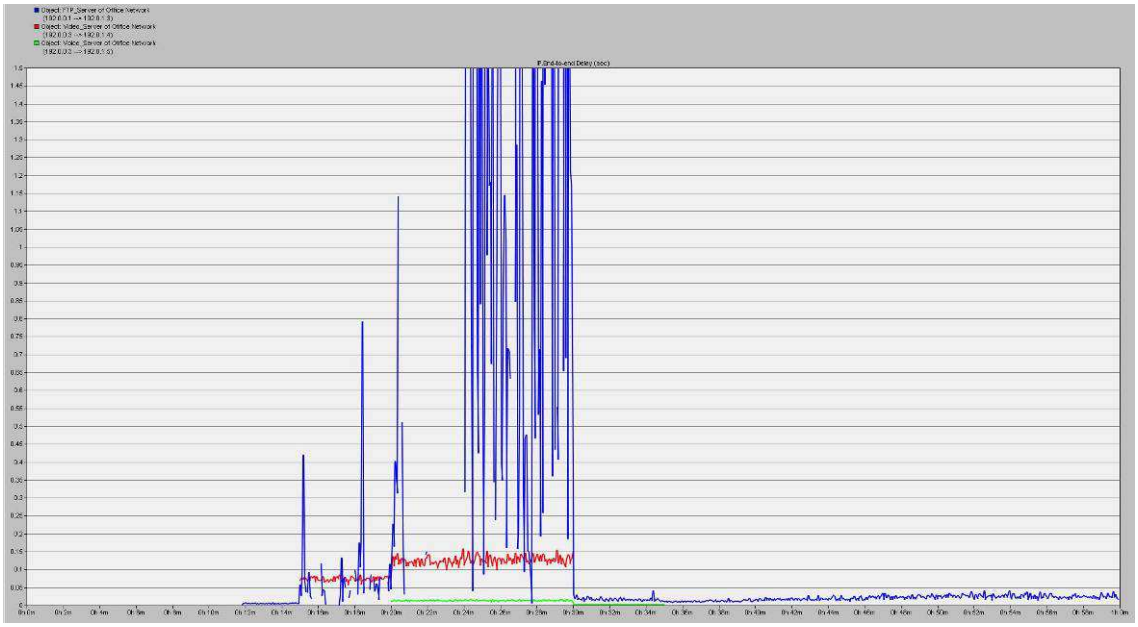
Kvalita hlasu	Dobrá	Vyhovující	Nevyhovující
Zpoždění	0 – 150 ms	150 – 300 ms	nad 300 ms
Kolísání zpoždění	0 – 20 ms	20 – 50 ms	nad 50 ms
Ztrátovost	0 – 0,5 %	0,5 – 1,5 %	nad 1,5 %



Obr. 11: zpoždění v síti bez podpory QoS

Podíváme-li se na scénář s podporou QoS, uvidíme, že se situace obrátila a videohovor má nejmenší zpoždění, které dosahuje hodnot do 50 ms. Kolísání zpoždění dosahuje 20 ms. To zcela vyhovuje tolerancím a kvalita hovoru by měla být dobrá. Zpoždění při přenosu videa dosahuje hodnot kolem 200 ms, což je sice o něco vyšší hodnota než u sítě bez podpory QoS, kde se hodnoty zpoždění pohybovaly kolem 100 ms. Výrazně se zvětšilo i jeho kolísání (nyní se pohybuje kolem 160 ms oproti

předchozím 50 ms). Zpoždění u přenosu dat pomocí FTP výrazně vzrostlo a pohybuje se od 0,2 do 2,4 sekund při přenosu videa a při současném přenosu videa a hlasu hodnoty zpoždění dosahují až stovek vteřin.



Obr. 12: Zpoždění v síti s podporou QoS

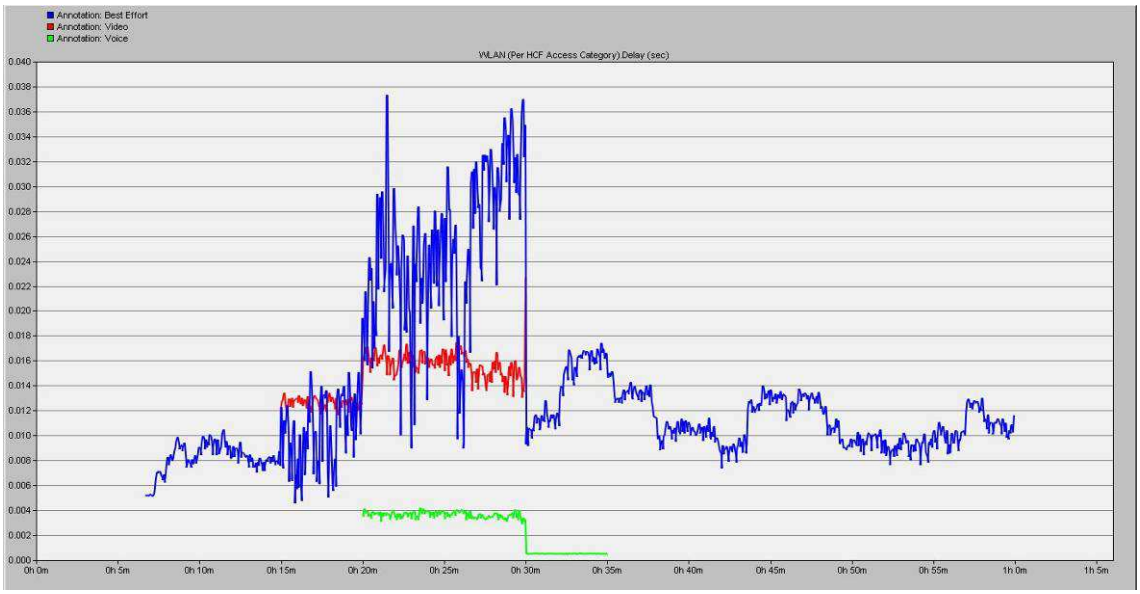
Dalším důležitým parametrem, který se při přenosu dat sleduje, je ztrátovost, tedy kolik procent z celkového počtu odeslaných paketů je při přenosu z nějakého důvodu zahozeno. V našem případě se ztrátovost díky vysoké vytíženosti sítě i přes použití QoS a prioritizaci provozu videohovoru pohybovala kolem 2%, což je již podle Tab. 2 nevyhovující hodnota. Po ukončení přenosu videa a uvolnění šířky pásma pak ztrátovost spadla na nulovou hodnotu a kvalita hovoru se tak prudce zlepšila. Ostatní typy provozu měly ztrátovost mnohem vyšší, protože měli v síti nižší nastavenu nižší prioritu, než přenos hlasu.

Z výsledků této simulace tedy jasně vyplývá vliv použití QoS na chování přenosu dat sítí. Telefonie, která je na zpoždění v síti velmi citlivá, má největší prioritu a díky ní mají pakety patřící tomuto provozu velmi malé zpoždění. Přenos videa má prioritu o něco menší (nižší nároky na zpoždění), což se projeví i na zpoždění, které je o něco větší než u přenosu telefonního hovoru. Přenos dat přes FTP má nejnižší prioritu a využívá pouze zbytek volné přenosové kapacity. Zpoždění díky tomu dosahuje velmi vysokých hodnot.

V další části práce bude demonstrována stejná topologie za použití ostatních dnes používaných standardů 802.11 a jednotlivé standardy budou porovnány z hlediska výše zmíněných parametrů přenosu dat.

7.1 Simulace sítě 802.11g

Jak už bylo řečeno, bude použita stejná topologie sítě, bude však použit novější standard 802.11g. Ten umožňuje přenos dat vyšší přenosovou rychlostí. Aby byla síť nadále plně využita, zapojí se do přenosu zbylé koncové stanice, které budou stahovat data z FTP serveru a využije se tak celé přenosové kapacity sítě a upřednostňování provozu bude lépe patrné.



Obr. 13: Zpoždění v síti 802.11g s podporou QoS

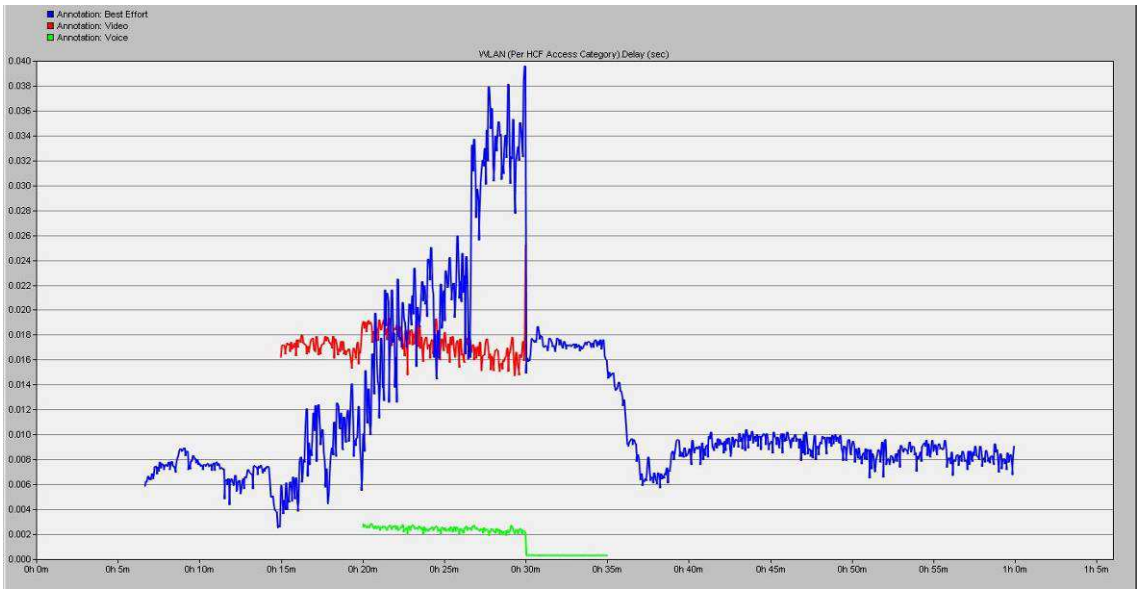
Z výsledného grafu zobrazující zpoždění v síti jsou opět jasně vidět jednotlivé typy datového přenosu. Průběh vypadá podobně jako v předchozím případě. Po zapnutí přenosu videa se u přenosu dat z FTP serveru (modrá křivka) zvětší nejenom zpoždění ale především jeho kolísání. Zpoždění při přenosu videa (červená křivka) je sice o něco větší (12 – 14ms), kolísání je však mnohem menší (2 ms u videa oproti 10 ms při FTP), přenos je tak plynulejší a nedochází k zasekávání videa.

Po zapnutí videohovoru se zpoždění ostatního provozu ještě zhorší. Nejvíce je to patrné u přenosu pomocí FTP, kde se zpoždění pohybovalo mezi 16 a 36 ms. U přenosu videa to bylo pouze mezi 15 a 17 ms, později zpoždění ještě o 1 ms kleslo. Zpoždění u videohovoru se pohybovalo v rozmezí od 3 do 4 ms a po skončení přenosu videa pak kleslo pod 1 ms.

Ztrátovost videohovoru se zde, stejně jako v předchozím případě, v době maximálního využití sítě pohybovala kolem 2% a pro přenos hlasu byla tedy nevyhovující (opět viz Tab. 2). Po skončení přenosu videa klesla ztrátovost na nulu a opět tak zlepšila kvalitu hovoru.

7.2 Simulace sítě 802.11a

Dalším standardem, kterým se budeme zabývat je 802.11a. Ten má stejnou maximální přenosovou rychlost jako předcházející standard 802.11g, liší se pouze ve využití přenosového pásma. Místo pásma 2,4 GHz využívá pásmo 5 GHz. Použitá topologie je shodná s předchozím scénářem. Po provedení simulace dostaneme následující graf zpoždění jednotlivých toků dat.



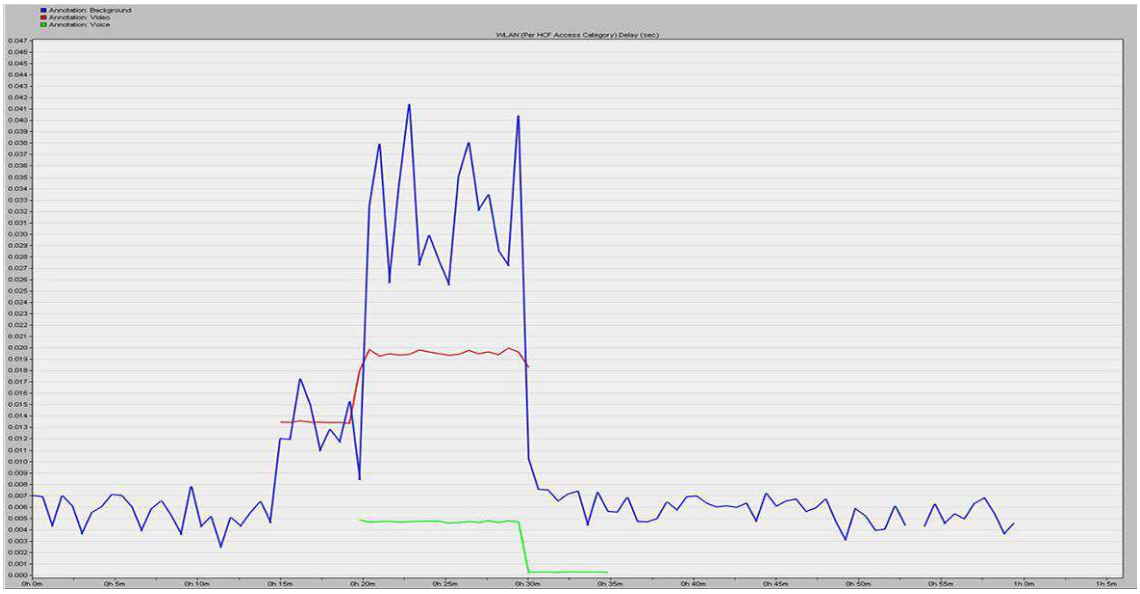
Obr. 14: Zpoždění v síti 802.11a s podporou QoS

Z výsledných průběhů zpoždění vyplývá, že použití QoS se zachovalo jako v předchozích případech a přenos videohovoru (zelená křivka) je upřednostněn před ostatním provozem. Dosahovaná zpoždění jsou nejmenší ze všech typů dat a pohybují se opět kolem 3 ms při současném přenosu hovoru a videa. Po ukončení přenosu videa zpoždění opět klesne pod 1 ms. Zpoždění přenosu videa se pohybuje mezi 17 a 18 ms a jeho kolísání je v rozmezí 2 ms. Přenos pomocí FTP má potom jak zpoždění tak i kolísání zpoždění největší. Situace je tak téměř stejná jako v případě standardu 802.11g a změna přenosového pásma z 2,4 GHz na 5 GHz neměla podle předpokladu žádný vliv na chování sítě.

Ztrátovost při přenosu videohovoru se zde však pohybovala kolem 0,8 %, při současném přenosu hovoru a videa, a došlo zde tak k zlepšení v porovnání s předchozími standardy. Po skončení videa však ztrátovost neklesla na nulu, ale pohybovala se na úrovni 0,1%. Kvalita hovoru tak byla podle Tab. 2 vyhovující, ke konci pak dobrá. Změnou přenosového pásma tak došlo ke zlepšení ztrátovosti a tím i kvalitě hovoru.

7.3 Simulace sítě 802.11n

Nejnovější používaný standard v současné době je 802.11n. Ten je schopen pracovat jak v pásmu 2,4 GHz tak i 5GHz. Přenosová rychlost pak hlavně díky technologii MIMO narostla na maximálních 600 Mbit, avšak současný stav techniky umožňuje přenosovou rychlost pouze 300 Mbit/s. Vzhledem k mnohem vyšším přenosovým rychlostem byla topologie doplněna o další dvě koncové stanice připojené k přístupovému bodu a dojde tak opět k plnému vytížení celé sítě.



Obr. 15: Zpoždění v síti 802.11n s podporou QoS

Výsledné průběhy zpoždění opět ukazují rozdělení přenosu jednotlivých typů dat tak, jak se očekávalo. Zpoždění přenosu dat z FTP (modrá křivka) serveru se postupně zvětšovalo, vždy s počátkem přenosu s vyšší prioritou. Nejprve se přidává přenos videa, který zapříčiní nejen zvětšení zpoždění (z 6 na 12 ms), ale i jeho výkyvy (9 ms). Přenos videa má sice zpoždění v průměru téměř stejné jako přenos pomocí FTP, výkyvy jsou však minimální (1 ms) a přenos videa je tak velice plynulý. Po zahájení videohovoru se zpoždění přenosu dat z FTP serveru opět zvýší a dosahuje 25 – 42 ms. Přenos má tedy i značné rozdíly ve zpoždění (17 ms). Zpoždění přenosu videa stoupne z předchozích 13 na 19 – 20 ms. Kolísání zpoždění se pohybuje opět v rozmezí 1 ms. Přenos hovoru, který má nejvyšší prioritu má zpoždění 5 ms a jeho kolísání se pohybuje opět v rozmezí 1 ms. Po ukončení přenosu videa pak zpoždění klesá pod 1 ms. Průběhy zpoždění jsou tedy opět velice podobné průběhům v předchozích scénářích.

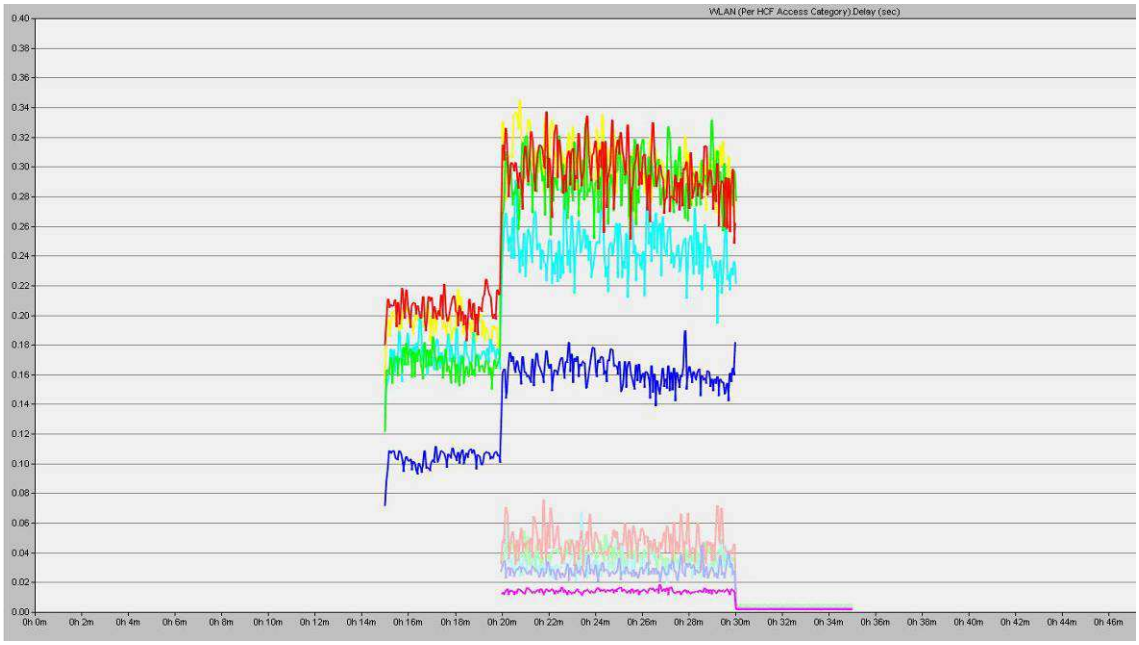
Ztrátovost při přenosu videohovoru se pohybuje kolem 0,77%, po skončení přenosu videa pak byla nulová. Kvalita hovoru tak byla podle Tab. 2 vyhovující, stejně jako v předchozím případě.

8 Simulace QoS v sítích rušených okolními sítěmi

Velkým problémem v dnešní době je velké množství domácích wifi sítí. Toto velké množství způsobuje, že se jednotlivé sítě navzájem ruší a dochází tak k většímu zpoždění přenášených paketů a také k jejich větší ztrátovosti. To má za následek zhoršení přenosu dat. Tento problém je navíc mnohem zřetelnější při přenosu multimediálních dat, které jsou právě na tyto parametry sítě velice závislé. V následujících scénářích se tedy pokusíme nasimulovat, jak si jednotlivé standardy poradí s rušením od okolních sítí.

8.1 Rušení sítě standardu 802.11b

Jako zdroj rušení naší sítě byla vytvořena ještě jedna bezdrátová síť, využívající stejný standard. Tato síť obsahuje čtyři klientské stanice, které jsou připojeny k přístupovému bodu a během simulace stahují data z druhého FTP serveru. Tato síť pracuje nejprve na jiném kanálu, v dalším scénáři používá stejný kanál, jako první síť. Pro oba tyto případy jsou pak přístupové body umístěny vedle sebe, čímž by se mělo rušení zesílit. Výsledné průběhy jsou zobrazeny na následujících grafech.

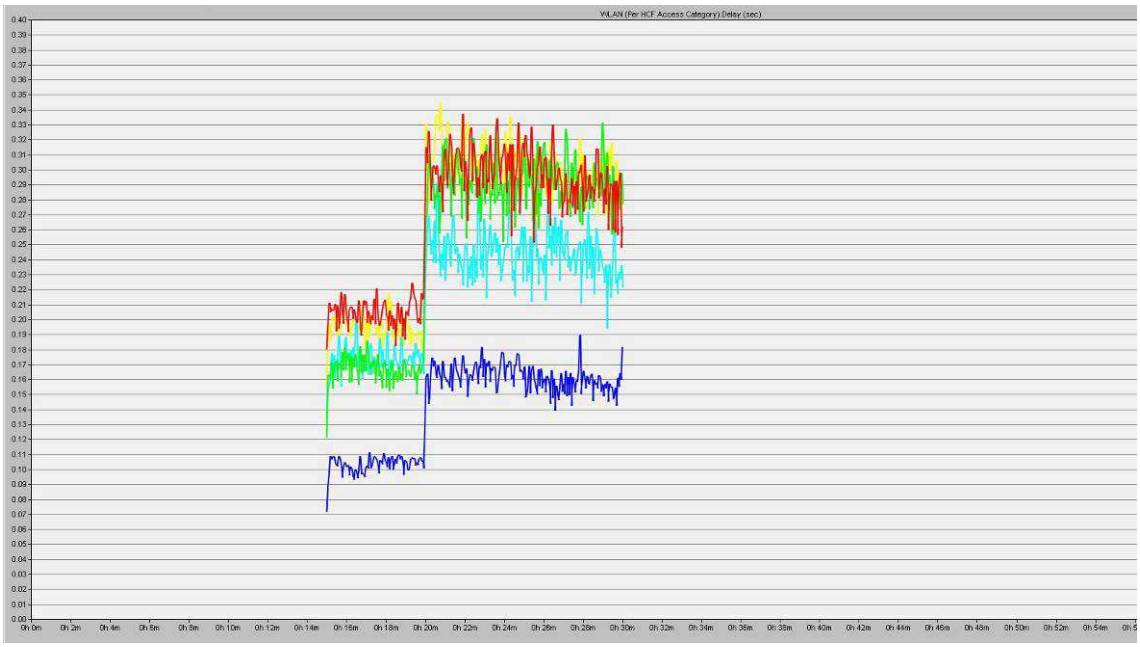


Obr. 16: Zpoždění v síti 802.11b pro přenos videa a videohovoru při rušení okolím

Z grafu na Obr. 16 vyplývá, že všechny popsané druhy rušení mají negativní vliv jak na zpoždění v síti, tak i na jeho kolísání. A to jak pro přenos videa, tak pro přenos videohovoru. Pro oba tyto datové toky je zpoždění jedním z kritických parametrů. Průběhy s větším zpožděním odpovídají přenosu videa a křivky s menším zpožděním pak odpovídají přenosu hovoru. Rozdělení datového toku do jednotlivých tříd podle

jeho priority je tedy stále patrné a plní svůj účel. Detailnější zobrazení pro jednotlivé datové toky jsou na Obr. 17 a 18.

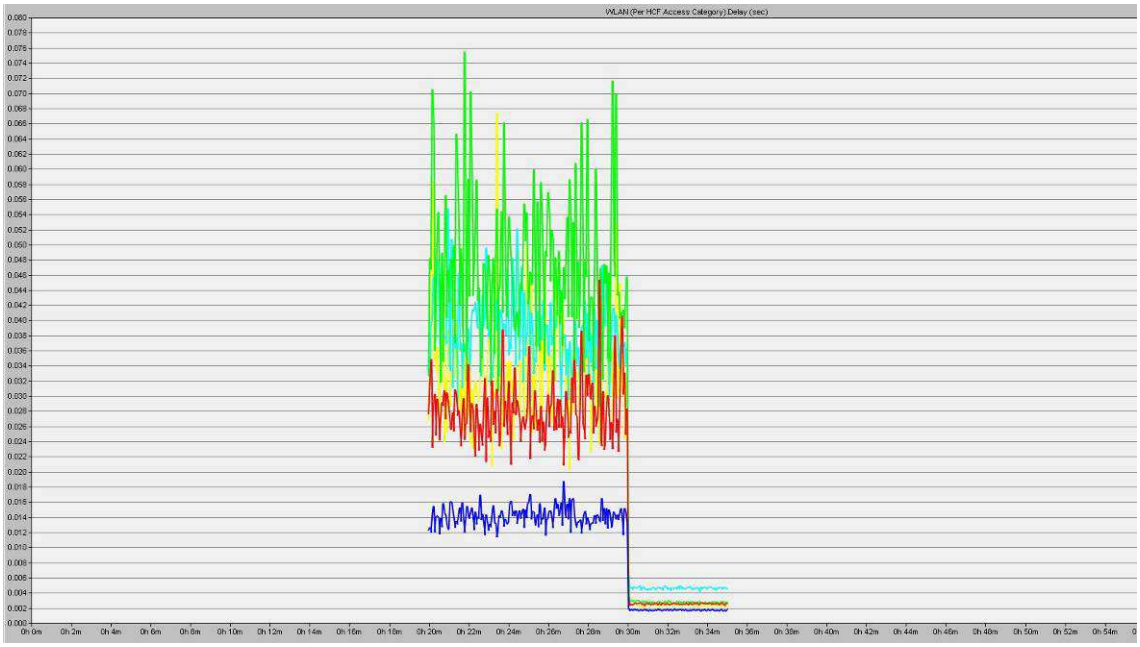
Zpoždění pro přenos dat z FTP serveru se u rušené sítě během přenosu videa a videohovoru pohybovalo v řádu jednotek až desítek vteřin a stejně na tom bylo i kolísání zpoždění, které rovněž dosahovalo až 12 vteřin. Z toho důvodu nejsou tyto průběhy v grafu znázorněny. Graf by pak byl díky velkému měřítku velmi nečitelný a ostatní průběhy by se slily do jednoho.



Obr. 17: Zpoždění přenosu videa v síti 802.11b během rušení okolím

Výsledné průběhy přenosu videa odpovídají předpokladům, že zpoždění u sítě, která není nijak rušena okolím (modrá křivka) jsou hodnoty zpoždění nižší, než v případě jeho rušení a to o 60 – 160 ms. Jako nejhorší se podle výsledků simulace poněkud překvapivě nejeví případ, kdy jsou umístěny dva přístupové body vedle sebe a zároveň pracují na stejném kanálu (žlutý průběh), ale případ, kdy je přístupový bod umístěn ve větší vzdálenosti (ale stále v dosahu) a pracuje na odlišném kanálu (červený průběh). Rozdíly ve zpoždění mezi těmito dvěma případy jsou však minimální. Zelený průběh pak představuje případ umístění dvou přístupových bodů v blízkosti u sebe, pracujících na různých kanálech a světle modrá (azurová) znázorňuje případ rušení z větší vzdálenosti, ale na stejném kanálu.

Dalším sledovaným parametrem je kolísání zpoždění. To u rušení sítě rovněž vzrostlo, z předchozích 30 ms u nerušené sítě, na 60 – 80 ms u sítě rušené. Nezáleží přitom, o které rušení se jedná, kolísání je ve všech případech přibližně stejné.



Obr. 18: Zpoždění přenosu hovoru v síti 802.11b během rušení okolím

V grafu na Obr. 18 je opět vidět vliv rušení, tedy zvýšení zpoždění i jeho kolísání. Barevné rozložení jednotlivých průběhů je shodné s předchozím případem. Nejlépe je na tom modrý průběh, tedy případ, kdy síť není ničím rušena. Nejhůře dopadl při přenosu hovoru stav, kdy byly dva přístupové body vedle sebe, ale každý pracoval na jiném kanálu (zelená). Hodnoty zpoždění se pohybovaly v rozmezí od 35 do 70 ms. Jeho kolísání tedy dosahovalo 35 ms.

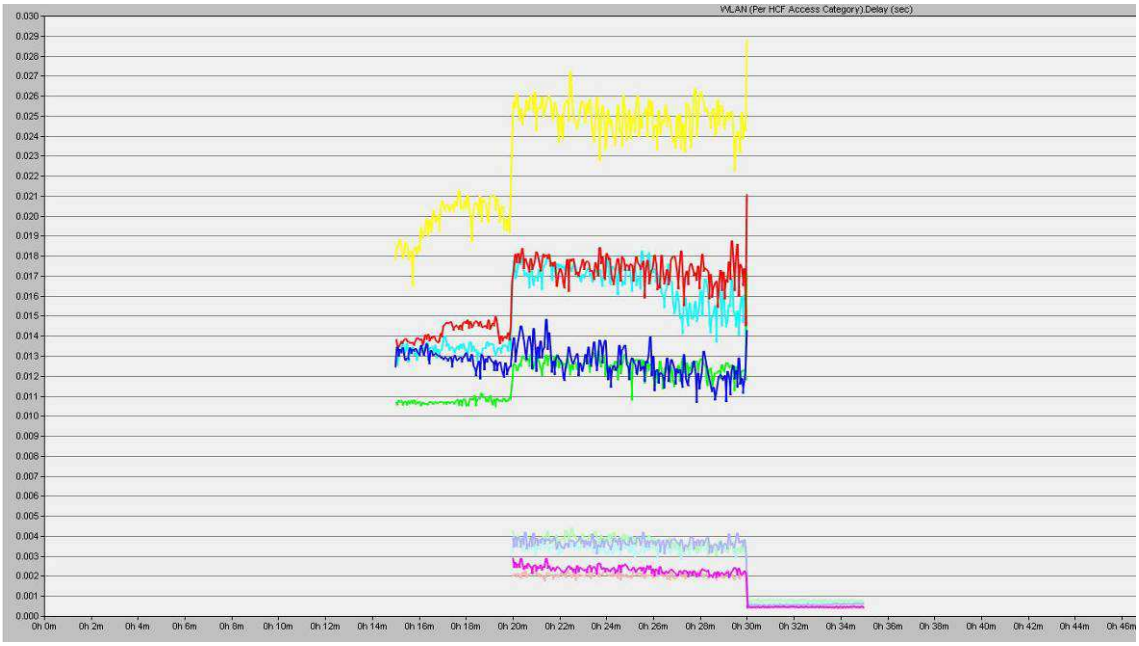
Teoreticky nejhorší kombinace rušení, tedy umístění vedle sebe dvou přístupových bodů pracujících na stejném kanálu (žlutá), se podle simulace jeví stejně, jako rušení vzdáleným přístupovým bodem pracujícím na jiném kanálu (červená). To se stalo i v případě přenosu videa. Tam se však jednalo o nejhorší případy, na rozdíl od přenosu hovoru. Zde patří hodnoty zpoždění k těm nižším (hodnoty zpoždění se pohybují od 22 do 35 ms).

Podle těchto parametrů by měla být kvalita hovoru stále vyhovující. Problém však nastane, vezmeme-li v úvahu ještě ztrátovost. Ta v případě rušení druhým přístupovým bodem na stejném kanálu dosáhla hodnoty 9 %, a při umístění obou přístupových bodů blízko u sebe ztrátovost vzrostla dokonce na 16 %. Tyto hodnoty se pohybují vysoko nad tolerancí uvedenou v Tab. 2 a kvalita hovoru se tak stává nevyhovující.

Rušení tak negativně působí nejen na zvětšení zpoždění nebo jeho kolísání, ale značný vliv má i na ztrátovost paketů, což se negativně projeví na přenosové rychlosti a tím i propustnosti sítě.

8.2 Rušení sítě standardu 802.11g

Rušení je prováděno stejně jako v případě rušení sítě standardu 802.11b, to znamená, že byla vytvořena ještě jedna bezdrátová síť, využívající stejný standard. Tato síť obsahuje opět čtyři klientské stanice, které jsou připojeny k přístupovému bodu a během simulace stahují data z druhého FTP serveru. Stejně jako v předchozím případě i zde se testovalo rušení jak na různých, tak na stejných kanálech a přístupové body byly opět buď hned vedle sebe, nebo opodál. Výsledky by tedy teoreticky měly vypadat podobně.



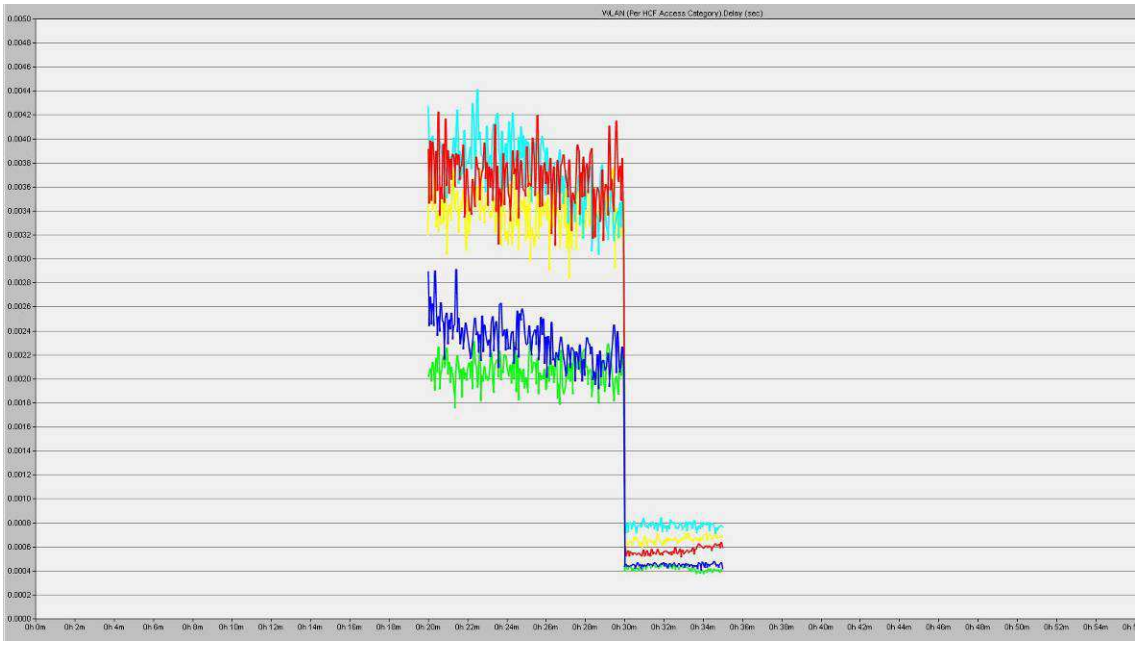
Obr. 19: Zpoždění v síti 802.11g pro přenos videa a videohovoru při rušení okolím

Z uvedeného grafu (Obr. 19) opět vyplývá, že rušení má negativní vliv na zpoždění v síti, i když na začátku přenosu videa, kdy ještě není zahájen videohovor, je zpoždění při přenosu videa v rušené a nerušené (modrá) síti téměř stejné (13 ms). Po jeho zahájení ale zpoždění v zarušené síti vzroste na 16 – 18 ms, na rozdíl od sítě, která není rušena. Poněkud překvapivě se už na první pohled jeví zelená křivka, která odpovídá zpoždění v síti, rušené blízko umístěným druhým přístupovým bodem a pracujícím na jiném kanálu. Zpoždění před zahájením videohovoru je v tomto případě menší než v nezarušeném prostředí. Po zahájení hovoru jsou pak hodnoty zpoždění srovnatelné.

Jako nejhorší kombinace rušení vyšel případ, kdy byly oba přístupové body ve své blízkosti a oba pracovaly na stejném kanálu. Zpoždění se v tomto případě zpočátku pohybovalo od 18 do 20 ms, po zahájení hovoru pak zpoždění vzrostlo na 24 – 27 ms. Kolísání zpoždění bylo tedy 2 – 3 ms.

Zpoždění přenosu hovoru je podle předpokladů nižší, než zpoždění při přenosu videa. A to z důvodu vyšší priority tohoto datového toku. Podle předpokladů je zpoždění v zarušených sítích, stejně jako při přenosu videa, o něco vyšší, kolísání poždění však nevykazuje zásadní rozdíly a je stále menší než v případě přenosu videa.

Zpoždění pro přenos dat z FTP serveru dosahovalo zpoždění v řádu stovek milisekund, nikdy však průběh nepřekročil jednu sekundu. Rovněž jeho kolísání bylo mnohem větší, než kolísání v případě přenosu videa. V souhrnném grafu (Obr. 19) tedy tyto průběhy nejsou zobrazeny opět z důvodu lepší čitelnosti přenosů dat s vyšší prioritou.



Obr. 20: Zpoždění přenosu hovoru v síti 802.11g během rušení okolím

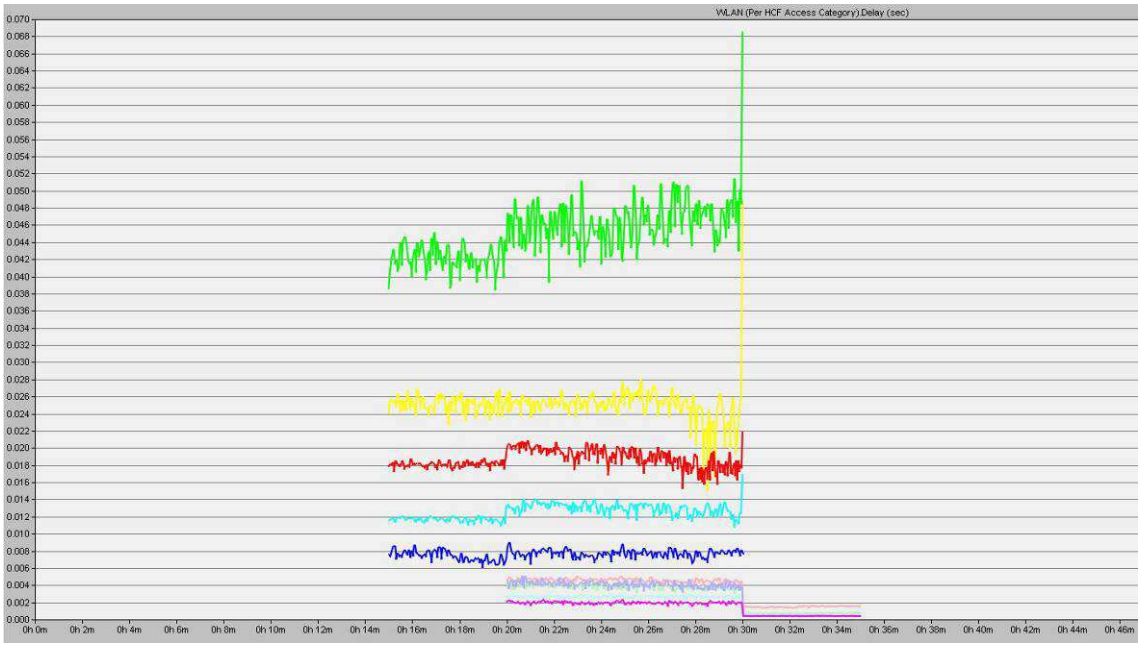
Obr. 20 ukazuje detailněji průběhy zpoždění pro přenos videohovoru. I v tomto případě měla zarušená síť, kdy byly oba přístupové body umístěny ve své blízkosti a pracovaly každý na jiném kanálu, menší zpoždění (2 ms) než síť v nezarušeném prostředí (2,5 – 3ms). Rozdíly jsou však minimální a dalo by se říct, že v reálném prostředí v podstatě bezvýznamné. Tento stav tedy pravděpodobně zapříčinilo vhodné rozmístění přístupových bodů a klientských stanic, kdy nedocházelo k záporným interferencím odražených vln v prostředí.

Ostatní zarušené sítě již měly hodnoty zpoždění vyšší než původní nezarušená síť a pohybovaly se kolem 4 ms. Rozdíly ve zpoždění činily maximálně 1 ms. Po ukončení přenosu videa pak zpoždění kleslo ve všech případech pod 1 ms.

Ztrátovost se ve všech případech rušení pohybovala mezi 0,6 a 1,5 %. Kvalitu hovoru tak lze podle Tab. 2 ve všech případech označit jako vyhovující.

8.3 Rušení sítě standardu 802.11a

Tento standard má přenosovou rychlost shodnou se standardem 802.11g, ale odlišuje se především použitou frekvencí, na níž přenos probíhá. Výsledky simulací tak ukáží nejen rozdíly ve zpoždění u rušené a nerušení sítě, ale bude možné přímo porovnat, který z obou kmitočtů je pro přenos dat vhodnější. Podmínky simulací jsou totožné s předchozími případy, takže rušení bude probíhat jak na stejném tak i na odlišném kanálu a stejně tak se bude porovnávat rušení přístupovým bodem umístěným v různých vzdálenostech. Výsledky simulací jsou znázorněny v následujícím grafu.



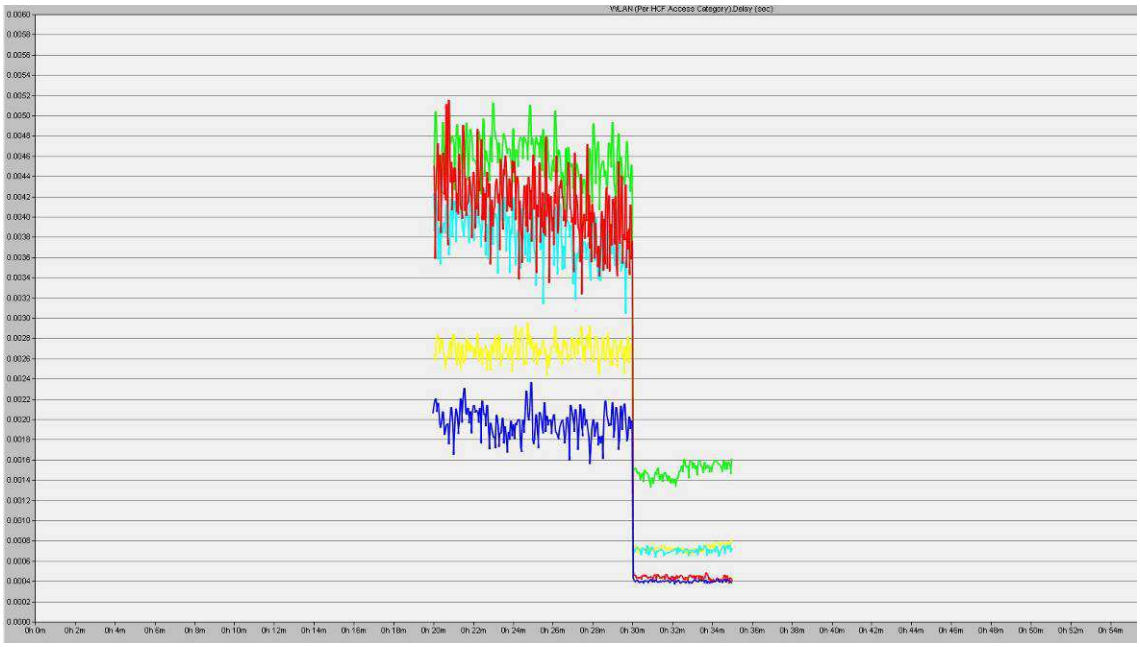
Obr. 21: Zpoždění v síti 802.11a pro přenos videa a videohovoru při rušení okolím

Výsledky opět ukazují, že nerušené sítě mají menší zpoždění a to jak u přenosu videa (modrá), tak při přenosu hlasu (sytě fialová). Přenos hlasu má rovněž ve všech případech nižší zpoždění i jeho kolísání. Priorita přenosu dat byla tedy zachována.

Jak už bylo řečeno, při přenosu videa měla nejnižší zpoždění síť, která nebyla rušena žádnou okolní sítí. Hodnoty zpoždění se pohybovaly mezi 7 a 9 ms. Naopak největší zpoždění měl případ, kdy byly oba přístupové body umístěny ve své blízkosti a pracovaly na různých kanálech. Hodnoty tohoto zpoždění se pohybovaly v rozmezí od 40 do 45 ms a po zahájení přenosu hovoru pak stouply na 45 – 50 ms. V případě, kdy

byly oba přístupové body ve vzájemné blízkosti a zároveň pracovaly na stejném kanálu (žlutá), byly hodnoty zpoždění o něco nižší a pohybovaly se kolem 25 ms.

Zajímavý rozdíl od předchozích standardů je, že při přenosu videa nedochází k téměř žádnému skokovému navýšení zpoždění (nebo jen minimálnímu), jakmile je zahájen přenos hovoru. U předchozích standardů byl tento skok vždy jasně zřetelný. Zahájení přenosu videohovoru tak v tomto případě neměl na zpoždění přenosu videa příliš velký vliv.



Obr. 22: Zpoždění přenosu hovoru v síti 802.11a během rušení okolím

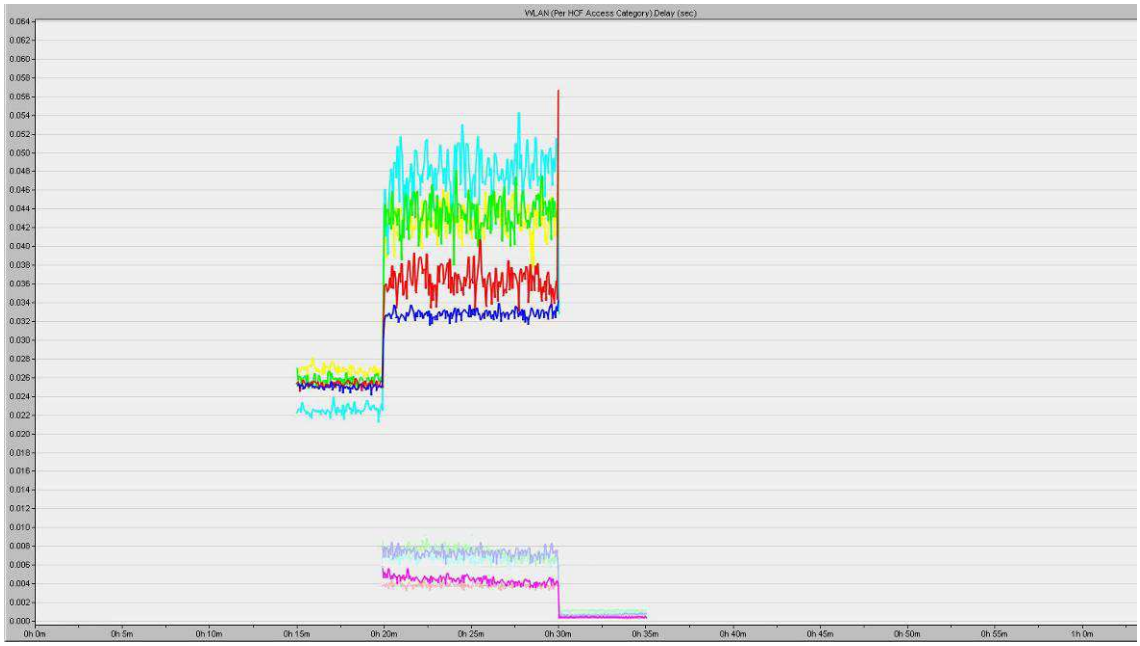
Z průběhů zpoždění na Obr. 22 zobrazujících detailnější pohled na zpoždění přenosu hlasu vyplývá, že nejmenší zpoždění měl opět přenos dat v nerušené síti (modrá), kdy se hodnoty zpoždění pohybovaly kolem 2 ms a rozdíly ve zpoždění byly nejvýše 1 ms. Největší zpoždění měl opět případ, kdy vedle sebe pracovaly dva přístupové body s jiným vysílacím kanálem (zelená), kdy hodnoty zpoždění kolísaly mezi 4 a 5 ms. Podobně na tom byly se zpožděním i sítě, u kterých docházelo k rušení vzdálenějšími přístupovými body pracujícími na stejném (světle modrá) nebo různém (červená) kanálu, kolísání zpoždění pak bylo maximálně 1,5 ms. Po ukončení přenosu videa všechny hodnoty zpoždění klesly a kromě zeleného průběhu se dostaly pod 1 ms.

Ztrátovost přenosu hlasu byla v případě nerušené sítě 1,38 % a v případě rušení sítě blízko umístěným druhým přístupovým bodem na jiném kanálu byla 1,29 %. V těchto případech lze tedy označit kvalitu hovoru podle Tab. 2 jako vyhovující. V ostatních případech se ztrátovost pohybovala na úrovni 1,9 % a v případě rušení

vzdáleným přístupovým bodem pracujícím na odlišném kanálu dosáhla ztrátovost dokonce 2,8 %. Kvalita hovoru tak již byla z tohoto důvodu nevyhovující.

8.4 Rušení sítě standardu 802.11n

Standard 802.11n je nejnovější dnes používaný standard. Jak už bylo zmíněno, jeho hlavní výhodou je navýšení přenosových rychlostí. To bylo dosaženo díky technologii MIMO, kde se datový tok dělí na několik dílčích toků, které se vysílají prostorově oddělenými kanály. Případné vzájemné rušení mezi těmito kanály se eliminuje výpočty na základě průběžně zasílaných testovacích bitů a fázových rozdílů mezi jednotlivými signály. Rušení okolím by tedy na přenos dat nemělo mít takový vliv, jako v předchozích případech. Topologie je téměř shodná s předchozími sítěmi. Jediným rozdílem je počet koncových stanic, který byl ještě o dvě stanice navýšen, aby byla síť opět naplno zatížena. Způsoby rušení zůstaly stejné jako v předchozích případech.



Obr. 23: Zpoždění přenosu videa a hovoru v síti 802.11n při rušení okolím

Výsledky této simulace opět ukazují, že přenos hlasu má vždy menší zpoždění než přenos videa a priorita přenosu tak byla zachována. Zpoždění při přenosu ostatních dat bylo řádově větší a dosahovalo až jednotek sekund. Tyto průběhy zde nejsou znázorněny, stejně jako v předchozích případech, z důvodu větší přehlednosti ostatních přenosů.

Výsledky průběhů zpoždění přenosu videa ukazují, že nejmenší zpoždění bylo, podle předpokladů v síti, která nebyla rušena okolními sítěmi (modrá). Hodnoty tohoto

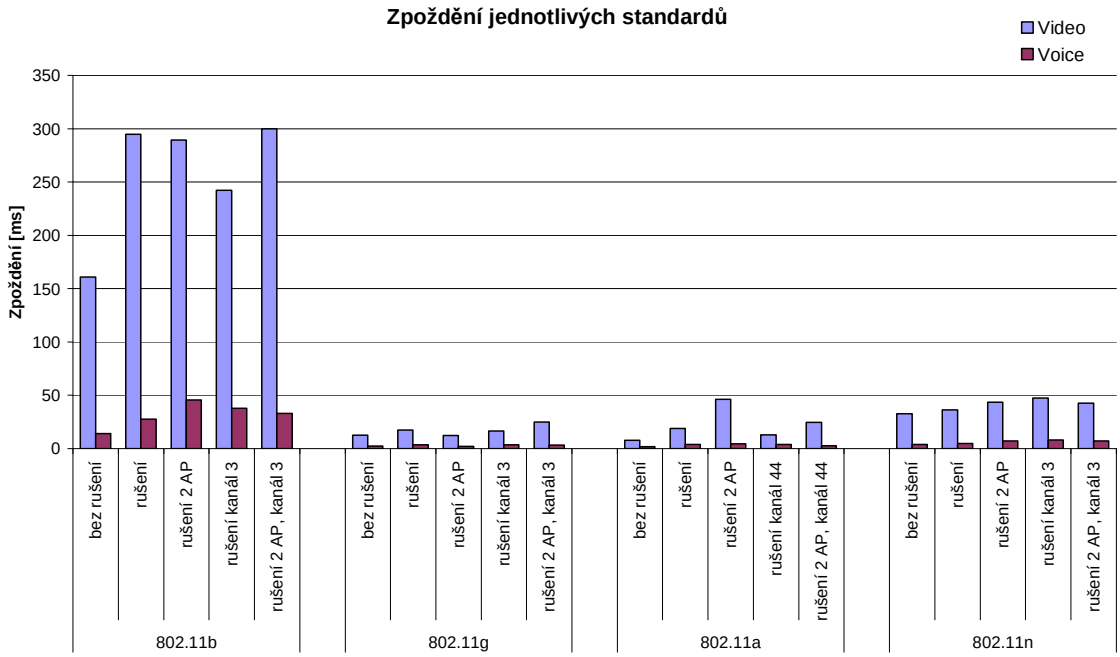
zpoždění se pohybovaly od 25 ms před spuštěním videohovoru, do 33 ms po jeho spuštění. Největší zpoždění bylo naopak naměřeno v síti, která byla rušena vzdáleným přístupovým bodem, pracujícím na stejném kanálu (azurová). Toto zpoždění se pohybovalo v rozmezí 23 – 52 ms. Za skokový nárůst zpoždění mohlo opět spuštění videohovoru. Zpoždění u ostatních zarušených sítí se pohybovalo mezi 24 a 26 ms, po spuštění hovoru pak mezi 34 a 40 ms v síti, která byla rušena vzdáleným přistupovým bodem pracujícím v jiném kanálu (červená). Zpoždění v síti rušené buďto blízkým přístupovým bodem na jiném kanálu (zelená) nebo vzdáleným přístupovým bodem na stejném kanálu (žlutá) se pohybovalo zpočátku v rozmezí 25 – 27 ms, po spuštění videohovru pak vzrostlo na 40 – 46 ms. Rozdíly ve zpoždění byly opět nejnižší v nezarušené síti (2 ms). Naopak největší rozdíly pak byly v síti rušené vzdáleným přístupovým bodem, pracujícím na stejném kanálu (azurová).

Obr. 24: Zpoždění při přenosu hovoru v síti 802.11n

Zpoždění při přenosu hlasu bylo opět nejmenší v nezarušené síti (modrá), kde dosahovalo hodnoty 4 ms. Největší zpoždění pak měl opět případ sítě rušené vzdáleným přístupovým bodem, pracujícím na stejném kanálu (azurová). Zde se hodnoty zpoždění pohybovaly mezi 8 a 9 ms. Přibližně o 1 ms menší zpoždění vykazovaly sítě rušené blízkým přístupovým bodem na jiném kanálu (zelená) nebo vzdáleným přístupovým bodem na stejném kanálu (žlutá). Kolísání zpoždění pak bylo opět nejmenší v nerušené síti (modrá), kde byly rozdíly ve zpoždění maximálně 1 ms. Největšího kolísání pak bylo zaznamenáno v síti rušené vzdáleným přístupovým bodem, pracujícím na stejném kanálu (azurová), kde byly rozdíly ve zpoždění 2 ms. Ztrátovost byla v případě nerušené sítě 0,4% a kvalitu hovoru tak lze podle tab. 2 označit jako dobrou. V ostatních případech se ztrátovost pohybovala do 1,5% a kvalita hovoru tak byla vyhovující.

8.5 Celkové srovnání všech standardů

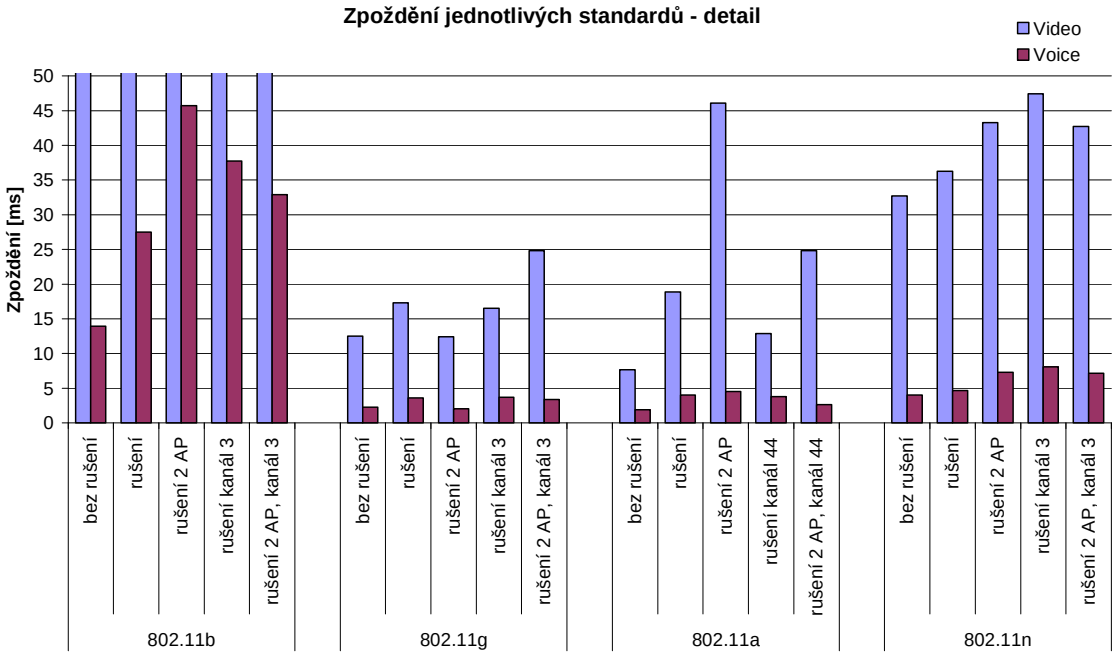
Zpoždění a jeho kolísání jsou nejdůležitějšími parametry při přenosu multimediálních dat sítí. V předchozích částech práce bylo demonstrováno, že aplikování mechanizmů na třídění provozu sítí podle typu přenášených dat (označováno jako QoS) má právě na zpoždění velmi pozitivní vliv napříč všemi standardy z rodiny standardů 802.11. Následující grafy porovnávají výsledné hodnoty zpoždění při přenosu multimediálních dat v předchozích simulacích mezi jednotlivými standardy 802.11 a/b/g/n.



Obr. 25: Porovnání zpoždění mezi jednotlivými standardy 802.11 a/b/g/n

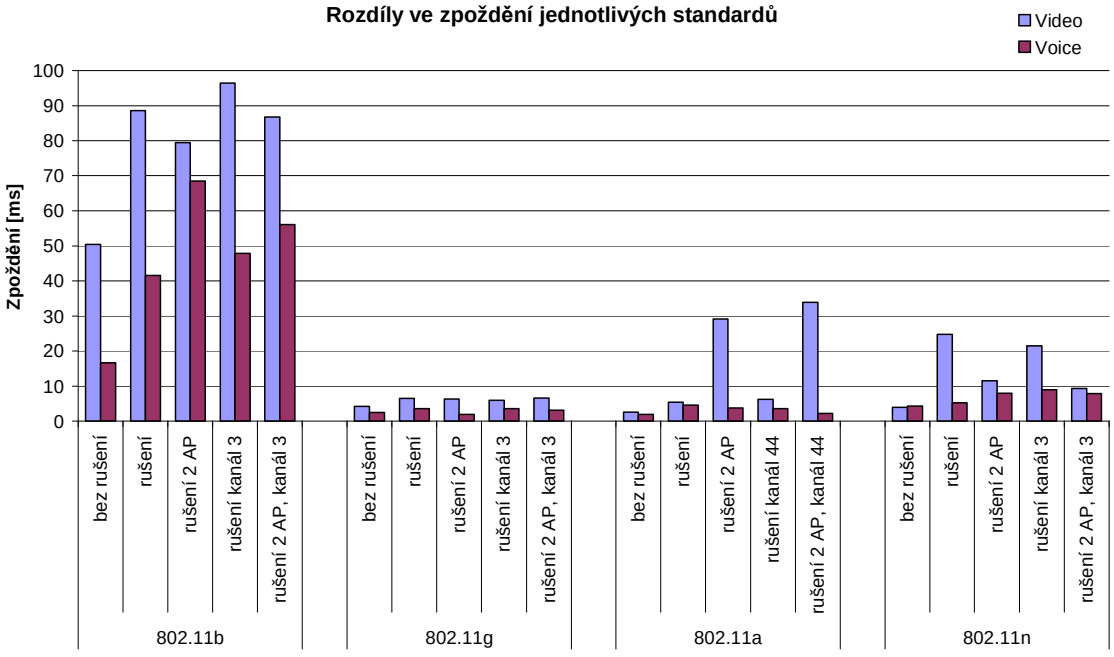
Z výsledného grafu zobrazující zpoždění je jasně patrné, že zdaleka největší zpoždění bylo naměřeno u standardu 802.11b. I v případě, že síť nebyla rušena jinou sítí, což je v dnešní době všudypřítomných bezdrátových sítí vzácné, byly hodnoty zpoždění vyšší, než u ostatních standardů a to i v případě jejich rušení okolím. Tento standard má i nejmenší přenosovou rychlost ze všech a pro přenos dat ho tak již nelze příliš doporučit. Není se však čemu divit, neboť tento standard je ze všech nejstarší.

Většina dnes používaných zařízení je schopna pracovat i se standardem 802.11g, který pracuje na stejné frekvenci, je zpětně kompatibilní, má mnohem vyšší přenosovou rychlost, a i zpoždění při přenosu dat je mnohem menší.



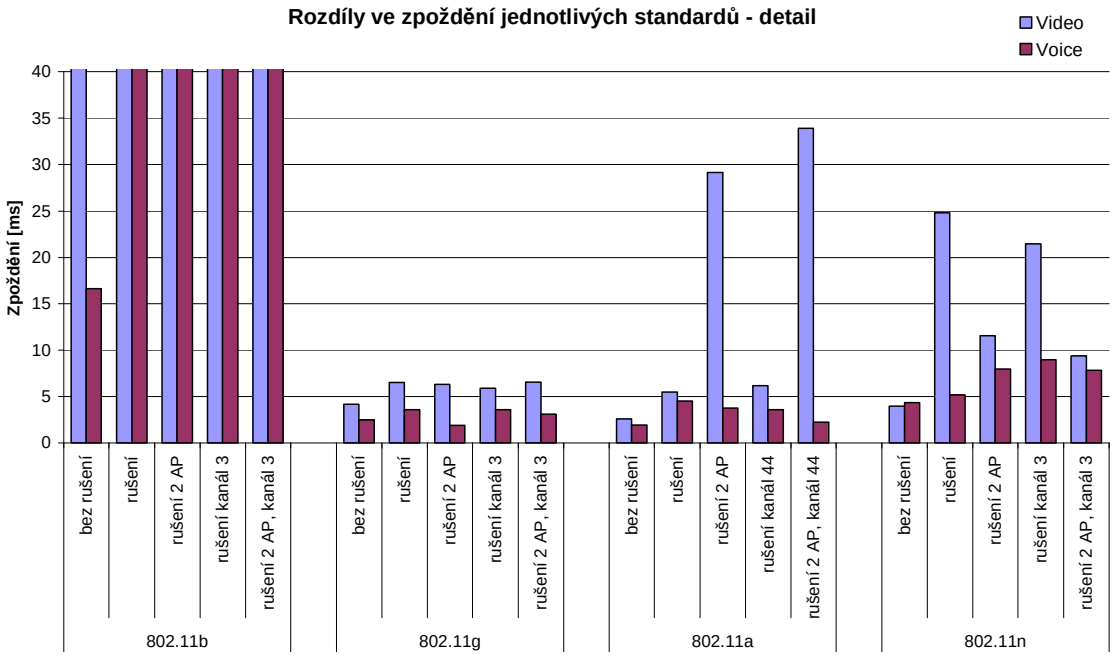
Obr. 26: Porovnání zpoždění mezi jednotlivými standardy 802.11 a/b/g/n - detail

Z detailního pohledu na výsledky měření je vidět, že má dokonce o trochu menší zpoždění než nejnovější standard 802.11n. Větší zpoždění u sítě standardu 802.11n je s největší pravděpodobností způsobeno větší výpočetní náročností technologie MIMO. Ve všech zbylých případech je však zpoždění při přenosu videa menší než 50 ms, při přenosu hlasu pak zpoždění není vyšší než 8 ms, což pro kvalitní přenos vyhovuje.



Obr. 27: Porovnání kolísání zpoždění mezi jednotlivými standardy 802.11 a/b/g/n

Při srovnání rozdílů ve zpoždění (obr. 27) je vidět, že nejvyšší jsou tyto opět v případě přenosu dat pomocí standardu 802.11b. Při přenosu videa se pohybovaly od 50 ms v nezarušené síti do 100 ms v síti rušené. Při přenosu hlasu byly výkyvy ve zpoždění nižší a hodnoty se pohybovaly od 18 ms (bez rušení) do 70 ms. I z tohoto hlediska tedy nelze standard 802.11b k přenosu multimediálních dat doporučit. Ostatní standardy mají rozdíly ve zpoždění mnohem menší. Standard 802.11a je však náchylný na rušení blízko umístěnými přístupovými body, kdy rozdíly ve zpoždění v případě přenosu videa dosáhly 30 ms.



Obr. 28: Porovnání kolísání zpoždění mezi jednotlivými standardy 802.11 a/b/g/n - detail

Z detailnějšího pohledu na výsledky kolísání zpoždění jednotlivých standardů je vidět, že nejmenší výkyvy ve zpoždění dosáhl standard 802.11g, kdy nebyly rozdíly větší než 4 ms v nezarušeném prostředí a 6 ms v prostředí zarušeném. Rozdíly ve zpoždění při přenosu hlasu pak nepřekročily 4 ms. Zcela nejmenší výkyvy ve zpoždění pak byly v případě přenosu hlasu pomocí standardu 802.11a v nezarušeném prostření, kdy výkyvy nebyly větší než 3 ms. Okolní rušení se na kolísání zpoždění při přenosu hlasu nijak znatelně neprojevilo. Zvýšily se však výkyvy ve zpoždění při přenosu videa, které dosáhlo až 35 ms v případě rušení.

Z celkového pohledu, a to i v případě porovnání kolísání, zpoždění nejlépe vychází standard 802.11g, který vykazuje nejmenší náchylnost na rušení okolními sítěmi a rozdíly ve zpoždění se pak mění pouze o několik ms.

Z celkového pohledu na dnes používané standardy se jeví jako nejlepší volba použití nejnovějšího z nich, tedy standardu 802.11n. Hodnoty zpoždění i jeho kolísání sice byly o několik milisekund vyšší než v případě staršího standardu 802.11g, je však třeba vzít v potaz i přenosovou rychlost, která je mnohem vyšší než v případě starších standardů. Díky tomu nedochází tak často k přetížení sítě a tedy i k nadměrnému prodlužování vstupních a výstupních front v jednotlivých rozhraních a následnému zahazování paketů v důsledku přetečení paměti. Většina dnes prodávaných přístupových bodů má navíc tento standard již standardně implementován.

V případě standardu 802.11n je však třeba klást větší pozornost ohledně rušení okolními sítěmi a tomuto jevu se pokud možno vyhnout. Z výsledků simulací totiž vyplývá, že standard 802.11n je více náchylný na rušení než starší standard 802.11g.

9 Závěr

Počítačové sítě hrají v moderním světě stále větší roli a to nejen díky tomu, že objem dat přenesených po těchto sítích neustále roste. Počítačové sítě se začínají stále více využívat i pro telekomunikační služby, které dříve využívaly svou vlastní síťovou infrastrukturu. Typickým příkladem může být přechod telekomunikačních služeb ze sítí pracujících na bázi přepojování okruhů na spojení paketové. Má to své výhody, protože díky efektivnějšímu využití síťových prostředků přenosová kapacita sítě není zbytečně blokována i v tom případě, že nic nepřenáší. Nevýhodou však je, že během přenosu dat sítí může dojít k většímu zpoždění a telefonní hovor tím značně zkomplikovat. Do sítí je tak aplikován mechanizmus, který zajišťuje určitou kvalitu služby a provoz sítí na základě priorit upřednostňuje.

Poslední dobou rovněž roste význam bezdrátových sítí, a to zejména díky velkému rozmachu chytrých mobilních telefonů a tabletů. Tyto sítě mají nejen nižší přenosovou kapacitu, ale jsou mnohem náchylnější na rušení okolním prostředím. K většímu zpoždění a ke ztrátám dat v nich dochází mnohem snadněji než u klasických kabelových sítí. Využití kvality služeb u těchto sítí tak rovněž najde své opodstatnění.

Simulace sítí s podporou QoS uvedené v této práci jasně dokazují vliv použití QoS na síťový provoz a to napříč všemi standardy 802.11 a/b/g/n. Telefonní hovor, mající nejvyšší prioritu, byl skutečně vždy upřednostněn před ostatním provozem a výsledné zpoždění bylo v toleranci pro dobrou kvalitu hovoru. Naopak přenos dat z FTP serveru, který měl nejnižší prioritu, byl pokaždé přesunut na pozadí a během využití sítě přenosem hovoru a videa téměř žádná komunikace neprobíhala až do doby uvolnění sítě provozem s vyšší prioritou. Telefonní hovor tak probíhal bez problémů a kvalita služby tak vždy byla dodržena.

V další části práce byly provedeny simulace sítí jednotlivých standardů, které podléhaly rušení okolními sítěmi. Toto rušení se až na jednu výjimku vždy negativně podepsalo na výsledném zpoždění i jeho kolísání. Kvalita služeb byla zachována a přenos hlasu, který měl nejvyšší prioritu, měl nejmenší zpoždění i rozdíly ve zpoždění. Naopak přenos dat z FTP serveru měl zpoždění zdaleka nejvyšší a často docházelo i k výpadkům spojení.

Ukázalo se tedy, že implementace QoS do sítí má své opodstatnění napříč všemi standardy a to tím víc, čím menší přenosovou kapacitu má daná síť. Čím je přenosová kapacita menší, tím dříve dojde k zahlcení sítě a tedy k potřebě upřednostňování datových toků s vyšší prioritou před těmi ostatními.

Dalším důvodem k nasazení QoS do sítí je vzájemné rušení bezdrátových sítí. Čím je rušení vyšší, tím dochází k větší chybovosti a tedy i ztrátovosti přenášených dat. To vede ke zpomalování přenosu dat a většímu vytížení sítě. Zcela se vyhnout rušení je však v dnešní době téměř nemožné.

Z našich simulací vychází, co se zpoždění týče, nejlépe standard 802.11g, z obecného hlediska je však výhodnější využití standardu 802.11n. Ten má sice o několik milisekund horší zpoždění a je náchylnější na rušení okolím (i když v případě přenosu hlasu nejsou rozdíly ve zpoždění větší než 5 ms), má však několikanásobně vyšší přenosovou rychlost a dokáže tak přenést větší množství dat aniž by došlo k přetížení sítě a tedy nutnosti upřednostňování provozu. Bude tak možné déle přenášet i data z FTP serveru vyšší rychlostí, případně obsloužit více hovorů nebo přenosů videa s odpovídající kvalitou služby.

Seznam použité literatury:

[1] BOUŠKA, P. Cisco QoS 1 - úvod do Quality of Service a DiffServ. [online]. [cit. 2013-11-20]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-qos-1-uvod-do-quality-of-service-a-diffserv/

[2] CESNET. *SIP*. [online]. [cit. 2013-11-20]. Dostupné z: http://sip.cesnet.cz/cs/protokoly/sip

[3] ČÍKA, P. *Multimediální služby*. Vyd. 1. Brno: Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací, 2012. ISBN 978-80-214-4443-0.

[4] DAŘÍLEK, M. *Standardy 802.11e a 802.11i*. Dostupné z: http://www.cs.vsb.cz/grygarek/TPS/projekty/0506Z/tps_dar022.pdf

[5] HON, P. *Jak funguje řízení datových toků s QoS*. Živě.cz [online]. [cit. 2013-11-20]. Dostupné z: http://connect.zive.cz/clanky/jak-funguje-rizeni-datovych-toku-s-qos/sc-320-a-161738

[6] JEŘÁBEK, J. *Komunikační technologie*. Vyd. 1. Brno: Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. ISBN 978-80-214-4713-4.

[7] LEDVINA, J. *QoS v datových sítích, IntServ a DiffServ*. Dostupné z: http://www.kiv.zcu.cz/~ledvina/Prednasky-PSI-2007/qos-text.pdf

[8] MOLNÁR, K. *Hardware počítačových sítí*. Vyd. 1. Brno: Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací, 2012. ISBN 978-80-214-4449-2.

[9] MOLNÁR, K. *Konfigurace zajištění kvality služeb*. [online]. [cit. 2013-11-20]. Dostupné z: http://www.utko.feec.vutbr.cz/~molnar/bhws/Lab_uloha-10-QoS_ver03.pdf

[10] NOVOTNÝ, V. *Architektura sítí*. Vyd. 1. Brno: Vysoké učení technické v Brně Fakulta elektrotechniky a komunikačních technologií Ústav telekomunikací, 2012. ISBN 978-80-214-4450-8.

[11] PASNET. *Služby QoS (Quality of Services)*. Pasnet [online]. [cit. 2013-11-20]. Dostupné z: http://www.pasnet.cz/sluzby-qos

[12] PUŽMANOVÁ, R. *802.11g: rychlejší WiFi?*. Lupa.cz [online]. [cit. 2013-11-20]. Dostupné z: http://www.lupa.cz/clanky/802-11g-rychlejsi-wifi/

[13] ŠEBESTA, V. *Teorie sdělování.* Brno: VUTIUM, 1998. 92 s. ISBN 80-214-1247-X.

[14] ŠLINZ, Petr. *Problematika vysokého zatížení bezdrátových sítí standardu 80.211b/g*. Dostupné z: is.muni.cz/th/208329/fi_m/thesis.pdf. Diplomová práce. Masarykova univerzita. [MUNI]

[15] VILLALÓN, J, GARRIDO, A, OROZCO-BARBOSA, L a CUENCA, P. *A QoS mechanism for multimedia communications over heterogeneous 802.11/802.11e WLANs.* [online]. [cit. 2013-11-20]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0140366408004209

Přehled použitých zkratek:

AIFS	Arbitration Inter-Frame Space
BPSK	Binary Phase Shift Keying
CBQ	Class Based Queing
CCK	Complementary Code Keying
CSMA/CA	Carier Sense Multiple Access with Colision Avoidance
CSMA/CD	Carier Sense Multiple Access with Colision Detection
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DiffServ	Differentiated Services
DQPSK	Differential Quadrature Phase Shift Keying
DSCP	Diffserv Code Point
DSSS	Direct Sequence Spread Spectrum
EDCF	Enhanced Distributed Coordination Function
EPCF	Enhanced Point Coordination Function
EWC	Enhanced Wireless Consortium
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
GFSK	Gaussian Frequency Shift Keying
HCF	Hybrid Coordination Function
HTML	HyperText Markup Language
HTTP	Hyper Text Transfer Protocol
IntServ	Integrated Services
IP	Internet Protocol
IPTV	Internet Protocol Television
MAC	Media Access Control
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
PCF	Point Coordination Function
PHB	Per Hop Behavior
PQ	Priority Queing
QoS	Quality of Service
QPPB	QoS Policy Propagation via BGP
QPSK	Quadrature Phase Shift Keying
RSVP	Resource reServation Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol

SAP	Session Announcement Protocol
SDP	Session Descrition Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TOS	Type Of Service
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VoWIP	Voice over Wireless IP
WFQ	Weighted Class Queing
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Seznam příloh: