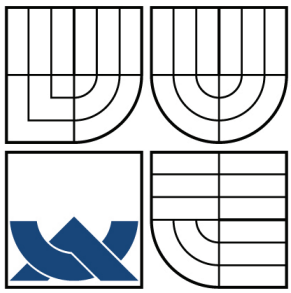
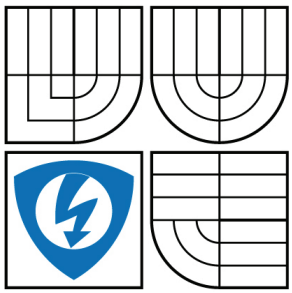


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ŘEŠENÍ PROBLEMATIKY ZAJIŠTĚNÍ KVALITY SLUŽEB V BEZDRÁTOVÝCH SÍTÍCH

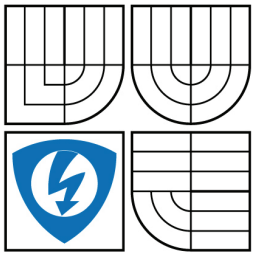
ANALYSIS OF QUALITY OF SERVICE ASSURANCE IN WIRELESS NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — TOMÁŠ HORNYAK
AUTHOR

VEDOUCÍ PRÁCE — Ing. JIŘÍ HOŠEK
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Tomáš Hornyak ***ID:*** 73028
Ročník: 3 ***Akademický rok:*** 2008/2009

NÁZEV TÉMATU:

Řešení problematiky zajištění kvality služeb v bezdrátových sítích

POKYNY PRO VYPRACOVÁNÍ:

Podrobně se seznamte s možnostmi zajištění kvality služeb (QoS) v bezdrátových sítích. Zaměřte se zejména na standard 802.11e. Dále se seznamte s technologií pro zajištění mobility v IP sítích (Mobile IP). V simulačním prostředí Opnet Modeler vytvořte model bezdrátové sítě, na kterém ověřte možnosti součinnosti obou technologií. Zdokumentujte případné problémy při použití mobilní IP adresy v bezdrátových sítích využívajících QoS mechanizmy.

DOPORUČENÁ LITERATURA:

[1] GAST, M.: 802.11 Wireless Networks: The Definitive Guide, Second Edition. Sebastopol: O'Reilly Media, 2005, ISBN: 978-0596100520.
[2] PRASAD, N., PRASAD, A.: 802.11 WLANs and IP Networking: Security, QoS, and Mobility. London: Artech House Publishers, 2005, ISBN: 1580537898.
[3] RAAB, S., CHANDRA, M.: Mobile IP Technology and Applications. Indianapolis: Cisco Press, 2005, ISBN: 978-1587051326.

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

Vedoucí práce: Ing. Jiří Hošek

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

UPOZORNĚNÍ:

Anotace

Tato práce se věnuje především možnostem zajištění kvality služeb a realizaci mobility v bezdrátových sítích. Zabývá se především možnostmi standardu IEEE 802.11e, využitelností protokolu Mobile IPv4 a počítačovou simulací jejich vzájemné součinnosti v prostředí OPNET Modeleru 12.0.

V první části je představen standard IEEE 802.11e, který je nejprve z teoretického hlediska rozebrán. Následuje podrobný popis standardu IEEE 802.11e, jeho jednotlivých součástí a možností implementace pokročilých technologií přístupu k médiu, které standard obsahuje. V této části jsou stručně nastíněny i jednotlivé výhody a nevýhody původních přístupových metod bezdrátových sítí standardů IEEE 802.11.

Další část práce se zabývá teoretickým rozborem zajišťování mobility v IP sítích a implementací mobility v jednotlivých vrstvách modelu ISO/OSI. Dále je zde představen protokol Mobile IPv4, který mobilitu v IP sítích realizuje. Je zde uveden princip tohoto protokolu, představeny jeho jednotlivé součásti a síťová architektura.

V další části je na základě teoretických poznatků v prostředí simulačního nástroje OPNET Modeler zkoumán vliv implementace standardu IEEE 802.11e na vybrané statistiky bezdrátové lokální sítě. Dále je sledován vliv zátěže v síti a jsou zde diskutovány modifikace standardu pro dosažení optimálních výsledků.

Poslední část se věnuje počítačové simulaci protokolu Mobile IPv4 v bezdrátových sítích. Dále je do funkčního modelu sítě implementována podpora standardu IEEE 802.11e a je zkoumána vzájemná součinnost obou technologií a případný výskyt jakýchkoli problémů. Pro porovnání je zde v prostředí OPNET Modeleru simulována i mobilita založená pouze na linkové vrstvě.

Klíčová slova: bezdrátová síť, IEEE 802.11e, kvalita služeb, Mobile IPv4, mobilita, OPNET Modeler, QoS, simulace

Abstract

This Bachelor thesis deals especially with possibilities of quality of service assurance and mobility implementation in wireless networks. It deals primarily with the possibilities of the IEEE 802.11e standard, with the applicability of the Mobile IPv4 protocol and with the computer simulation of their mutual coactions in the OPNET Modeler 12.0 environment.

In the first part of the thesis the standard IEEE 802.11e is first of all analysed from the theoretical point of view. It is followed by the detailed description of the IEEE 802.11e standard, its individual parts and implementation possibilities of advanced technologies of the access to the medium which are included in the standard. In this part even the individual advantages and disadvantages of the original access methods of wireless networks of IEEE 802.11 standards are briefly outlined.

Further part of this work deals with the theoretical analysis of mobility service assurance in the IP networks and with the mobility implementation in individual layers of the ISO/OSI models. Then the Mobile IPv4 protocol is presented here that carries out the mobility in the IP networks. The principle of this protocol is mentioned here and its individual components and the network architecture are presented.

In the next part, on the basis of theoretical pieces of knowledge in the environment of the OPNET Modeler simulation tool the effect of the standard IEEE 802.11e implementation is examined on the selected statistics of the wireless local network. Furthermore the effect of the load in the network is followed up and standard modifications are discussed here to reach optimum results.

The last part deals with the computer simulation of the Mobile IPv4 protocol in the wireless networks. Then the support of the IEEE 802.11e standard is implemented into the functioning network model and the reciprocal coactions of both technologies and a possible appearance of any problems are examined. For comparison, it is here in the OPNET Modeler environment even the mobility simulated which is based solely on the link layer.

Key words: IEEE 802.11e, Mobile IPv4, mobility, OPNET Modeler, QoS, quality of service, simulation, wireless network

HORNYAK, T. *Řešení problematiky zajištění kvality služeb v bezdrátových sítích.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 52 s. Vedoucí bakalářské práce Ing. Jiří Hošek.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma „Řešení problematiky zajištění kvality služeb v bezdrátových sítích“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny uvedeny v seznamu literatury na konci práce.

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

V Brně dne …….. .....

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Jiřímu Hoškovi za velmi užitečnou metodickou pomoc, cenné rady při zpracování práce, ochotu ke konzultacím a řadu užitečných rad k samotnému textu práce.

Dále děkuji Ing. Jiřímu Hoškovi a doc. Ing. Karolu Molnárovi, Ph.D. za ochotu pravidelně řešit problémy vzniklé při realizaci práce.

V Brně dne …….. .....

podpis autora

Obsah

1 Úvod

Za posledních několik let se ve světě začal významně klást důraz na mobilitu. Lidé zjistili, že dosavadní podoba sítí nedokáže plnit jejich měnící se požadavky. Pokud je totiž uživatel nucen být k síti připojen kabelem, jeho mobilita je výrazně omezena.

Naproti tomu díky bezdrátovému připojení je uživatel omezen pouze dosahem radiového signálu a v tomto prostoru se může volně pohybovat. Díky této nesporné výhodě nyní pronikají bezdrátová řešení do oblastí, které byly dříve striktně doménou klasického připojení pomocí kabelů.

Lze se domnívat, že jsme svědky skutečné změny v podobě počítačových sítí. Mobilní telefonie již v minulosti určila jistý standard, kterého se nyní mobilní počítače snaží dosáhnout.

Hlavní výhodou mobility je, že se uživatel může volně pohybovat. U zařízení určených k mobilní komunikaci však uživatel očekává, že pojem mobilita bude znamenat více, než možnost zařízení přenášet z místa na místo. Cílem mobility je mít zařízení schopné komunikace i během pohybu. Tyto zařízení tedy musí být plně funkční kdykoli a kdekoli budou uživatelem používány.

Současné komunikační schopnosti počítačových sítí rychle nahrazují proces tištěné a doručované korespondence. Vývoj internetu udělal z počítačů, původně určených pouze pro zpracovávání dat, zařízení pro multimediální komunikaci v reálném čase. Uživatelé začínají masově používat bezdrátové sítě (WLAN), protože chtějí být připojeni k internetu kdekoli a kdykoli zapnou počítač. Kromě počítačů se dnes vyvíjí celá řada zařízení jako chytré telefony, tzv. PDA, samostatné navigační systémy atd. Všechna tato zařízení nyní potřebují komunikovat v reálném čase. To ale s sebou nese jistou potřebu kontroly nad procesem přenosu dat. S přenášením hlasu, nejdůležitější služby již od počátků komunikačních sítí, byl v sítích založených na paketovém přenosu dat vždy problém. Implementace mechanizmů zajišťujících kvalitu služeb však umožňuje bezproblémovou hlasovou komunikaci v reálném čase.

Bezdrátové sítě zažívají v poslední době prudký rozvoj, jsou zajímavou a perspektivní technologií v oblasti počítačových sítí a proto se jim jejich možnostem věnuje i tato práce. Dále bude řeč zvláště o standardu IEEE 802.11e (jako o možnosti zajištění kvality služeb) a o protokolu Mobile IPv4 (jako o prostředku pro realizaci mobility v IP sítích).

2 Standard IEEE 802.11e

2.1 Quality of Service

Pojem kvalita služby (Quality of Service, QoS) se v současnosti stává stále důležitějším prvkem každého moderního komunikačního systému. QoS znamená zajištění úplného a předvídatelného přenosu dat, jinými slovy také zajištění požadavků uživatelských aplikací. QoS zajišťuje jak služby neprobíhající v reálném čase tak také služby jako třeba přenos hlasu, které musí probíhat v reálném čase. A jelikož hlas je již od počátků komunikačních sítí nejdůležitějším přenášenou službou, je mu i zde věnována speciální pozornost.

Podpora hlasové komunikace přes IP (Internet Protocol) se označuje jako VoIP (Voice over IP). VoIP se dá definovat jako schopnost uskutečnit telefonní hovor (nebo také umožňovat vše, co nabízí PSTN (standardní veřejná telefonní síť)) přes datové sítě založené na IP (s patřičnou podporou QoS). Jelikož bezdrátové sítě rozšiřují IP protokol, je důležité mít protokol, který splní požadavky pro telefonní hovor. Tento protokol se označuje jako VoWLAN (Voice over WLAN)[2] a pro zajištění správného přenosu hlasu používá MAC (Media Access Control – řízení přístupu k médiu) podvrstvu doplněnou o QoS. Úkolem tohoto protokolu je přidat do bezdrátových sítí pracujících na IP protokolu schopnost provést telefonní hovor a propojit tyto sítě do veřejné telefonní sítě a soukromých hlasových sítí tak, aby byl zachován současný standard kvality hlasu a také funkce nabízené telefonem.

Hlas je služba probíhající v reálném čase, což znamená jistá omezení týkající se maximálního přípustného zpoždění přenosu. Bylo zjištěno, že hlavní vliv na kvalitu hlasové služby mají tyto tři faktory [2]:

- **Delay (zpoždění):** pokud mají pakety na cestě od jednoho účastníka telefonního hovoru k druhému zpoždění větší než 250 milisekund, neuslyší se účastníci navzájem včas a může docházet ke skákání si do řeči a tudíž ke zhoršení celkové kvality hovoru.

- **Jitter (proměnlivost zpoždění):** v počítačových sítích a převážně v sítích založených na protokolu IP jako je Internet, znamená jitter kolísání velikosti zpoždění paketů při průchodu sítí [3]. Jitter je způsoben různými celkovými zpožděními jednotlivých paketů procházejících sítí. Jeho odstranění je možné zachycením přijatých paketů a jejich „pozdržením“ po dobu nutnou k umožnění příchodu paketů s větším zpožděním a následným přehráním ve správném pořadí. Tato vyrovnávací paměť, umožňující odstranit (nebo alespoň potlačit) jitter, ale také přidává paketům určité zpoždění, se kterým je nutno počítat. O jitter se může postarat přístupový bod bezdrátové sítě (Access Point, AP). Pro tento účel musí AP implementovat plánovací schéma, které dokáže rozlišit rozdílné třídy služeb. Avšak tohoto rozlišování by nemělo být dosaženo „rozbalením“ paketu až po aplikační vrstvu, měly by existovat mechanismy pro určení třídy služeb již z hlavičky paketu.

- **Packet loss (ztrátovost paketů):** bezdrátové (a obecně IP sítě) nemohou zaručit, že všechny pakety budou doručeny k cíli (ještě méně že budou doručeny ve správném pořadí). Pakety jsou „zahazovány“ při přetíženích sítě. Do určité ztrátovosti paketů mohou být chybějící pakety vynechány nebo nahrazeny bez slyšitelného vlivu na kvalitu hovoru. Ztrátovost je problém kanálu. V případě IEEE 802.11 může být ztrátovost snížena snížením datového toku. Jelikož v IEEE 802.11b není použito opravování chyb Forward Error Correction (FEC), není zde

ani jiná možnost jak ztrátovost snížit. V případě IEEE 802.11a,g je již FEC použito, ale v kombinaci s modulací upravující datový tok.

2.2 Původní přístupové metody 802.11 MAC vrstvy

2.2.1 Distribuovaná koordinační funkce (Disttributed Coordination Function, DCF)

DCF je základní metoda přístupu k médiu podporující asynchronní přenos dat založený na principu best-effort (bez podpory QoS). Výhodou DCF je to, že stanice jsou při soutěžení o přístup k médiu rovnocenné, bohužel DCF nemá prostředky pro zaručení zpoždění pro stanice provozující časově vázané služby (např. hlas nebo video rozdělené do paketů – vyžadují minimální zpoždění). Teoreticky by sice bylo možné provozovat hlasové služby v oddělené síti s málo uživateli, ale za normálních podmínek (spousta stanic komunikujících pomocí hlasu i dat současně) je většinou kvalita telefonního hovoru velmi špatná. Rovnocennost je podporována tím, že se každá stanice musí znovu připojit ke kanálu po té, co odvysílá paket. Všechny stanice mají stejnou pravděpodobnost získat přístup ke kanálu po uplynutí jejich povinné doby čekání po zjištění nečinnosti na kanálu – mezirámcová mezera (DCF InterFrame Space, DIFS).

Jelikož DCF je základní přístupová metoda bezdrátových sítí standardu IEEE 802.11, je její podpora implementována ve všech zařízeních podporujících tento standard, tudíž kompatibilita s touto funkcí není problémem. Problémem DCF je nepřítomnost plánování a priorizace dat v AP a také ve stanicích. Toto může být například jednoduše vyřešeno zpožděním provozu ze stanic neběžícím v reálném čase a přidělením priority provozu v reálném čase. V AP se toto řeší zavedením metody cyklické obsluhy pro přenos paketů v reálném čase a přiřazením nízké priority paketům neběžícím v reálném čase.

Škálovatelnost, ve smyslu rozšiřování počtu stanic, které používají jedno AP, není u DCF problém. Standard nedefinuje maximální počet uživatelů kanálu, avšak přístup ke kanálu je založen na metodě CSMA/CA, což je metoda s vícenásobným přístupem a naslouchání nosné. Pokud tedy stanice před vysíláním zjistí, že je obsazeno, počká náhodnou dobu a sníží tak pravděpodobnost kolize [3]. Při větším počtu stanic, které se snaží vysílat ve stejný čas, tedy s použitím metody CSMA/CA celkové zpoždění v síti poroste. Také škálovatelnost ve smyslu několika AP používajících DCF není problém. Jednotlivé AP použijí odlišné kanály, a pokud by i tak docházelo k překrývání kanálů, metoda CSMA/CA se s tím vypořádá.

2.2.2 Centralizovaná koordinační funkce (Point Coordination Function, PCF)

PCF je volitelná přístupová metoda, která je spojově orientovaná a poskytuje přenos dat bez soutěžení o médium. Pro PCF je důležitý centralizovaný koordinátor (Point Coordinator, PC), který posílá rámce výzvy (POLL rámce) zajišťující stanicím možnost vysílat i bez soutěžení. PCF vždy existuje spolu s DCF, a tudíž dochází k pravidelnému střídání doby přístupu se soutěžením o médium (contention period, CP) a bez něj (contention-free period, CFP).

Existují tři problémy týkající se služeb v reálném čase a PCF. Prvním je nemožnost současného použití centralizovaného módu v sousedních „buňkách“ bezdrátových sítí, protože existuje jen málo nepřekrývajících se kanálů definovaných standardem IEEE 802.11 (je zde vysoká pravděpodobnost interference u sousedních buněk). Také jednotlivé AP nejsou časově synchronizovány a existuje zde možnost kolizí díky současnému startu CFP. Tento problém je znám jako problém překrývajících se buněk.

Za druhé, výsledkem protokolu CSMA/CA může být neschopnost PC převzít kontrolu nad kanálem při začátku CFP. Pokud stanice začne vysílat během DCF fáze a toto vysílání by trvalo déle než je doba zbývající do začátku příští CFP, PC musí své vysílání odložit do doby, než bude médium volné po PIFS. Toto zkracuje CFP a degraduje QoS.

Za třetí, PCF je založeno na centrální kontrole, ale právě velká režie vyúsťuje v nižší počet uskutečnitelných telefonních hovorů.

PCF je navíc ve standardu IEEE 802.11 volitelný prvek a většinou výrobců není vůbec zařazován. Realizace PCF nemusí být obtížná, ale dobrá realizace je komplikovaná kvůli řešení všech problému s touto funkcí spojených.

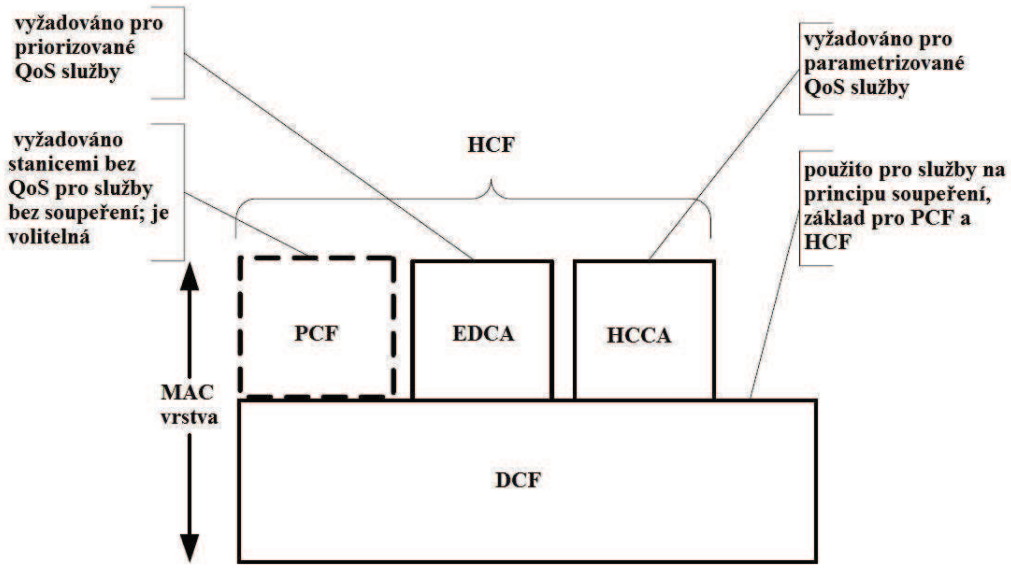
Jelikož je PCF definováno ve standardu, kompatibilita by neměla být problémem. Ale dobrá realizace může působit problémy s kompatibilitou.

PCF nepodporuje škálovatelnost [2].

2.3 QoS mechanismy standardu 802.11e

Původní protokoly 802.11 MAC vrstvy nemají žádné prostředky k rozlišení jednotlivých skupin dat nebo jejich zdrojů. Se všemi skupinami dat je v PCF i DCF zacházeno stejně (tzn. Stejná priorita přístupu ke kanálu). Datům s nároky na šířku pásma nebo zpoždění nemohou být jejich požadavky zaručeny. Pak může například datový provoz s nízkou prioritou úplně „ucpat“ datový tok videa a zhoršit tím jeho přijímanou kvalitu. Stanice pracující jako centrální koordinátor pro ostatní stanice uvnitř stejné QoS podporující BSS (QBSS) se nazývají hybridní koordinátory (HC). BSS (základní sada služeb) je základní infrastrukturní jednotka, která se skládá z jediného přístupového bodu připojujícího skupinu bezdrátových klientů k pevné síti [10]. Stejně jako PC, HC se nachází uvnitř AP podporujícího 802.11e. 802.11e rozšiřuje původní 802.11 MAC vrstvu o podporu aplikací s požadavky na QoS. Zařízení podporující QoS obsahují navíc koordinační funkci nazývanou hybridní koordinační funkce (HCF), která je použitelná pouze v QBSS. HCF kombinuje funkce DCF a PCF, navíc přidává další typy rámců a některé mechanismy specifické pro QoS zajišťující jednotné postupy výměny rámců při CP i CFP.

Jak ukazuje Obrázek 2.1 [2], HCF používá dvě metody přístupu k médiu. Jsou to metody EDCA (přístup k médiu na základě soutěžení) a HCCA (kontrolovaný přístup k médiu pro přenos bez soutěžení) [2]. HCF podporuje až 8 tříd pro prioritu provozu.



Obrázek 2.1 - Struktura IEEE 802.11e MAC vrstvy

2.3.1 EDCA

EDCA je založena na soupeření QoS stanic o přístup k médiu a poskytuje jim odlišný a rozdělovaný přístup k médiu. EDCA definuje mechanismus přístupových kategorií (access category, AC), který nabízí podporu pro priority na každé stanici. Každá stanice může mít až čtyři AC k podpoře osmi uživatelských priorit (UP). To znamená, že k jedné AC je přiřazena jedna nebo více UP. Stanice pak přistupuje k médiu na základě AC rámce, který má být vysílán. Přiřazení jednotlivých UP do AC ukazuje Tabulka 2.1 [2].

Každá AC je tedy rozšířená varianta DCF. Soutěží o možnost zasílat pakety (TXOP) použitím sady EDCA parametrů. TXOP je interval, kdy má stanice právo k přenosu dat. K AC s vyšší prioritou je přiděleno kratší „okno sváru“ (CW, chvíle nečinnosti po mezirámcové mezeře, kdy probíhá soutěž o médium), aby bylo zajištěno, že AC s vyšší prioritou začne vysílat dříve než AC s nižšími prioritami. Toto je zajištěno přidělením limitů CWmin a CWmax (ze kterých je poté CW určeno) různě pro různé AC. Pro další oddělení jsou různým AC přiděleny rozdílné mezirámcové mezery (IFS). Místo DIFS (pro DCF) je použit AIFS, který trvá nejméně DIFS a je možné jej prodloužit individuálně pro každou AC. Stejně jako v DCF, pokud stanice zjistí, že je médium nečinné, může okamžitě začít přenos. Pokud je detekován přenos, stanice počká až do jeho ukončení. Poté stanice čekají po dobu AIFS, aby mohly začít tzv. backoff algoritmus (je to doba odkladu vysílání). Backoff interval je náhodné číslo z intervalu [1, CW(AC)+1].

Každá AC uvnitř jedné stanice se nyní chová jako virtuální stanice. Soutěží o přístup k médiu a nezávisle startuje svůj backoff algoritmus po zjištění nečinnosti na médiu po dobu delší než AIFS. Může vzniknout situace, kdy v rámci jedné fyzické stanice získá více AC přístup současně, tj. vznikne virtuální kolize. V takovém případě stanice může odeslat pouze jeden rámec, a proto je TXOP přidělen rámci z kategorie přístupu s větší prioritou. Nevybrané kategorie přístupu vyhodnotí vzniklou situaci jako kolizi a provedou příslušná opatření [10].

Tabulka 2.1 - Přiřazení jednotlivých UP k AC

	Uživatelská priorita (UP)	Přístupová kategorie (AC)	Určení
Nejnižší	1	0	Best Effort
	2	0	Best Effort
	0	0	Best Effort
	3	1	Video Probe
	4	2	Video
	5	2	Video
	6	3	Voice
Nejvyšší	7	3	Voice

Přednostní přístup k médiu tedy EDCA zajišťuje přidělením odlišných CW a AIFS k různým AC (typické hodnoty uvádí Tabulka 2.2 [2]). Datové jednotky jsou doručovány pomocí mnoha backoff instancí uvnitř jedné stanice. Každá takováto instance je popsána specifickými parametry pro kategorii provozu (TC). Tento model je znázorňuje Obrázek 2.2 [2].

Tabulka 2.2 - Typické hodnoty CW a délky AIFS

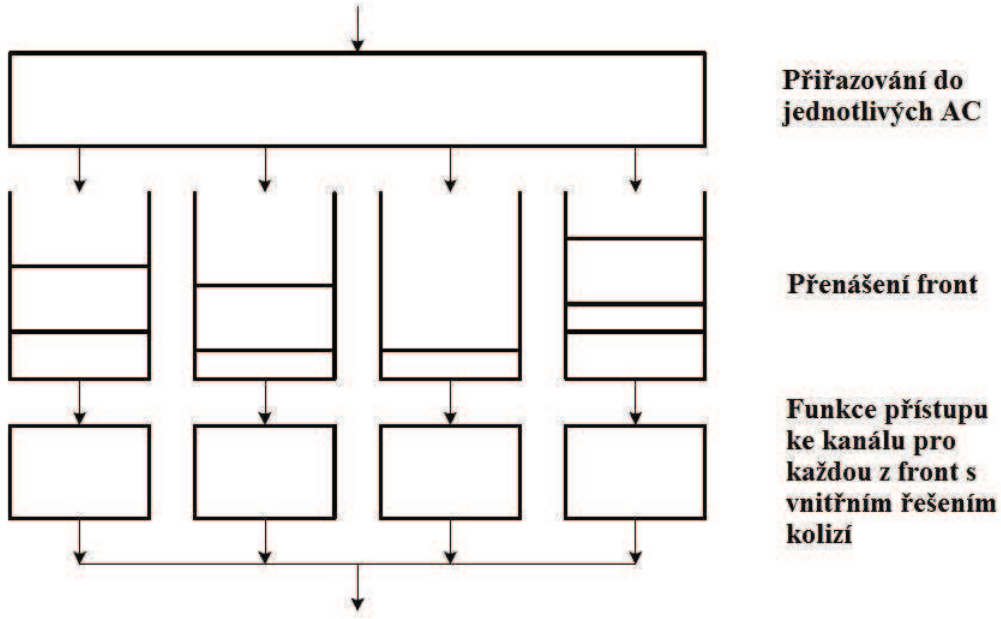
AC	CWmin	CWmax	AIFS
0	CWmin	CWmax	2
1	CWmin	CWmax	1
2	[(Cwmin+1)/2]-1	CWmin	1
3	[(Cwmin+1)/4]-1	[(Cwmin+1)/2]-1	1

Existují dva režimy pro EDCA TXOP. Prvním je zahájení EDCA TXOP, druhým je trvání EDCA TXOP. Zahájení TXOP nastane, když pravidla EDCA povolí přístup k médiu. Trvání TXOP nastane, pokud funkce pro přístup ke kanálu ponechá práva pro přístup k médiu po ukončení sekvence pro výměnu rámců, například pro obdržení ACK rámce. Limity pro trvání TXOP jsou stanicím oznamovány QoS přístupovým bodem (QAP) v poli pro EDCA parametry v beacon rámci (základní řídící rámec bezdrátové sítě). Pokud je hodnota TXOP nula, signalizuje to, že může být vyslán během TXOP pouze jediný rámec.

QoS stanice (QSTA) se musí ujistit, že trvání TXOP získané použitím EDCA pravidel nepřekračuje TXOP limit. Během této doby si držitel TXOP udržuje nepřetržitou kontrolu nad médiem včetně času potřebnému k poslání rámců, které slouží jako okamžité odpovědi na přenos dat (potvrzení správného přijetí - ACK). QSTA musí fragmentovat unicastové rámce tak, aby přenos prvního fragmentu rámce v TXOP nepřekročil TXOP limit při rychlosti na fyzické vrstvě (PHY) zvolené pro počáteční přenos tohoto fragmentu. TXOP limit může být překročen, pokud je použita nižší PHY rychlost než původně zvolená pro tento počáteční přenos prvního rámce, pokud jde o opakovaný přenos rámce, pokud jde o první přenos rámce (pouze pokud byl kterýkoli předchozí rámec opakovaně vyslán) nebo pokud jde o broadcastové nebo multicastové rámce. Pokud je TXOP limit překročen kvůli opakovanému vysílání rámců vysílanému redukovanou PHY rychlostí, stanice by neměla vyslat více jak jeden rámec během TXOP. Pokud jsou rámce přenášeny s jiným potvrzovacím

mechanismem, než je okamžité ACK, měl by být použit ochranný mechanismus (jako RTS/CTS, RTS - požadavek k rezervaci přenosového média, CTS – potvrzení úspěšné rezervace [10]).

Pro broadcastové nebo multicastové rámce náležící do QoS lokální multicastové služby je buď vysílán vždy jeden rámec a proveden backoff algoritmus nebo může být vysláno více rámců za sebou tak, že se nejdříve vyšle RTS rámec s trváním a identifikací celé dávky do QAP a počká se na odpovídající CTS rámec. QAP může vysílat broadcastové nebo multicastové rámce bez použití jakéhokoliv ochranného mechanismu. V QoS nezávislé BSS (QIBSS) musí být broadcastové nebo multicastové rámce náležící do QoS lokální multicastové služby vysílány po jednom a proveden backoff algoritmus [2].



Obrázek 2.2 - Realizace mechanismu EDCA

2.3.2 HCCA

HCCA používá pro přístup ke kanálu centrální koordinátor spolupracující s QoS, který se nazývá hybridní koordinátor (HC) a pracuje podle pravidel, která jsou odlišná oproti PC pracujícímu pod PCF. HC je umístěný v QAP a používá vyšší prioritu pro přístup k médiu pro započetí sekvence výměny rámců a přidělení TXOP pro sebe a ostatní QoS stanice, aby poskytl časově omezenou fázi kontrolovaného přístupu (CAP) pro přenos QoS dat bez soutěžení o médium [2].

Data pro doručení pomocí HC a alokace TXOP jsou naplánovány během CP a všech lokálně generovaných CFP (generovány volitelně pomocí HC) pro splnění QoS požadavků jednotlivých kategorií provozu (TC) a skupin dat (TS). Alokace TXOP a přenosy QoS provozu bez soutěžení o médium mohou být založeny na znalostech HC o množství čekajícího provozu, který náleží do různých TC a TS a podléhá specifické QoS politice. QAP může indikovat dostupnost CF-poll rámců (HC jím může vyzvat stanici k odeslání dat) stanicím nepodporujícím QoS, čímž zajišťuje přenos bez soutěžení o médium během CFP těmto stanicím, avšak není to doporučováno, protože dosažitelná kvalita služeb bude velmi pravděpodobně snížena zasíláním CF-Poll rámců stanicím bez QoS. HCF chrání

přenosy v průběhu každé CAP použitím virtuálního mechanismu pro naslouchání médiu. Stanice s QoS může zahájit několik sekvencí pro výměnu rámců během intervalu TXOP (který je pro to dostatečně dlouhý) získaného díky CF-Poll rámci. Použitím virtuálního naslouchání médiu zajišťuje HC vylepšenou ochranu při CFP [2].

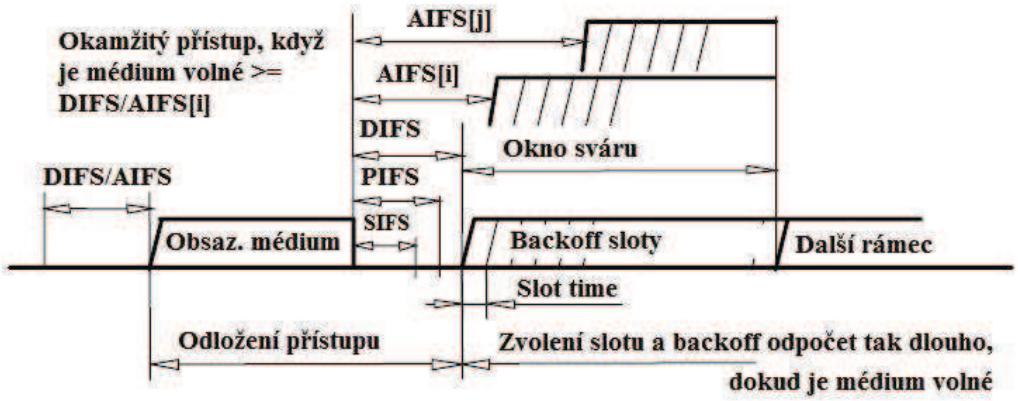
2.4 Koexistence DCF, PCF a HCF

DCF a centralizované koordinační funkce (PCF nebo HCF) koexistují způsobem, který dovoluje, aby pracovaly souběžně uvnitř jedné BSS. Pokud v BSS pracuje PC, střídají se přístupové metody PCF a DCF, tedy CFP následována CP. Pokud HC pracuje v QBSS může generovat střídání CFP a CP stejně jako PC, použitím přístupové metody DCF jen během CP. Přístupové metody HCF (kontrolovaná a založená na soutěžení) operují postupně, když je kanál v CP. Postupný provoz dovoluje metodám přístupu založeným na posílání Poll rámců a metodám založeným na soutěžení střídání v rámci intervalu potřebného k přenosu rámcové výměnné sekvence.

Je definováno pět rozdílných mezirámcových mezer (IFS) pro zajištění stupňů priorit pro přístup k médiu (následuje jejich výpis od nejkratší po nejdelší s výjimkou AIFS, ta může nabývat různých hodnot pro různé AC). Obrázek 2.3 [2] znázorňuje vztahy mezi nimi [2],[10].

1. **SIFS** - krátká IFS
2. **PIFS** - IFS pro PCF
3. **DIFS** - IFS pro DCF
4. **AIFS** - IFS výběru (používá se pro QoS)
5. **EIFS** - rozšířená IFS

Rozdílné IFS jsou nezávislé na bitové rychlosti stanice. IFS jsou definovány jako časové mezery na médiu a kromě AIFS jsou všechny pevně určeny pro každou PHY (i v těch PHY, schopných mnoha bitových rychlostí). Hodnoty IFS jsou určeny podle atributů specifikovaných v PHY.



Obrázek 2.3 - mezirámcové mezery u IEEE 802.11e

3 Mobilita

3.1 Plná mobilita

Termín „mobilita“ není pevně definován. Stolní počítač, který je připojen pomocí mnoha kabelů a používá mnoho pomocných externích zařízení, jistě nemůže být považován za mobilní, tento termín je tedy spojen s určitou jednoduchostí pohybu. Zde ale musíme rozlišovat termíny přenositelnost a mobilita. Přenositelný může v tomto případě i notebook, který je přenesen z jednoho místa na druhé a je na něm vytvořeno nové připojení k Internetu. Uživatel ale musí ukončit a znovu spustit veškeré aplikace. Naším cílem je však plná mobilita, tedy zařízení, které je vždy připojeno k nejlepší dostupné síti.

Požadavkem na plnou mobilitu je schopnost udržet komunikaci i při změnách připojení. Uživatel si tedy nesmí všimnout, že došlo k nějaké změně. Všechny technologie zajišťující mobilitu musí být schopny lokalizovat zařízení v síti a doručit tomuto zařízení příslušná data. Tyto technologie tedy musí zajišťovat základní čtyři požadavky [5]:

- **Zjištění polohy:** Aby mohla síť doručit data koncovému zařízení, musí vědět, kde toto zařízení najít. Existují dva přístupy ke zjištění polohy:

  a) **Reaktivní přístup:** V tomto případě je sítí vysílán požadavek pouze tehdy, když má síť data k doručení. Tento přístup je použit v buňkových telefonních sítích, kde je udržován záznam o lokalitě, ve které se telefon nachází a ve chvíli, kdy je nutno spojit hovor, vyšle síť všesměrovou zprávu do této lokality. Toto je výhodné, pokud dochází k doručení malých objemů dat, protože síť nemusí udržovat obsáhlá data o dílčích pohybech zařízení.

  b) **Proaktivní přístup:** V těchto sítích se udržují záznamy o přesné pozici všech zařízení.

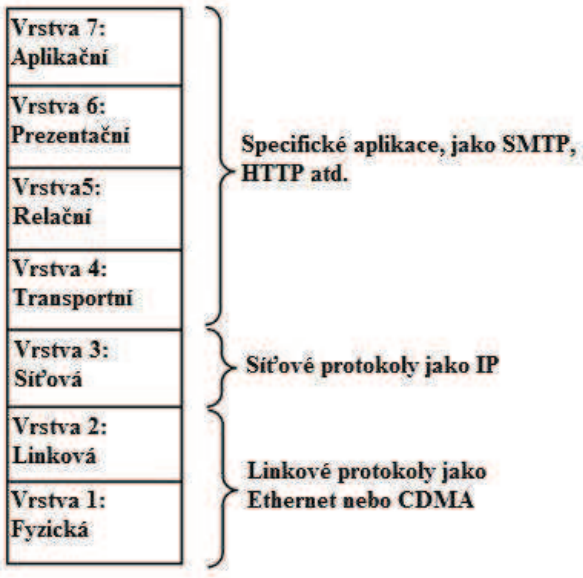
- **Detekce pohybu:** I když má tento termín obecně většinou fyzický význam, v tomto případě se jedná o pohyb logický. Detekce pohybu by se tedy dala popsat jako změna v seznamu dostupných přístupových sítích. Většina mobilních zařízení má na výběr několik možností připojení. Protokol zajišťující mobilitu je potom zodpovědný za výběr nejlepší dostupné přístupové sítě a za připojení k této síti. Protokoly zajišťující plnou mobilitu mohou udržovat plynulost spojení i při změně přístupové sítě. Změna polohy způsobená detekcí pohybu se nazývá handover.

- **Zasílání aktualizací:** Pomocí aktualizací se oznamuje současná poloha mobilního zařízení zbytku sítě, změny polohy a informace o aktivitě zařízení.

- **(Znovu)vybudování cesty:** Pokud zařízení signalizuje, že změnilo svou polohu, síť musí umět vybudovat cestu k zařízení a pokud byla předchozí cesta právě používána, musí změnit cestu tak, aby mohla data být doručena na novou adresu.

3.2 Mobilita a Referenční model ISO/OSI

Plná mobilita může být implementována na různých místech referenčního modelu (základní rozdělení referenčního modelu OSI ukazuje Obrázek 3.1)[5]:



Obrázek 3.1 - Rozdělení referenčního modelu ISO/OSI [5]

- **Mobilita na vrstvách 4 až 7**: Mobilita na vyšších vrstvách je nepraktická, protože by každá aplikace musela obsahovat svou specifickou podporu mobility. Přesto některé aplikace implementují určitou úroveň mobility (např. komunikační klienti pravidelně kontrolují, zda je přístupová linka stále aktivní a síťová adresa nebyla změněna, emailoví klienti se umí vypořádat se změnou IP adresy mezi kontrolami emailů), ale co se týče plné mobility, pokud dojde při běhu aplikace ke změně IP adresy, dochází k chybám.

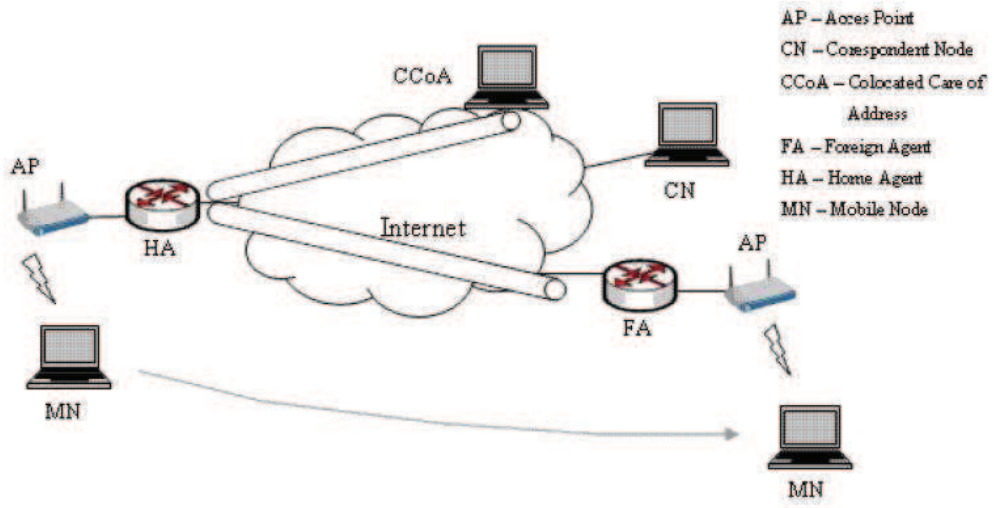
- **Mobilita na vrstvě 3:** Síťová vrstva a IP protokol jsou ideální pro podporu plné mobility. IP protokol je podporován většinou sítí a drtivou většinou aplikací. IP mobilita dovoluje aplikacím používajícím libovolné transportní protokoly zdědit plnou mobilitu napříč širokému rozsahu typů přístupových linek. Uživatelé mohou přecházet z pevného připojení do bezdrátových sítí a zaznamenat pouze jistou horší kvalitu připojení, nemusí však přerušovat navázaná spojení a ukončovat aplikace.

- **Mobilita na vrstvě 2:** Mobilita spojená s přístupovou technologií na linkové vrstvě se ukázala jako úspěšná. Protokoly na druhé vrstvě sledují všechny změny v přístupových spojích. Díky tomu jsou informace potřebné pro detekci pohybu přístupné. Handover může proběhnout velmi rychle, tudíž bez dopadu na aplikace vyšších vrstev. Jako u většiny protokolů na vrstvě 2 může být problém se škálovatelností.

- **Slučování protokolů mobility:** Protokoly mobility na vrstvách 2 a 3 mají své výhody, které do sebe zapadají a dovolují vytvořit řešení pro plnou mobilitu. Mobilita na vrstvě 2 zajišťuje rychlý handover u přístupových linek na malém prostoru využívajících stejnou technologii. Mobilita síťové vrstvy je pak přidána nad mobilitu na linkové vrstvě, aby podporovala škálovatelnost a nezávislost na linkové vrstvě.

3.3 Komponenty protokolu Mobile IPv4

Protokol Mobile IPv4 umožňuje stanici s IP adresou ze sítě o daném rozsahu IP adres být připojena a komunikovat v sítích o jiném rozsahu IP adres. Zařízení je přitom v sítí identifikovatelné stále pod stejnou IP adresou a změna polohy mezi podsítěmi nebo sítěmi je vzhledem k aplikacím transparentní [7]. Jak je ukazuje Obrázek 3.2 [8], pro svou základní funkci musí protokol Mobile IPv4 obsahovat minimálně domácího agenta (Home Agent, HA) a mobilní stanici (Mobile Node, MN) a může také obsahovat hostitelského agenta (Foreign Agent, FN). Jakýkoli směrovač může sloužit jako kterákoli z těchto tří komponent nebo jako všechny zároveň. Protokol Mobile IPv4 obsahuje i další důležité části, následuje popis všech důležitých součástí tohoto protokolu [5]:



Obrázek 3.2 - Komponenty protokolu Mobile IPv4 [8]

- **Mobile Node (MN):** Mobilní stanice je jakékoli zařízení podporující IP protokol a mající doplněk Mobile IP. Mobilní stanicí tedy může být cokoli od PDA, počítačů až po samotné směrovače. Mobilní stanice je zodpovědná za svou vlastní detekci pohybu a tudíž musí být schopna detekovat logický pohyb a poznat svou aktuální pozici. Logický pohyb neznamená vždy fyzický pohyb zařízení. Pokud se zařízení fyzicky nepohybuje a připojení k síti přestane fungovat, může se stanice připojit k jiné dostupné síti a podniknout tak logický pohyb. Pokud se MN rozhodne pro handover, musí své rozhodnutí dát vědět HA (typicky zprávou přes FA). MN a HA musí sdílet bezpečnostní klíč, který zaručí, že jejich komunikace bude zabezpečena.

- **Domácí síť a domácí adresa:** IP adresa MN je označována jako domácí adresa (home address). Domácí adresa je vybrána z IP adres náležících domácí síti, která je připojena k HA, a může být přidělena staticky nebo dynamicky během registračního procesu. Koncept domova je základním bodem protokolu Mobile IP. Pokud je MN připojen ke své domácí síti, protokol Mobile IP není potřebný, protože data mohou být k MN doručena tradičním způsobem. Pokud MN opustí domácí síť a připojí se k jiné síti, je tato nová síť označována jako cizí síť (foreign network).

- **Home Agent (HA):** Data určená pro domácí adresu MN jsou poslána do domácí sítě, i když již v této síti MN není. Tato data musí být přesměrována k aktuální pozici MN. Zodpovědnost za toto přesměrování má HA. HA je například směrovač schopný zpracovávat aktualizační zprávy protokolu Mobile IP (registrace) a přeposílat data k MN dynamicky vytvořenými tunely.

- **Care of address (CoA):** CoA je IP adresa, která je platná a použitelná na aktuální pozici MN připojeného v cizí síti. MN informuje HA o své CoA během registračního procesu protokolu Mobile IP. Zapouzdřená (tunelovaná) data jsou poté doručena od HA k CoA, která je logickou polohou MN v cizí síti. Tunel je tedy vytvořen mezi HA a CoA. Existují dva typy CoA:

  a) **Colocated CoA (CCoA):** V tomto případě získá MN přímo IP adresu platnou v cizí síti (například pomocí Dynamic Host Configuration Protokolu - DHCP). Tato adresa se tedy označuje jako CCoA. MN má tedy v tomto případě dvě IP adresy – domácí adresu a CCoA. CCoA je platná a použitelná a je schopna přijmout tunelovaný provoz. MN musí být schopný ukončit Mobile IP tunel. Domácí adresa není v cizí síti použitelná, přesto je používána jako zdrojová a cílová adresa všech přenášených dat.
     CCoA je považován jako neefektivní zacházení s IP adresami, protože každý MN potřebuje platnou a použitelnou IP adresu v každé cizí síti. I přes tuto neefektivitu je CCoA často používána a často je spojena s privátními IP adresami, aby se minimalizovalo plýtvání.

  b) **Foreign Agent CoA (FA CoA):** Další možností je použití FA CoA, kdy více stanic sdílí jednu CoA. FA CoA je jedna nebo více IP adres rozhraní FA.

- **Foreign agent (FA):** FA je směrovač, který je schopen ukončit tunel místo MN. FA může nabízet jednu nebo více svých IP adres jako CoA. Pokud se MN v cizí síti registruje s HA, dělá to přes FA. FA udržuje záznam o lince, ke které je MN připojen. Data určená MN jsou tunelována od HA k FA, který nejprve odstraní hlavičku zapouzdřeného paketu a poté jej doručí MN. FA musí být přímo připojen k přístupové lince MN, protože data mohou být doručena pouze pomocí adres MAC vrstvy. Pokud by totiž FA poslal paket dále do sítě, vrátil by se zpět k HA a poté by skončil v nekonečné smyčce.

- **Correspondent node (CN):** CN není vlastně částí Mobile IP protokolu, ale je to prvek, který pomáhá v představách o toku dat. CN je rovnocenný s MN ve vzájemné IP komunikaci (například další MN, nebo pevný stolní počítač). Pokud například MN používá webový prohlížeč, CN by představoval webový server.

3.4 Koncept protokolu Mobile IPv4

Dříve zde byly popsány základní kritéria pro zajištění mobility. Protokol Mobile IP splňuje tyto kritéria následujícím způsobem [5]:

- **Zjištění polohy:** V Mobile IP existují 2 prostředí – domácí a cizí síť. Typ sítě, ke které je MN připojen, je pro tento protokol velmi důležitý, protože rozhoduje o typu handoveru a vyžaduje rozdílnou signalizaci. Pozice je určena prozkoumáním zpráv směrovače (agent advertisements) nebo prozkoumáním přidělené CCoA.

- **Detekce pohybu:** MN se neustále zabývá procesem detekce pohybu, což je monitorování změn v přístupových cestách do sítí. Mobile IP je protokol síťové vrstvy referenčního modelu ISO/OSI, proto je detekce pohybu proces zjišťování změn v cestách síťové vrstvy, které může MN použít pro připojení k síti. Kdykoli je detekován pohyb, Mobile IP použije algoritmus ke zhodnocení všech dostupných cest a k rozhodnutí, jestli je nutná změna v připojení k síti. Tato změna se nazývá Mobile IP handover.

- **Zasílání aktualizací:** Poté, co je spuštěn handover, MN rozhodne, jaké signalizační zprávy je nutné zaslat (toto záleží na typu současné a budoucí sítě). Tyto zprávy jsou vlastně žádostmi o registraci a zrušení registrace v síti (Registration Request – RRQ a Deregistration Request). FA nebo HA vyhodnotí tyto zprávy a pošlou zprávu o úspěšné nebo neúspěšné registraci (Registration Reply - RRP). Tato výměna zpráv je označována jako proces registrace protokolu Mobile IP.

- **(Znovu)vybudování cesty:** Pro úspěšnou registraci je vybudován mezi CoA a HA tunel. Naopak pro úspěšné zrušení registrace musí být tento tunel zrušen. HA a FA upraví své adresní tabulky, aby odpovídaly aktuální poloze MN. MN se po úspěšném handoveru vrátí zpět do fáze detekce pohybu a proces začíná znovu.

3.5 Nalezení agentů protokolu Mobile IPv4

Detekce pohybu a zjištění polohy jsou v Mobile IP adresovány pomocí agent advertisements zpráv. Tyto zprávy jsou založeny na protokolu IRDP (ICMP (Internet Control Message Protocol) Router Discovery Protocol). IRDP se skládá ze dvou typů zpráv, které jsou určeny pro podporu protokolu Mobile IP [5]:

- **Router advertisement:** Jsou to zprávy, které jsou vysílány směrovači pomocí multicastu nebo broadcastu v definovaných pravidelných intervalech. Směrovač podporující protokol Mobile IP posílá router advertisement zprávy, které obsahují rozšíření, informující o specifických službách Mobile IP protokolu, které směrovač podporuje.

- **Router solicitation:** Tyto zprávy posílá MN požadující, aby směrovače, které ji slyší, vyslaly své router advertisement zprávy. TTL těchto zpráv je nastavena na 1 a mohou být vysílány multicastem nebo broadcastem. Router solicitation zprávy dovolují zjištění aktuální polohy mnohem rychleji, než kdyby musela MN čekat na periodické router advertisement zprávy.

3.6 Proces registrace v protokolu Mobile IPv4

Když se MN rozhodne, že je potřeba připojit se k jiné síti (ať už jde o přechod mezi dvěma FA nebo návrat domů), přejde do registrační fáze a spustí tak handover. Během této fáze zašle MN svému HA informace o své pozici. Tato signalizace je uskutečněna pomocí Mobile IP RRQ zpráv. RRQ zprávy jsou ekvivalentem směrovacích informací zasílaných směrovači, protože také informují o způsobu doručení dat k MN (přes CoA). RRP je pozitivní nebo negativní potvrzení RRQ zprávy a může být vysláno buď HA, nebo FA. Průběh výměny zpráv při registraci je znázorňuje Obrázek 3.3 [5].

Při handoveru (jiném než návratu domů) je MN po úspěšné výměně Mobile IP RRQ a RRP zpráv označován jako registrovaný u HA (a FA, pokud je použit) po dobu specifikovanou v RRP zprávě. MN tedy musí poslat RRQ zprávu i v případě, že vyprší tzv. doba života registrace.

Pokud dochází k návratu domů, dochází při výměně RRQ a RRP zpráv ke zrušení registrace MN.

RRQ a RRP zprávy jsou základním prvkem registrační fáze v Mobile IP protokolu. Jsou posílány přes UDP transportní protokol na portu číslo 434.

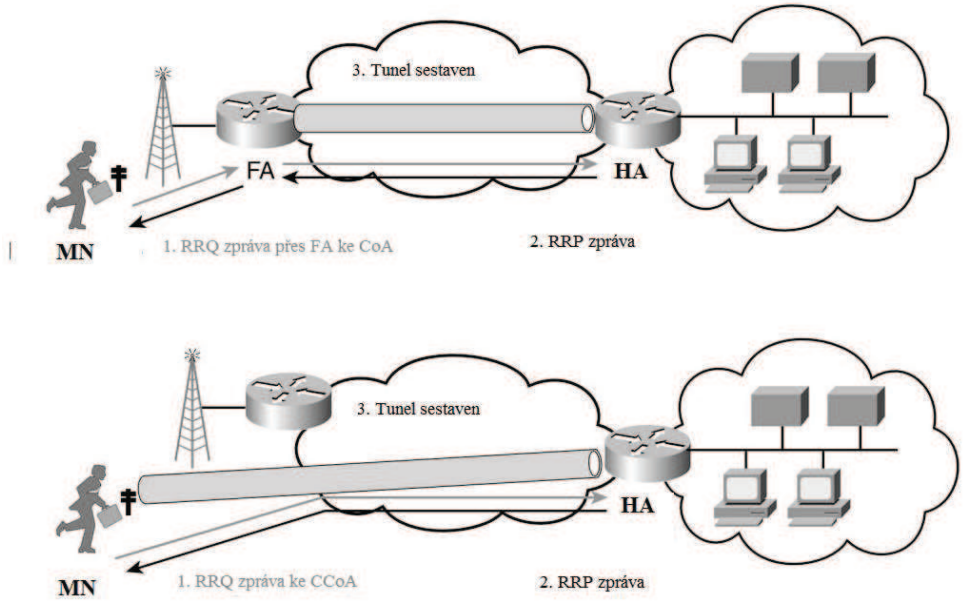
Výměna zpráv musí být jednoznačná a zabezpečená, protože upravuje směrování dat k MN. Kvůli tomu tyto zprávy obsahují tři hlavní části.

RRQ zprávy se skládají z těchto tří hlavních částí [5]:

- **Identifikace:** jedinečná identifikace RRQ a jedinečná identifikace MN
- **Požadavky na služby:** vyjednávání o službách Mobile IP protokolu
- **Parametry pro ověření:** bezpečnostní parametry pro ověření pravosti zpráv

RRP zprávy se skládají z těchto tří hlavních částí [5]:

- **Identifikace:** jedinečná identifikace aby RRP odpovídala RRQ a jedinečná identifikace MN
- **Kódy odpovědí:** stav registrace MN
- **Parametry pro ověření:** bezpečnostní parametry pro ověření pravosti zpráv



Obrázek 3.3 - Průběh výměny zpráv při registraci MN do cizí sítě pro CoA i CCoA

3.6.1 Identifikace

Rozhodujícím aspektem výměny zpráv při registraci Mobile IP protokolu je to, že zprávy musí být jedinečné a specifické ve své identitě. V každé RRP a RRQ zprávě jsou dva typy identifikace – prvním úkolem je identifikovat MN a druhým identifikovat tuto zprávu samotnou. Aby bylo možno rozpoznat, od koho zpráva pochází, jaké služby MN podporuje a jaké způsoby ověřování mají být použity, je vyžadován jedinečný identifikátor MN. MN může být identifikován statickou domácí

adresou nebo pomocí identifikátoru přístupu k síti (Network Access Identifier, NAI), který může být použit i při dynamicky přidělené domácí adrese [5].

3.6.2 Služby

Klíčový výsledek registrační fáze je pro MN a HA domluva na službách protokolu Mobile IP, které budou používány během doby života této registrace. HA nebo FA nabídne MN služby, které podporuje ve svých agent advertisement zprávách. MN poté zažádá o konkrétní služby v RRQ zprávě. FA a HA poté buď přijmou, nebo odmítnou tyto požadavky ve svých RRP zprávách.

Většina služeb, které MN může požadovat, se týká Mobile IP tunelu a s ním spojených možností doručování dat. MN může například požadovat jako zakončení tunelu určitou CoA, použití specifického zapouzdřování v tunelu atd. Služby mohou být vyžadovány nastavením určitých bitů v RRQ zprávě nebo přidáním vhodného rozšíření Mobile IP protokolu (použití rozšíření dovoluje libovolné přidávání nových služeb do protokolu Mobile IP) [5].

3.6.3 Handover jiný než do domácí sítě

Prvním krokem je zpracování RRQ zpráv, které spouštějí handover do jiné než do domácí sítě. HA zjistí, jestli musí být přidělena adresa domácí sítě prozkoumáním pole domácí adresy v RRQ zprávě (Pokud MN požaduje dynamické přidělení domácí adresy, nastaví toto pole na hodnotu 0.0.0.0).

Poté HA aktualizuje mobilní vazbu s MN (pokud již existuje) nebo vytvoří vazbu novou. Mobilní vazba je struktura, která udržuje záznam o vlastnostech aktivního MN. HA používá vazbu ke sledování služeb používaných MN, aktuální CoA a doby života registrace. HA uchovává mobilní vazby v tabulce vazeb, což je databáze všech aktivních MN (jedná se o podobný způsob, jako je například databáze v OSPF). Mobilní vazby jsou unikátně indexovány domácí adresou MN a jsou z tabulky odstraněny, pokud vyprší doba života vazby.

HA využívá informace obsažené v mobilní vazbě k vytvoření IP tunelu ke CoA. HA aktualizuje své směrovací tabulky tak, aby všechna data určená pro MN byla posílána přes IP tunel. HA potom vyšle do domácí sítě nevyžádanou ARP zprávu, aby zajistil, že všechna data určená pro MN budou doručena k HA a poté odeslána IP tunelem.

Nakonec zašle HA RRP zprávu k MN (buď přes FA, nebo přímo). Pokud HA přidělil MN dynamicky domácí adresu, vloží tuto adresu do pole domácí adresy v RRP zprávě.

Pokud FA obdrží RRP zprávu a považuje ji za platnou, schválí pobyt MN ve své síti. FA zapíše tuto registrační zprávu do své tabulky návštěv. Tato tabulka uchovává záznam o všech aktivních MN a je podobná tabulce vazeb u HA. Záznam v této tabulce je udržován až do vypršení doby života vazby nebo do obdržení zprávy o zrušení registrace [5].

3.6.4 Handover do domácí sítě

Okamžitě po potvrzení žádosti o zrušení registrace (posílá MN, který provádí handover do domácí sítě nebo se vypíná), zruší HA IP tunel a vymaže záznam o mobilní vazbě. Od této chvíle již není protokol Mobile IP používán pro směrování dat k MN. HA pošle MN RRP zprávu označovanou jako potvrzení zrušení registrace.

Pokud FA obdrží zprávu s potvrzením o zrušení registrace, odstraní záznam o MN ze své tabulky návštěv a tuto zprávu přepošle k MN.

Okamžitě po zrušení registrace pošle MN v domácí síti nevyžádanou ARP zprávu, aby zajistila, že data určená pro MN již nebudou směrována přes HA. Obvykle se MN zřekne své dynamicky přidělené domácí adresy [5].

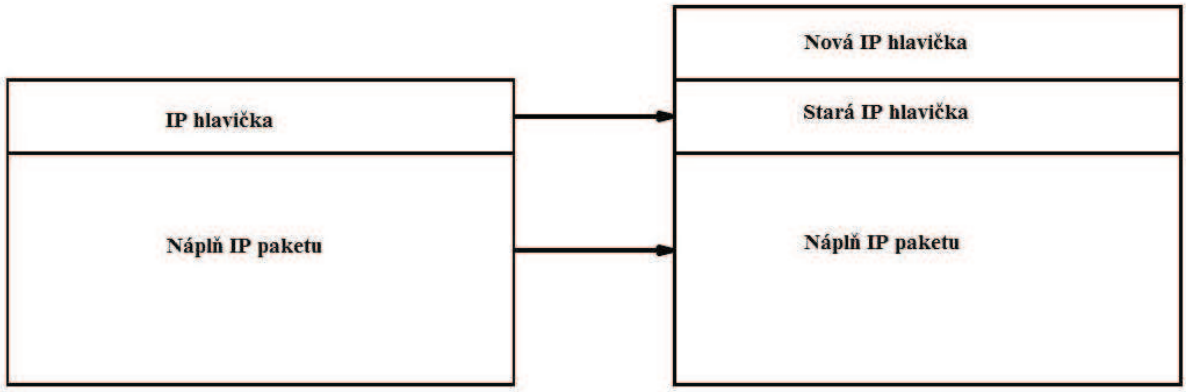
3.7 Tunelování

Místo zasílání směrovacích informací celé síti vybuduje Mobile IP logické linky (tunely) k hranici cizí sítě, ke které je připojen MN. Tento tunel dokáže přenést mezi svými koncovými body (na straně FA je to buď CCoA nebo FA CoA) IP paket. Pokud má HA více MN připojených ke stejnému FA, je provoz pro všechny tyto MN posílán jediným tunelem k FA CoA. HA může mít více tunelů k jedné CoA, ale tyto tunely musí mít odlišný zapouzdřovací protokol [5].

3.7.1 Zapouzdřování

Základním protokolem pro tunelování v Mobile IP je IP-in-IP. Původní paket je doručen jako náplň nového IP paketu. Hlavička nového paketu je označována jako vnější hlavička. Cílová adresa vnější hlavičky je adresa konce tunelu (CoA), zdrojová adresa náleží zařízení, které provedlo zapouzdření (HA).

Jak ukazuje Obrázek 3.4 [4], IP-in-IP je jednoduchý protokol, který nadměrně nezatěžuje HA ani CoA. Hodnoty všech polí ve vnější hlavičce jsou nastaveny HA, kromě pole typu služby a pole zákazu fragmentace. Hodnota pole typu služby je zkopírována z vnitřního paketu, což má pomoci zachovat QoS pro tento paket. Bit zákazu fragmentování je nastaven ve vnější hlavičce, pokud je nastaven v zapouzdřeném paketu, nebo se HA rozhodne tento bit nastavit.



Obrázek 3.4 – Zapouzdření IP-in-IP [4]

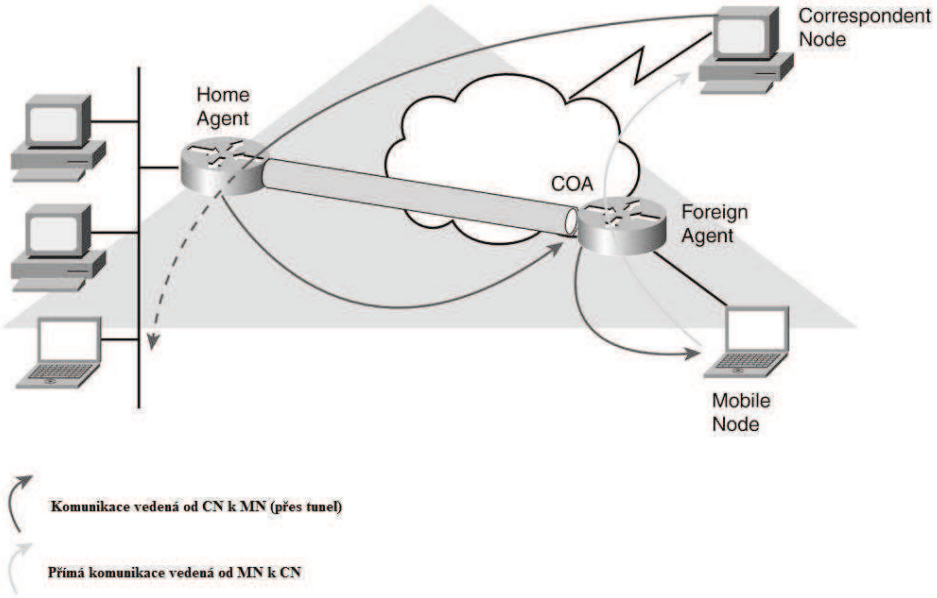
Minimální zapouzdření je pokus o zmenšení velikosti vnitřní hlavičky eliminováním duplicitních informací. To znamená, že z vnitřní hlavičky jsou odstraněny nadbytečné informace, které jsou obsaženy také ve vnější hlavičce. Minimální zapouzdření je užitečné, pokud má paket po cestě projít linkou s nízkou propustností, kde záleží na každém bitu.

3.7.2 Trojúhelníkové směrování

Protokol Mobile IP používá asymetrické směrování označované jako trojúhelníkové směrování. Data určená MN jsou od CN nejprve poslána k HA a až poté k MN. Zpětný provoz pak je směrován přímo od MN k CN, což vytváří trojúhelník (zobrazuje Obrázek 3.5). Hlavním důvodem, proč HA neinformuje CN přímo o pozici MN, je především bezpečnost [5].

K výměně takto důležitých údajů během registračního procesu by musela mezi MN a CN existovat důvěryhodná vazba. Jinak by totiž mohlo dojít k DoS útoku, kdy by útočníkův počítač poslal CN falešnou registrační zprávu a pak by mohl jednoduše přijímat data určená MN. Protože důvěrný vztah mezi MN a CN je nezvyklý, využívá Mobile IP trojúhelníkové směrování a důvěrný vztah MN a HA.

IP směrování nevyužívá při doručování zdrojovou adresu paketu. Mobile IP tohoto faktu využívá k optimalizaci doručování dat. Pakety posílané MN mají jako zdrojovou adresu nastavenu domovskou adresu MN, i když je MN připojen v cizí síti, a jsou doručeny k cíli s použitím FA jako brány. MN posílá data přes jednu z adres směrovače zjištěných z router advertisement zpráv a pokud je připojen v cizí síti, nemusí posílat ARP žádosti.



Obrázek 3.5 - Trojúhelníkové směrování [5]

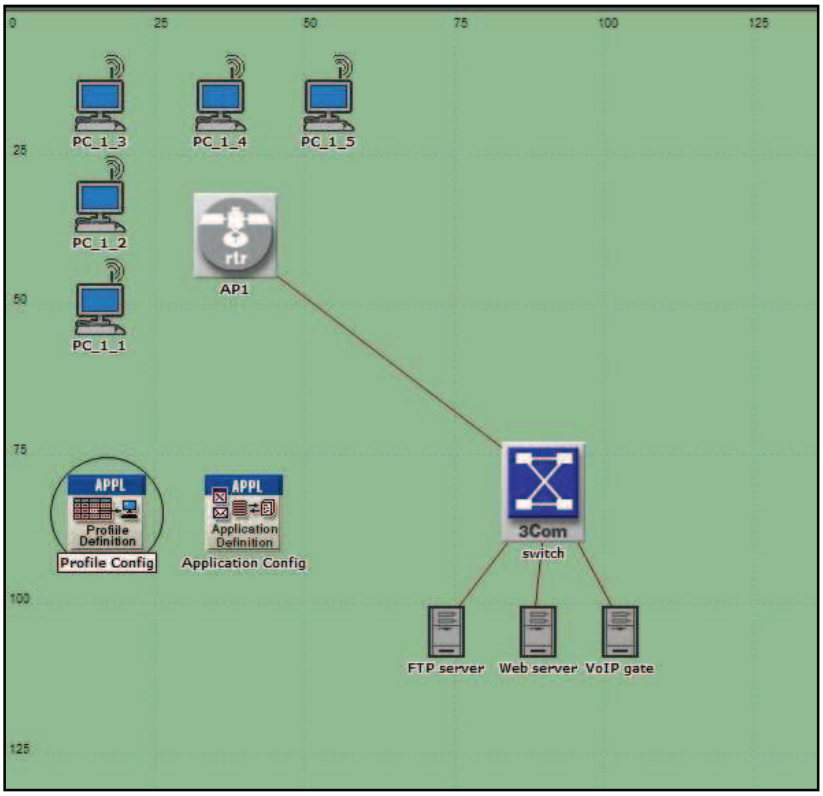
Pakety určené MN použijí klasické IP směrování k dosažení domácí sítě MN, kde HA zachytí data určená pro MN a pošle je tunelem k CoA.

Takzvané zpětné tunelování umožňuje datům, která posílá MN připojený v cizí síti, být poslána zpět k HA zpětným tunelem. Tyto pakety jsou poté standardně směrovány od HA k cíli. Zpětné tunelování odstraňuje pojem trojúhelníkového směrování a zajišťuje, že jsou pakety od MN topologicky korektní. Toto může být důležité pro zdolání bezpečnostních prvků rozmístěných v Internetu.

4 Simulace bezdrátové sítě s podporou QoS v prostředí OPNET Modeleru

4.1 Vytváření modelu

Při vytváření síťového modelu v prostředí simulačního programu OPNET Modeler byla zvolena rozloha modelu jako *Office*. Pro základní scénář byly vybrány sady objektů *Sm_Int_Model_List* [7] a *wireless_lan_adv*, které obsahují jak základní objekty pro tvorbu LAN sítí (*Sm_Int_Model_List*), tak i speciální objekty pro tvorbu bezdrátových sítí WLAN (*wireless_lan_adv*). Obrázek 4.1 zobrazuje topologii sítě použitou pro většinu simulací (jeden ze scénářů obsahuje deset stanic pro simulaci vlivu počtu stanic na vlastnosti sítě). Je použita jednoduchá infrastrukturální topologie s jedním AP a několika stanicemi (tzv. Basic Service Set, BSS). Pro koncové stanice byl použit model *wlan_wkstn_adv* podporující mobilitu (z důvodu budoucího rozšíření projektu o IP mobilitu), pro AP pak model *wlan_ethernet_router_adv*. Tato BSS topologie je napojena na distribuční síť v podobě přepínače a tří serverů. Použití přepínače umožňuje budoucí doplnění projektu o další BSS a vytvoření ESS topologie (Extended Service Set) pro implementaci IP mobility. Jednotlivé servery jsou použity jako HTTP server, FTP server a brána pro VOIP. Pro přepínač bylo použito modelu *3C_SSII_1100_3300_4s_ae52_e48_ge3*, pro servery je to pak model *ethernet_server*. Kromě bezdrátových stanic jsou všechny uzly sítě propojeny pomocí 100Mb Ethernetu.



Obrázek 4.1 - Topologie sítě

4.2 Základní konfigurace síťových prvků a aplikací

4.2.1 Vytvoření aplikací a profilů:

Nejprve byly pomocí editace objektu *Application Config* nastaveny potřebné aplikace a objem jimi přenášených dat:

1. Obrázek 4.2 ukazuje zvolené nastavení aplikace Ftp. *Command Mix* nastavený na 50% znamená rovnoměrné rozdělení mezi downloadem a uploadem. Pro jednotlivé Ftp přenosy byla zvolena konstantní velikost přenášeného souboru 5MB. Tato služba je typu Best Effort s prioritou přenosu nula a je obstarávána FTP Serverem.

Attribute: Application Definitions.Description [0].Ftp

Command Mix	50%
Inter-Request Time	constant (5)
File Size	constant (5000000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back-End Custom Application	Not Used

Obrázek 4.2 - Nastavení aplikace Ftp

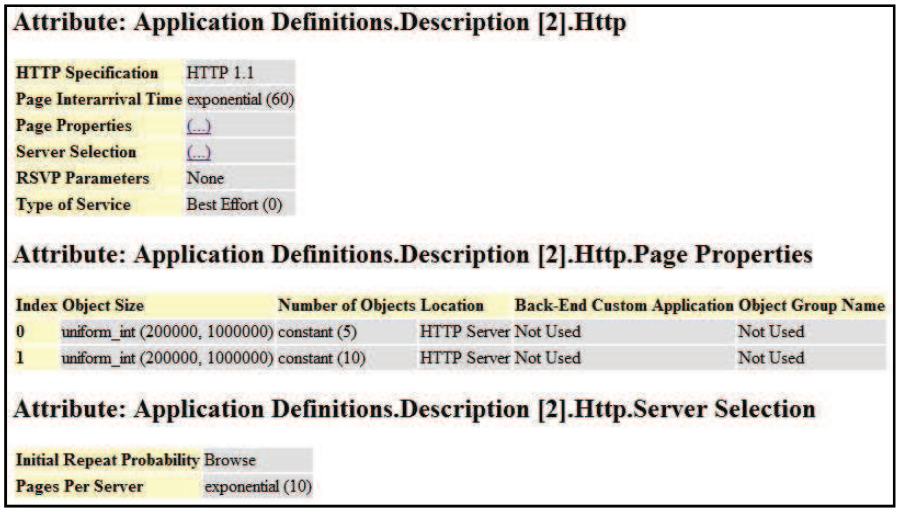
2. Obrázek 4.3 ukazuje nastavení aplikace Voice. Služba má přenosovou prioritu 6, takže bude mít při použití QoS při přenosu přednost před službami s nižší prioritou. Pro kódování hlasových dat před přenosem bylo zvoleno schéma G.711.

Attribute: Application Definitions.Description [1].Voice

Silence Length	default
Talk Spurt Length	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.711 (silence)
Voice Frames per Packet	1
Type of Service	Interactive Voice (6)
RSVP Parameters	None
Traffic Mix	All Discrete
Signaling	None
Compression Delay	0.02
Decompression Delay	0.02
Conversation Environment	(...)

Obrázek 4.3 - Nastavení aplikace Voice

3. Obrázek 4.4 zobrazuje nastavení aplikace Http. Byla zvolena verze protokolu HTTP 1.1, typ provozu Best Effort s prioritou nula. Nastavené vlastnosti jednotlivých HTTP stránek jsou patrné z obrázku.



Attribute: Application Definitions.Description [2].Http

HTTP Specification	HTTP 1.1
Page Interarrival Time	exponential (60)
Page Properties	(...)
Server Selection	(...)
RSVP Parameters	None
Type of Service	Best Effort (0)

Attribute: Application Definitions.Description [2].Http.Page Properties

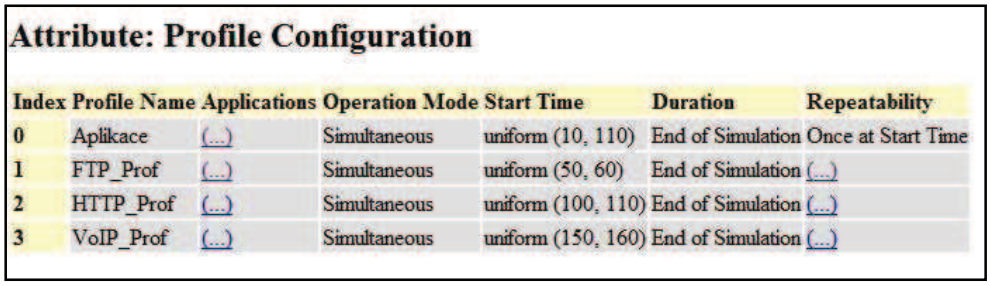
Index	Object Size	Number of Objects	Location	Back-End Custom Application	Object Group Name
0	uniform_int (200000, 1000000)	constant (5)	HTTP Server	Not Used	Not Used
1	uniform_int (200000, 1000000)	constant (10)	HTTP Server	Not Used	Not Used

Attribute: Application Definitions.Description [2].Http.Server Selection

Initial Repeat Probability	Browse
Pages Per Server	exponential (10)

Obrázek 4.4 - Nastavení aplikace HTTP

Dále byly, pomocí objektu *Profile Config*, nastaveny profily pro jednotlivé aplikace. Tyto profily například určují, kdy se jednotlivé aplikace spustí a kolikrát se budou moci během simulace zopakovat. Obrázek 4.5 zobrazuje , že pro každou aplikaci (viz. výše) byl vytvořen zvláštní profil (profil se jménem Aplikace byl vytvořen na začátku vytváření modelu pro testovací potřeby a ve výsledných simulacích není vůbec použit).

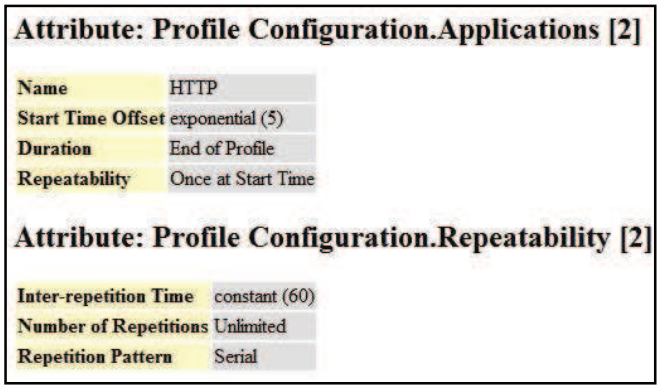


Attribute: Profile Configuration

Index	Profile Name	Applications	Operation Mode	Start Time	Duration	Repeatability
0	Aplikace	(...)	Simultaneous	uniform (10, 110)	End of Simulation	Once at Start Time
1	FTP_Prof	(...)	Simultaneous	uniform (50, 60)	End of Simulation	(...)
2	HTTP_Prof	(...)	Simultaneous	uniform (100, 110)	End of Simulation	(...)
3	VoIP_Prof	(...)	Simultaneous	uniform (150, 160)	End of Simulation	(...)

Obrázek 4.5 - Nastavení profilů jednotlivých aplikací

Jak je dále vidět z obrázku, přiřazení jedné aplikace ke každému profilu umožňuje také nastavit rozdílné časy spouštění aplikací a díky tomu může být sledován např. vliv telefonního hovoru na již spuštěné aplikace s nižší prioritou provozu. Obrázek 4.6 znázorňuje příklad nastavení opakování profilu HTTP. Ostatní profily jsou nastaveny podobně.



Attribute: Profile Configuration.Applications [2]

Name	HTTP
Start Time Offset	exponential (5)
Duration	End of Profile
Repeatability	Once at Start Time

Attribute: Profile Configuration.Repeatability [2]

Inter-repetition Time	constant (60)
Number of Repetitions	Unlimited
Repetition Pattern	Serial

Obrázek 4.6 - natavení opakování profilu

Konfiguraci objektů *Application Config* a *Profile Config* je dobré věnovat zvýšenou pozornost, protože dobré rozvržení zátěže v síti je důležité pro výsledky simulace. Zátěž v síti nesmí být moc malá, nemusely by se pak projevit rozdíly pro jednotlivé scénáře. Pokud by naopak zátěž byla moc velká (zvětšením počtu opakování jednotlivých aplikací nebo zvětšením objemu přenášených dat zvláště u FTP a HTTP přenosu), může dojít k zahlcení paměti a ukončení simulace. Takovéto chybové hlášení je znázorňuje Obrázek 4.7.

```
<<< Recoverable Error >>>
Allocation of memory failed; request = 40 bytes
T (583.166), EV (442720103), MOD (top.Office Network.FTP server.tcp)
----
<<< Program Abort >>>
Virtual memory limits exceeded.
Too many allocated objects.
T (583.166), EV (442720103), MOD (top.Office Network.FTP server.tcp)
```

Obrázek 4.7 - Chybové hlášení o zahlcení paměti

4.2.2 Konfigurace síťových uzlů

Všem síťovým uzlům byly přiděleny IPv4 adresy pomocí volby v menu *Protocols-> IP-> Addressing-> Auto-Assign IPv4 Addresses* [7]. Servery byly nakonfigurovány každý pro použití jedné aplikace (např. FTP pro FTP server atd.) nastavením položek *Application-> Supported Profiles* a *Application-> Supported Services* pro podporu jednotlivých profilů a aplikací. Konfigurace přepínače nebyla změněna. U jednotlivých stanic a u AP byl nakonfigurován identifikátor sítě SSID na hodnotu „1“, aby mohly stanice a AP vzájemně komunikovat.

Jednotlivé stanice potom byly nakonfigurovány pro podporu různých aplikací (jak zobrazuje Tabulka 4.1). V položce *Application-> Supported Services* byla přidána podpora pro VoIP protokol. Podporované profily byly nakonfigurovány v položce *Application-> Supported Profiles* a nakonec byly v položce *Application-> Destination Preferences* [7] přidány cílové uzly komunikace jednotlivých aplikací (např. u *PC_1_1* to byly *VoIP gate* a *PC_1_2* pro VoIP aplikaci).

Tabulka 4.1 - Stanice a jimi provozované aplikace

Jméno stanice	Provozované aplikace
PC_1_1	FTP, VoIP (VoIP gate a PC_1_2)
PC_1_2	HTTP, VoIP (VoIP gate a PC_1_1)
PC_1_3	FTP
PC_1_4	FTP
PC_1_5	HTTP

4.3 Použité scénáře

Pro srovnávání parametrů byly použity celkem 4 scénáře:

- ***HCF_OFF***:

  V tomto scénáři je vypnuta podpora HCF, takže se vlastně jedná o simulaci provozu v síti bez zajištění QoS. Nastavení všech objektů odpovídá základní konfiguraci popsané výše.

- ***HCF***:

  Tento scénář byl nastaven pro podporu HCF změnou parametru *Wireless LAN Parameters-> HCF Parameters->Status* z hodnoty *Not Supported* na hodnotu *Default* jak u všech stanic v síti, tak u AP. Tento scénář je výchozí scénář se zajištěným QoS a výstupní nasimulované hodnoty u ostatních scénářů s podporou QoS jsou srovnávány s tímto scénářem.

- ***HCF_10STA***:

  Nastavení tohoto scénáře je shodné s nastavením scénáře HCF s tím rozdílem, že je použito deset stanic pro možnost sledovat vliv počtu stanic na provoz v síti. Jednotlivá nastavení stanic byla zkopírována tak, že např. *PC_1_1* má shodné nastavení jako *PC_1_6*, *PC_1_2* pak shodné jako *PC_1_7* atd.

- ***HCF_MOD:***

  V tomto scénáři byl zkoumán vliv pomalu rostoucího okna soutěžení CW [9] pro AC Voice a Video (viz. Tabulka 2.1) na provoz v síti s podporou QoS. Pomalu rostoucí CW zajistí, že v případě kolize se CW u AC Voice a Video zdvojnásobí až při každé druhé kolizi. U ostatních AC je použito základní CW.

  Pro zajištění pomalu rostoucího CW pro AC Voice a Video bylo nutné editovat původní process model *wlan_dispatch*, který podle toho, jestli je na stanicích a AP povolena podpora HCF použije procesy *wlan_mac* nebo *wlan_mac_hcf*. Obrázek 4.8 ukazuje proces *wlan_dispatch*, který byl nastaven, aby místo procesu *wlan_mac_hcf* použil vytvořený process model *wlan_mac_hcf_MOD*.

```
13
14  /* Create the appropriate MAC process model.                */
15  mac_prohandle = (hcf_support_int == OPC_BOOLINT_ENABLED) ?
16                      op_pro_create ("wlan_mac_hcf_MOD", OPC_NIL) :
17                      op_pro_create ("wlan_mac"    , OPC_NIL);
18
```

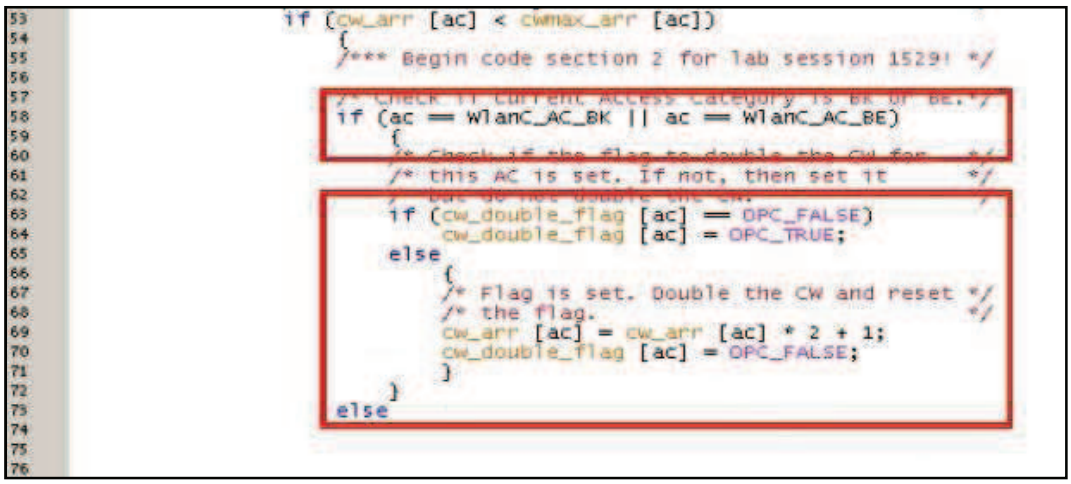
Obrázek 4.8 - Upravený process model *wlan_dispatch*

Process model *wlan_mac_hcf_MOD* vychází z process modelu *wlan_mac_hcf*. Pro úpravu CW bylo nutné před úpravou kódu vytvořit novou stavovou proměnnou se jménem „*cw_double_flag* [9]“ (je to vlastně dvojrozměrné pole – jedna buňka pro každou AC) typu *Boolean* a přidat do původního process modelu následující kód (Obrázek 4.9 [9] a Obrázek 4.10 [9]).

```
67              else
68                  {
69                  /* First trial. Hence, CW size equals to CWmin.     */
70                  cw_arr [ac] = cwmin_arr [ac];
71
72                  /*** Begin code section 1 for lab session 1529!     */
73
74                  /* Initialize the flags for doubling the CW         */
75                  /* size for BE and BK access categories.            */
76                  if (ac == WlanC_AC_BK || ac == WlanC_AC_BE)
77                      cw_double_flag [ac] = OPC_FALSE;
78
79                  /*** End code section 1 for the lab of session 1529!*/
80                  }
```

Obrázek 4.9 - Úprava *wlan_mac_hcf* - 1.část

Před úpravou process modelu je třeba zajistit, že nebude upraven výchozí model. V tomto případě by totiž byl původní model nevratně přesán a používán změněný i v jiných projektech a to je nežádoucí. Možným řešením je zkopírování všech modelů do nové složky a v nastavení OPNET Modeleru změnit v souboru *mod_dirs* cestu k modelům. Tímto je zajištěno, že i v případě chybné konfigurace budou výchozí modely vždy uloženy v původní složce neupravené.



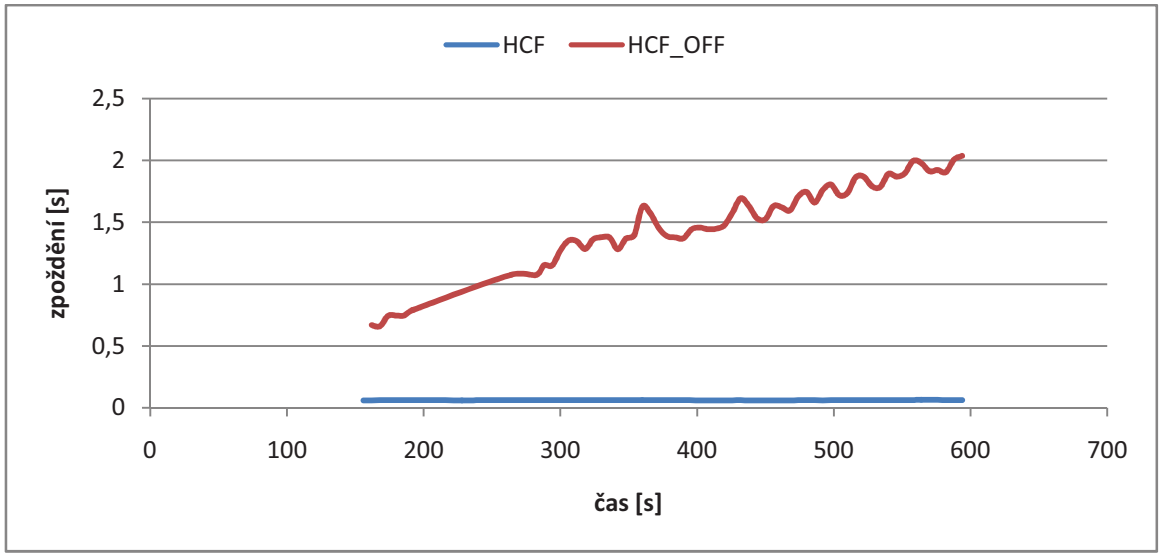
Obrázek 4.10 - Úprava *wlan_mac_hcf* - 2.část

Další vlastností OPNET Modeleru je, že pokud dojde ke změně process modelu v jednom scénáři, projeví se tato změna i u dalších scénářů. Řešením může být uložení modelu uzlu používajícího *wlan_mac_hcf_MOD* pod jiným jménem. Tento model se poté objeví v seznamu objektů *Object Pallete Tree* a je možné jej použít.

4.4 Výsledky simulací

4.4.1 Použití IEEE 802.11e

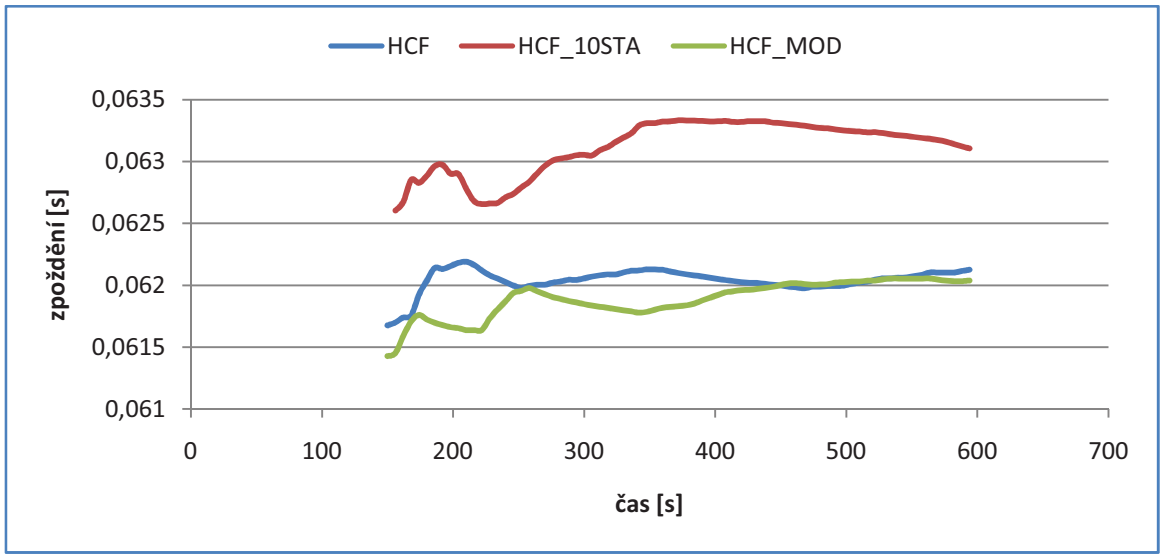
Obrázek 4.11 jasně ukazuje, že v síti se silným provozem FTP a HTTP je provozování hlasových aplikací bez implementace QoS téměř nemožné. V síti bez podpory HCF parametr *End To End delay* (absolutní zpoždění hlasového paketu, zpoždění = zpoždění přenosem sítí + kódovací zpoždění + dekódovací zpoždění + zpoždění kompresí + zpoždění dekompresí) postupně roste se zvyšující se zátěží v síti až k hranici dvou sekund, zatímco v síti s podporou HCF zůstává zpoždění malé a konstantní. Podobné výsledky se objevily i v ostatních grafech týkajících se hlasu, proto v nich nejsou data ze scénáře *HCF_OFF* zobrazena.



Obrázek 4.11 - *End to End Delay* pro Voice u *PC_1_1*

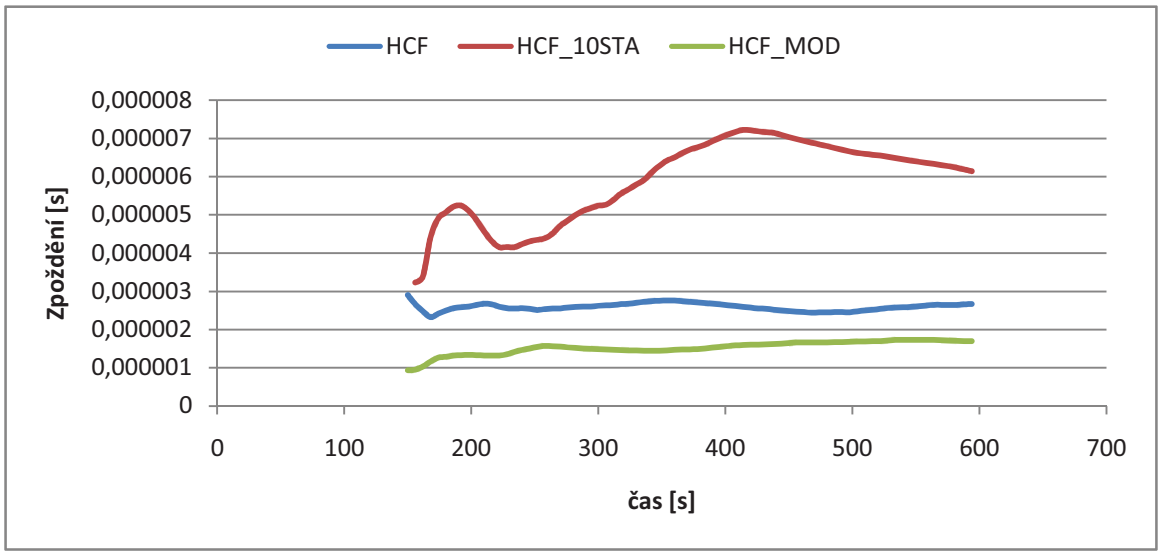
4.4.2 Více stanic v síti

Obrázek 4.0.1 ukazuje, že použití více stanic zvyšuje zpoždění *End To End Delay* hlasových paketů v síti. Obrázek 4.13 ukazuje vyšší hodnoty parametru *Packet Delay Variation* (rozdíly mezi *End To End* zpožděními jednotlivých paketů přijatých touto stanicí) pro hlasové pakety při použití více stanic v síti. Obrázky 4.14 a 4.15 zobrazují zpoždění přístupu k médiu pro jednotlivé kategorie provozu. Na Obrázku 4.14 je sice vidět, že v síti s deseti stanicemi čekají hlasové pakety na přístup k médiu delší dobu, ale rozdíl není nijak závratný. Více se rozdíl v počtu stanic projeví při čekání na přístup k médiu u paketů kategorie *Best Effort* (Obrázek 4.15). Díky velkému datovému toku této kategorie dat dochází k častějším kolizím a ucpání sítě.



Obrázek 4.0.12 - *End to End Delay* pro Voice pro celou síť

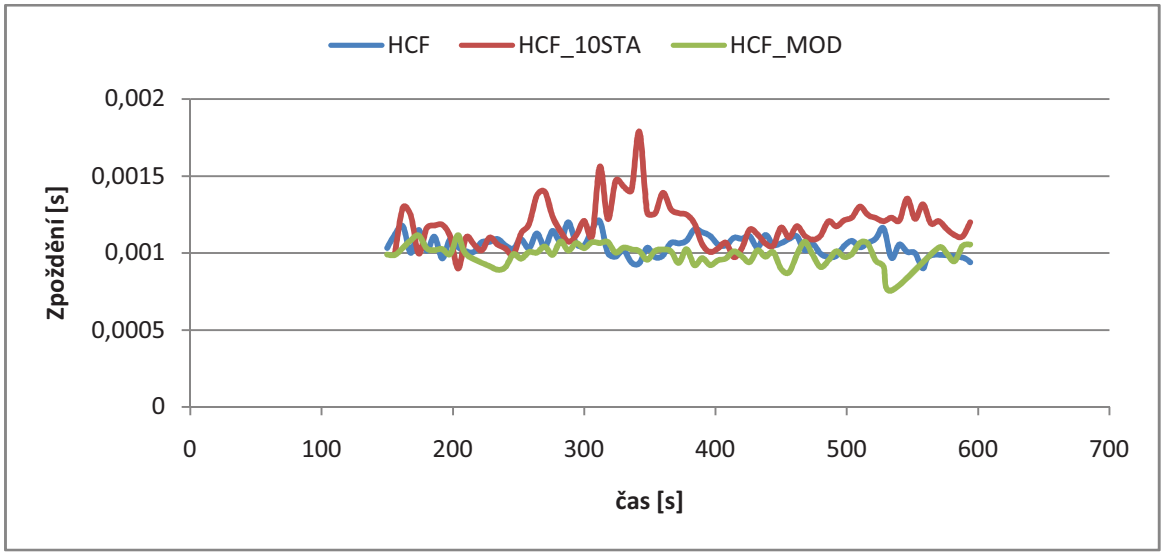
To potvrzuje i Obrázek A.4 (uveden v příloze), ze kterého je vidět, že v síti s deseti stanicemi dochází k největšímu zahazování paketů síťovými prvky. Obrázek A.1 a Obrázek A.2 (oba uvedeny v příloze) je možné dále vyčíst, že vyšší počet stanic neznamená nutně vyšší datovou prostupnost sítě. Při silném provozu naopak dochází ke kolizím a výsledný objem doručených dat může být tedy menší.



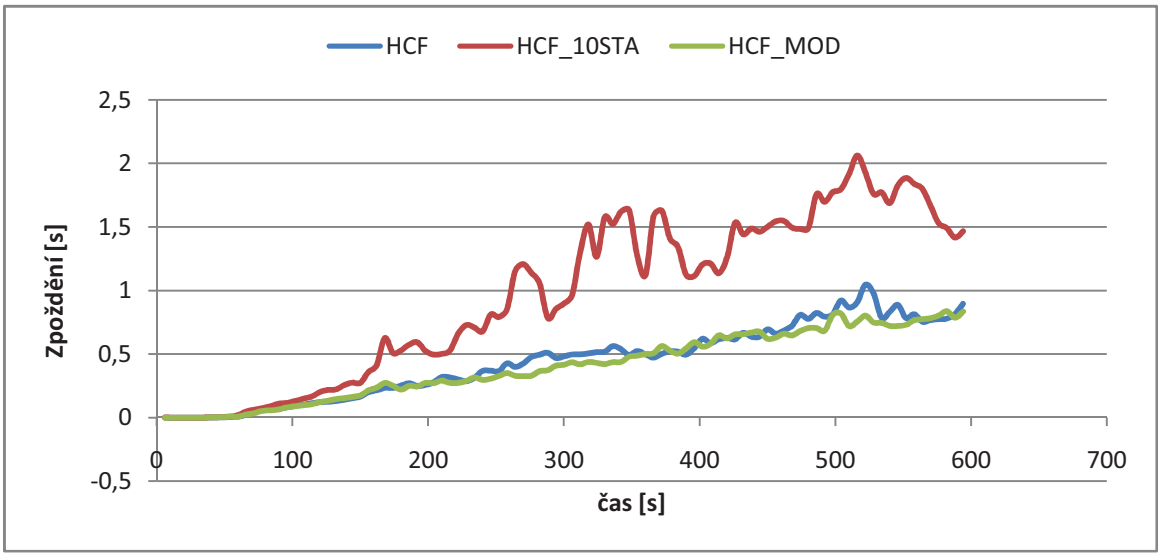
Obrázek 4.13 - *Packet Delay Variation* pro Voice pro celou síť

4.4.3 Pomalu rostoucí CW

Na Obrázcích 4.14, 4.15 nebo Obrázek A.3 (uveden v příloze) je rozdíl mezi hodnotami zpoždění přístupu k médiu mezi sítěmi s pomalu rostoucím CW a bez něj malý a přínos pomalu rostoucího CW je z těchto obrázků neprůkazný. Naproti tomu na Obrázcích Obrázek 4.0.12 a 4.13 je vidět, že v síti s pomalu rostoucím CW jsou celková zpoždění hlasových paketů menší a hlavně rozdíly zpoždění paketů jsou stabilnější.



Obrázek 4.14 - Zpoždění přístupu k médiu pro Voice



Obrázek 4.15 - Zpoždění přístupu k médiu pro Best Effort

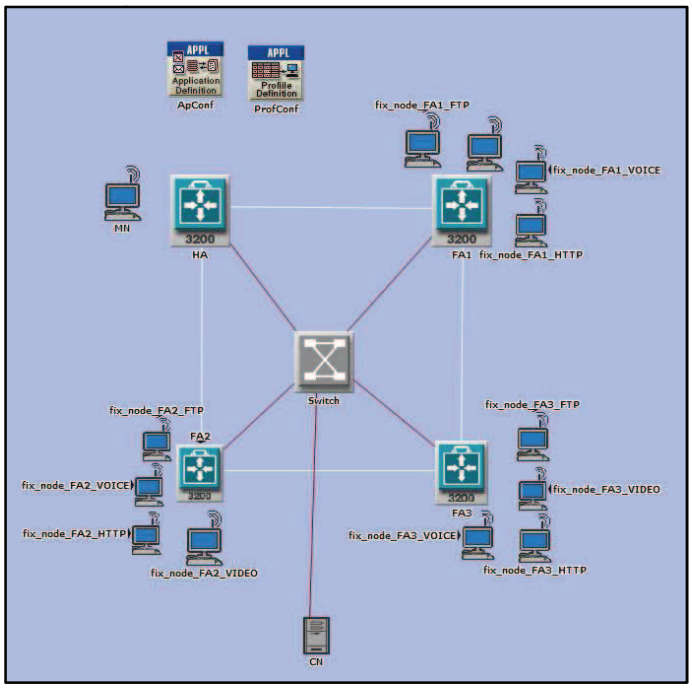
5 Simulace protokolu MIPv4 v prostředí OPNET Modeleru

5.1 Vytváření modelu

I když během práce na semestrálním projektu byl již v prostředí OPNET Modeleru vytvořen funkční model bezdrátové sítě s podporou QoS, pro simulaci mobility v bezdrátových sítích byl vytvořen model nový. Vytvoření zcela nového modelu, který by byl lépe přizpůsoben pro simulování protokolu Mobile IPv4 se jevilo jako lepší volba hlavně díky nutnosti nejprve funkci tohoto protokolu vyzkoušet na nezatížené síti bez jakýchkoli rušivých vlivů (datový provoz ostatních stanic). Po odladění funkčnosti samotného protokolu Mobile IPv4 byly poté do modelu základní sítě přidávány další stanice s nakonfigurovaným datovým provozem a vše bylo optimalizováno pro dosažení co nejlepších výsledků. Podpora QoS byla do tohoto modelu naimplementována až v závěrečné fázi práce.

Při vytváření modelu bezdrátové sítě se vycházelo z tutoriálu [7] pro OPNET Modeler, který slouží pro předvedení základních funkcí protokolu Mobile IPv4. Po zajištění základní funkcionality byl tento tutoriál dále upravován a rozšiřován.

Rozloha modelu tedy byla zvolena jako *Campus* [7], rozměry byly ponechány na 10 x 10 km (později bylo zjištěno, že tyto rozměry jsou pro úspěšnou simulaci protokolu Mobile IPv4 až příliš velké a rozestupy mezi jednotlivými komponenty byly zmenšeny). V základním modelu byly pro směrovače zvoleny objekty *mip_wlan_ethernet_slip4_agent* (jsou to objekty knihovny *mobile_ip* v okně *Object Palette Tree*), které přímo podporují protokol Mobile IPv4. Jeden ze směrovačů byl určen jako Home Agent (domácí síť pro mobilní stanici - MN), ostatní pak jako Foreign Agenti. Pro propojení těchto směrovačů byl zvolen přepínač *ethernet16_switch* opět z knihovny *mobile_ip*. Objekt *wlan_wkstn* z knihovny *wireless_lan* je použit pro všechny koncové bezdrátově připojené stanice. Zde je obzvláště nutné, aby byl pro mobilní stanici MN použit typ objektu *Mobile Node*. U typu *Fixed Node* není možné definovat trajektorii pro pohyb stanice. Ke každému směrovači, který funguje pro MN jako Foreign Agent, byly přiřazeny čtyři bezdrátové stanice s nastavenými datovými přenosy. Pro server je pak použit objekt *ethernet_server* z knihovny *internet_toolbox*. Použitou topologii ukazuje Obrázek 5.1.



Obrázek 5.1 - Topologie pro simulaci protokolu Mobile IPv4

5.2 Základní konfigurace síťových prvků a aplikací

5.2.1 Vytvoření aplikací a profilů:

U každého směrovače byly umístěny čtyři bezdrátově připojené stanice, provozující čtyři různé datové komunikace (každá z jiné přístupové kategorie) – hlas, video, HTTP a FTP. Potřebné nastavení pro podporu těchto aplikací bylo provedeno pomocí objektu *Application Config*. Obrázky Obrázek 5.2, Obrázek 5.3, Obrázek 5.4 a Obrázek 5.5 ukazují nastavení těchto aplikací.

Attribute: Application Definitions.Description [0].Ftp

Command Mix	75%
Inter-Request Time	exponential (5)
File Size	constant (50000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back-End Custom Application	Not Used

Obrázek 5.2 - Nastavení aplikace FTP

Attribute: Application Definitions.Description [1].Http

HTTP Specification	HTTP 1.1
Page Interarrival Time	exponential (60)
Page Properties	(...)
Server Selection	(...)
RSVP Parameters	None
Type of Service	Background (1)

Attribute: Application Definitions.Description [1].Http.Page Properties

Index	Object Size	Number of Objects	Location	Back-End Custom Application	Object Group Name
0	constant (1000)	constant (1)	HTTP Server	Not Used	Not Used
1	Medium Image	constant (5)	HTTP Server	Not Used	Not Used

Attribute: Application Definitions.Description [1].Http.Server Selection

Initial Repeat Probability	Browse
Pages Per Server	exponential (10)

Obrázek 5.3 - Nastavení aplikace HTTP

Attribute: Application Definitions.Description [2].Video Conferencing

Frame Interarrival Time Information	10 frames/sec
Frame Size Information	128X120 pixels
Symbolic Destination Name	Video Destination
Type of Service	Interactive Multimedia (5)
RSVP Parameters	None
Traffic Mix	All Discrete

Obrázek 5.4 - Nastavení aplikace Video

Attribute: Application Definitions.Description [3].Voice

Silence Length	default
Talk Spurt Length	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.729 A
Voice Frames per Packet	1
Type of Service	Interactive Voice (6)
RSVP Parameters	None
Traffic Mix	All Discrete
Signaling	None
Compression Delay	0.02
Decompression Delay	0.02
Conversation Environment	(...)

Attribute: Application Definitions.Description [3].Voice.Conversation Environment

Incoming Conversation Environment	Land phone - Quiet room
Outgoing Conversation Environment	Land phone - Quiet room

Obrázek 5.5 - Nastavení aplikace Voice

V objektu *Profile Config* byly nastaveny profily pro podporu jednotlivých aplikací (viz. Obrázek 5.6 – vždy jeden profil pro jednu aplikaci).

Attribute: Profile Configuration

Index	Profile Name	Applications	Operation Mode	Start Time	Duration	Repeatability
0	FTPprof	(...)	Serial (Ordered)	uniform (100,110)	End of Simulation	Once at Start Time
1	HTTProf	(...)	Serial (Ordered)	uniform (10, 11)	End of Simulation	(...)
2	VIDEOProf	(...)	Serial (Ordered)	uniform (100,110)	End of Simulation	Once at Start Time
3	VOICEProf	(...)	Serial (Ordered)	uniform (10, 11)	End of Simulation	(...)

Obrázek 5.6 - Nastavení objektu *Profile Config*

Aplikace a profily byly nastaveny tak, aby stanice připojené ke směrovačům označeným jako FA vytvořily dostatečný datový provoz (nikoli však až příliš velký, který by způsoboval zahlcení sítě) složený z různých přístupových kategorií, což pomůže ke sledování vlivu QoS.

5.2.2 Konfigurace síťových uzlů

Jednotlivým směrovačům byly přiděleny identifikátory sítě SSID (hodnoty 1 až 4) a poté bylo potřeba zajistit, aby hodnoty identifikátorů SSID u jednotlivých stanic odpovídaly hodnotám SSID směrovačů, se kterými mají tyto stanice komunikovat. Pokud by si totiž navzájem hodnoty SSID neodpovídaly, ke komunikaci by nedošlo. Poté mohly být všem síťovým uzlům přiděleny IP adresy pomocí volby v menu *Protocols-> IP-> Addressing-> Auto-Assign IPv4 Addresses* [7].

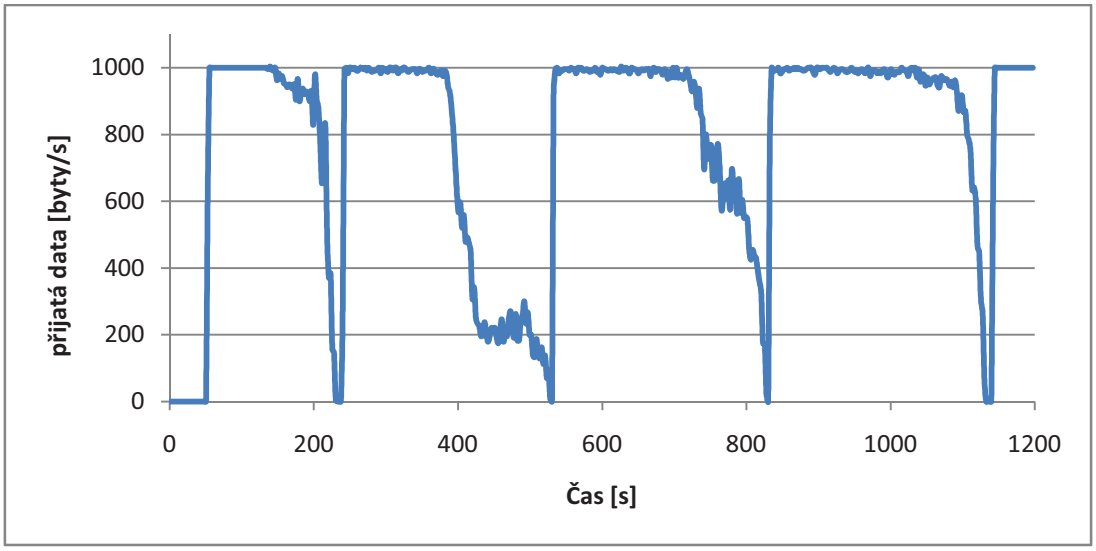
Jednotlivé stanice byly poté nakonfigurovány pro podporu profilů pomocí položky *Application-> Supported Profiles* (každá podporuje jeden profil). Mobilní stanice MN podporuje profil *VOICEProf*, což jí umožňuje provoz IP telefonie. Každá ze stanic u ostatních směrovačů je nakonfigurována pro jednu z aplikací FTP, HTTP, Video a Voice. Jako cílový bod komunikace pro všechny stanice byl pomocí položky *Application-> Destination Preferences* zvolen server CN, na kterém byly také pomocí položky *Application-> Supported Services* povoleny všechny dostupné aplikace.

Pro zajištění podpory protokolu Mobile IPv4 ve scénáři byla u směrovače HA v položce *Mobile IPv4 Parameters-> Interface Information* pro bezdrátové rozhraní *IF1* nastavena hodnota parametru *Agent type* na hodnotu *Home Agent*. Pro směrovače FA 1 – 3 byl tento parametr nastaven na hodnotu *Foreign Agent*. Dále musela být u stanice MN nastavena v položce *Mobile IPv4 Parameters* adresa Home Agenta (v tomto případě IP adresa směrovače HA).

Pro zajištění pohybu byla stanici MN přiřazena definovaná trajektorie ve tvaru čtverce (ukazuje ji Obrázek 5.1 – bílá barva), procházející všemi čtyřmi směrovači (jedna hrana stanici trvá 5 minut – celková doba simulace je tedy 20 minut).

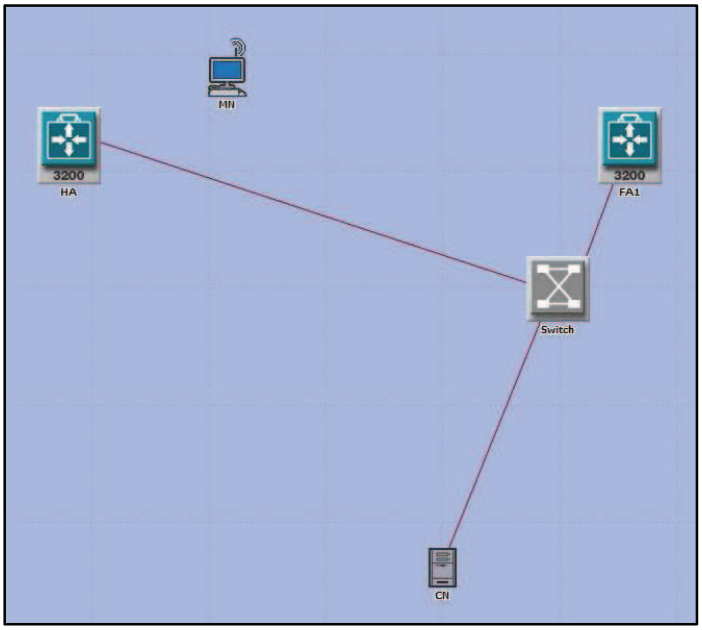
5.3 Nastavování výkonu a polohy AP

Zpočátku byla mobilita testována ve scénáři *Mobility* pouze s komunikující stanicí MN. Po připojení ostatních stanic se projevily v datovém provozu aplikace Voice u stanice MN značné výpadky komunikace (jak ukazuje Obrázek 5.7), které se nedařilo odstranit. Jako příčina se začala jevit vzdálenost mezi jednotlivými směrovači, která v našem původním modelu byla několik kilometrů a mobilní stanice MN se tudíž pohybovala rychlostí několika desítek kilometrů za hodinu, což mohlo způsobovat nestabilitu.

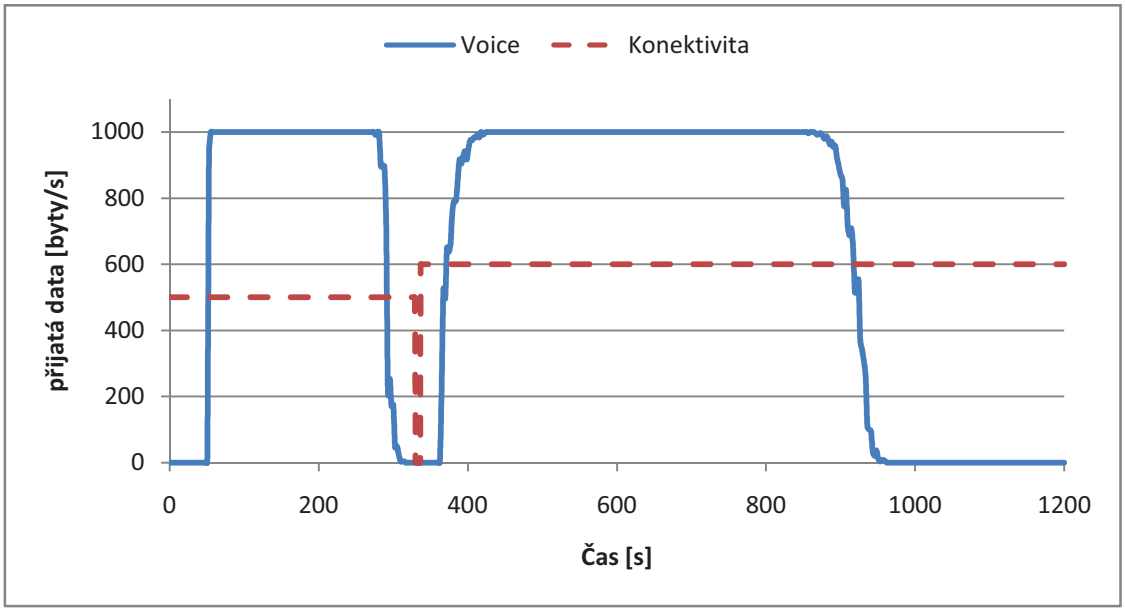


Obrázek 5.7 - Výpadky komunikace u datového provozu aplikace Voice stanice MN

Při určování nových poloh jednotlivých směrovačů hrála roli právě rychlost pohybu MN při simulaci, která měla dosahovat zhruba 5 kilometrů za hodinu. Ideální polohy směrovačů jsme určili díky pomocnému scénáři, ve kterém jsme nechali pouze MN, a dva směrovače připojené k serveru CN pomocí přepínače (Obrázek 5.8). Trajektorie stanice MN byla upravena tak, aby stanice putovala po přímce vedoucí oběma směrovači. Postupným upravováním vzájemné vzdálenosti obou směrovačů, vysílacího výkonu směrovačů i MN (parametr *Wireless LAN Parameters-> Transmit Power*) a hodnoty úrovně signálu, při které je signál ze směrovače považován za špatný a dojde k handoveru (pouze u MN, parametr *Wireless LAN Parameters-> Packet Reception-Power Threshold*) jsme získali optimální průběh datového provozu aplikace *Voice* (příklad špatného nastavení ukazuje Obrázek 5.9, optimální výsledek pak Obrázek 5.10, v grafech jsou zobrazeny i doby, ve kterých je MN připojena k jednotlivým směrovačům – přerušovaná čára).



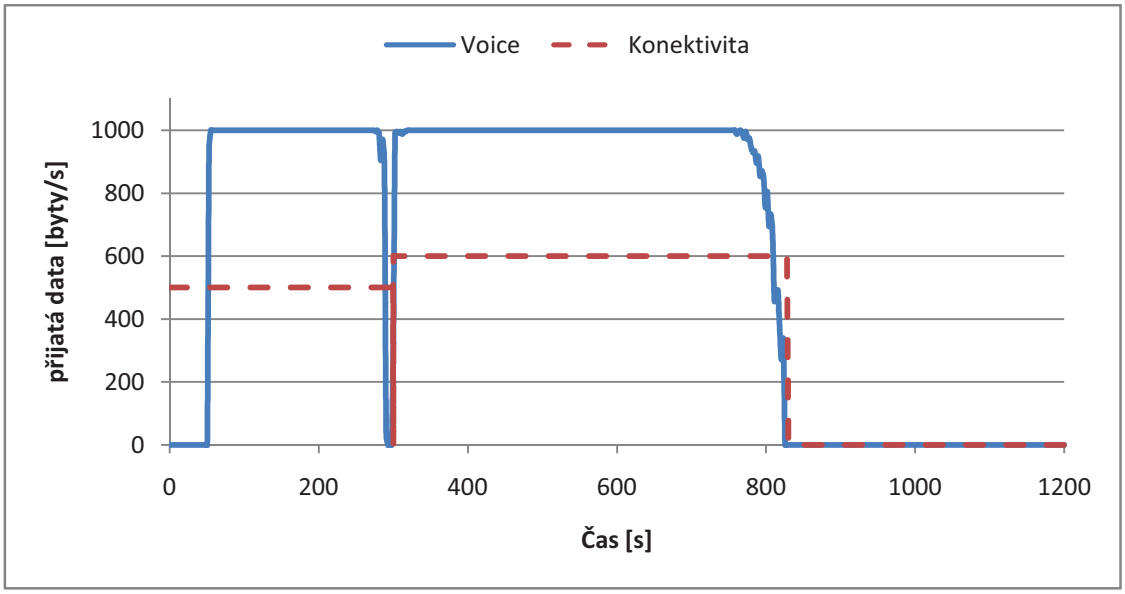
Obrázek 5.8 - Topologie při nastavování výkonu



Obrázek 5.9 - Nastavování výkonu a polohy AP – začátek

Optimální hodnoty všech nastavovaných parametrů byly určeny takto:

- **Vzdálenost dvou sousedních směrovačů:** 400 m
- **Vysílací výkon směrovačů:** 0,005 W
- **Vysílací výkon stanice:** 0,005 W
- **Rozhodovací hladina:** -80 dBm



Obrázek 5.10 - Nastavování výkonu a polohy AP – výsledek

5.4 Použité scénáře

V této kapitole budou stručně nastíněny jednotlivé simulované scénáře a jejich účel:

- **Mobility:**
  Toto je původní scénář použitý pro základní zprovoznění protokolu Mobile IPv4. Vychází z tutoriálu v literatuře [7] a problémy s tímto scénářem a jeho následná úprava je popsána v kapitole 5.3.
- **HCF OFF:**
  Tento scénář ukazuje simulaci protokolu Mobile IPv4 bez podpory QoS.
- **HCF:**
  Oproti scénáři *HCF OFF* zajišťuje podporu QoS. V simulacích tedy bude jednoduché pozorovat rozdíly při podpoře QoS a bez zajištění této podpory.
- **Bridge mode:**
  Tento scénář byl vytvořen pro porovnání mobility na síťové vrstvě referenčního modelu ISO/OSI (tuto mobilitu představují výše popsané scénáře) a mobility na linkové vrstvě. Pro zajištění simulace mobility na linkové vrstvě byly směrovače nahrazeny pomocí přepínačů v bridge modu (objekt *wlan_eth_bridge* ve složce *wireless_lan* ve stromu *Object Palette Tree*), takže všechny zařízení při této konfiguraci pracují ve stejné podsíti a nedochází k handoveru na síťové vrstvě. Pro vytvoření topologie ESS by měly mít všechny Bridge stejné číslo SSID, pokud však byla spuštěna simulace s tímto nastavením, došlo k chybě a simulace byla zastavena (popis chyby ukazuje Obrázek 5.11). Proto bylo nastavení SSID ponecháno stejné, jako při použití směrovačů. V tomto případě bylo ale nutné manuálně natavit IP adresy všech uzlů, protože automatické přidělování IP adres nefungovalo korektně (rozdělilo dostupné stanice do několika podsítí).

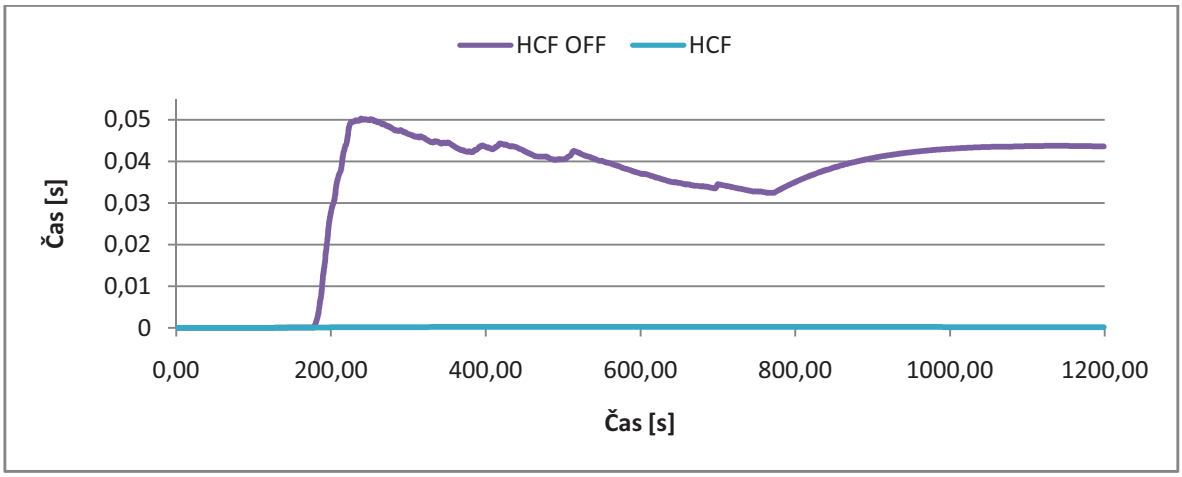
```
Beginning simulation of Mobile_QOS-bridgeMode at 10:39:52 Thu Apr 23 2009
----
Kernel: development (not optimized), sequential, 32-bit address space
----
Simulation terminated by process (wlan_mac_hcf) at module (top.Campus
Network.MN.wireless_lan_mac), T (0), EV (106)
Error reported by Wireless LAN MAC process:
More than one Access Point found within the same BSS (BSS ID = 1)
or in the same OPNET subnet.
Check the configuration.
----
Simulation Completed - Collating Results.
Events: Total (129); Average Speed (68 events/sec.)
Time  : Elapsed (1.9 sec.); Simulated (0.00 sec.)
DES Log: 2 entries

----
```

Obrázek 5.11 - Neúspěšná simulace

5.5 Výsledky simulací

5.5.1 Použití IEEE 802.11e

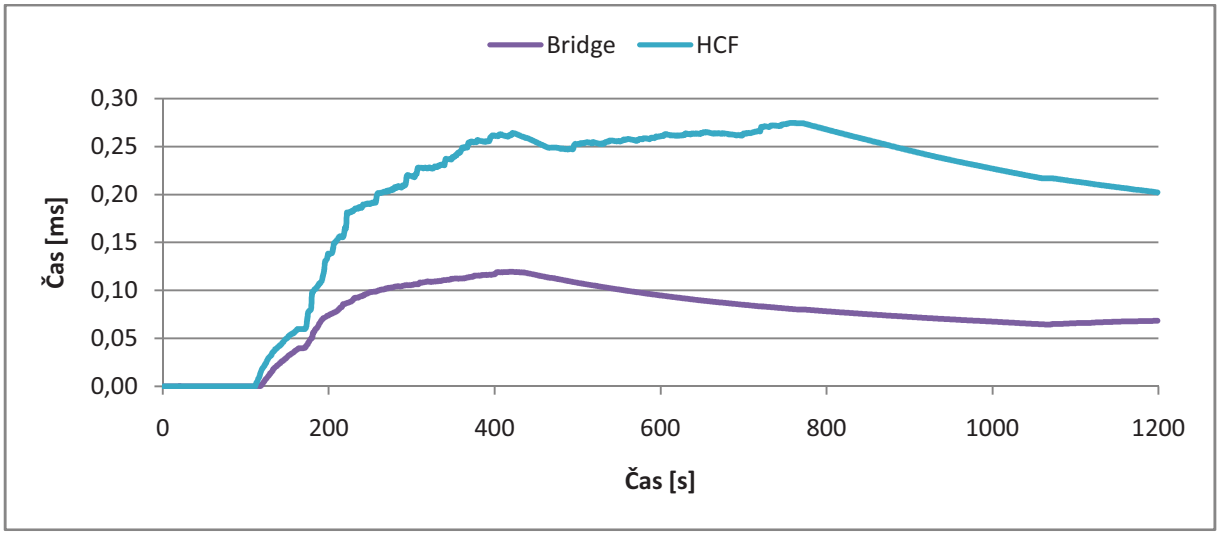
Obrázek 5.12 a Obrázek B.1 (uveden v příloze) ukazují, že přesně podle předpokladů z kapitoly QoS jsou při aktivní podpoře protokolu Mobile IPv4 průběhy parametrů *End to End Delay* (popis v kapitole 4.4.1) a *Packet Delay Variation* (popis v kapitole 4.4.2) pro hlas výrazně horší ve scénáři bez podpory QoS. Hlasové pakety nejsou bez QoS před ostatními pakety nijak upřednostňovány a proto je celková doba jejich zpracování příliš dlouhá. Parametr *End to End Delay* má místy hodnotu vyšší než 0,5 sekundy, což by neumožnilo provozovat kvalitní telefonní hovor.



Obrázek 5.12 - *Packet Delay Variation* pro celou síť

5.5.2 Mobilita na síťové a linkové vrstvě

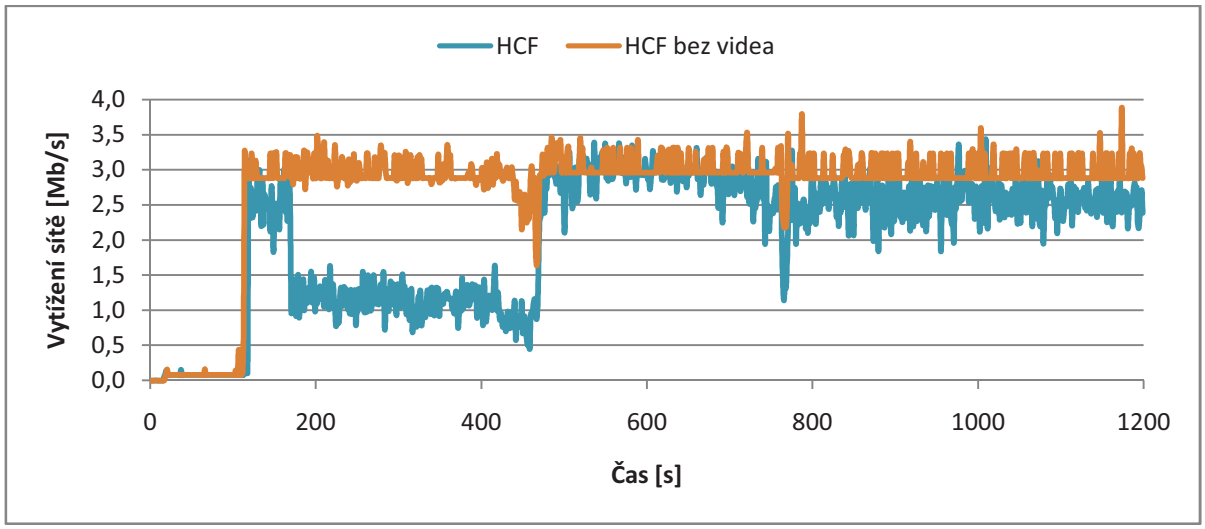
Při mobilitě na linkové vrstvě jsou všechny stanice ve stejné podsíti, proto by se dalo předpokládat, že díky menšímu administrativnímu provozu v síti a kvůli absenci směrovačů budou vlastnosti mobility na linkové vrstvě celkově lepší. Obrázek 5.13 ukazuje, že hodnoty parametru *Packet Delay Variation* předpoklady potvrzují. Průběh tohoto parametru je ve scénáři *Bridge* výrazně lepší. Lepších vlastností dosahuje mobilita na linkové vrstvě i u parametru *End to End Delay* (Obrázek B.2 - uveden v příloze) a je také dosaženo lepšího a stabilnějšího přenosu hlasových paketů (Obrázek B.3 - uveden v příloze).



Obrázek 5.13 - Packet Delay Variation pro Voice v celé síti

5.5.3 Problémy při simulaci

Při simulaci protokolu Mobile IPv4 došlo při použití uvedené topologie k několika problémům. Co se týče rychlosti handoveru, který se pohyboval v jednotkách sekund (optimální hodnotou by byly maximálně stovky milisekund, aby nedocházelo ke znatelnému přerušení aplikací pracujících v reálném čase), je pravděpodobné, že další změny konfigurace by jej dokázaly ještě více snížit. Dalším problémem byl výrazný pokles celkového objemu přenesených dat v síti ve chvíli, kdy se ze sítě odpojila mobilní stanice MN. O to podivnější byl tento problém i kvůli tomu, že postihoval pouze sítě s BSS 2 a 4. Komunikace v síti s BSS = 3 probíhala normálně (Obrázek B.4 - uveden v příloze). Tento nechtěný pokles se nepodařilo odstranit ani zvětšením vyrovnávací paměti na serveru, nastavováním parametrů IRDP protokolu atd. Obrázek 5.14 ukazuje pokles objemu přenesených dat v síti s BSS = 4 (tento pokles nastane ve chvíli, kdy je MN připojena k síti s BSS = 2). Pokud byl ze sítě s BSS = 2 smazán počítač přenášející video, k poklesu přenášených dat v síti s BSS = 4 již nedošlo (i toto je vidět z Obrázek 5.14).



Obrázek 5.14 – Celkové zatížení podsítě s BSS = 4

6 Závěr

Výsledky simulací v prostředí OPNET Modeler podle předpokladů potvrdily, že implementace standardu IEEE 802.11e má pozitivní vliv na provoz aplikací pracujících v reálném čase. V síti bez podpory tohoto standardu běžně dosahovalo celkové zpoždění hlasových paketů i několika vteřin, což neumožňuje vedení telefonního hovoru.

Více stanic v síti má podle očekávání na sledované parametry negativní vliv. V síti s deseti stanicemi došlo ke zhoršení všech parametrů zpoždění. Zajímavé je, že díky implementaci IEEE 802.11e nebyl nárůst zpoždění přístupu k médiu pro hlasové pakety nijak dramatický a za povšimnutí stojí také, že pravděpodobně díky kolizím a zpožděním v síti je celkový objem přenesených dat v této síti dokonce menší než při použití jen pěti stanic.

Některé sledované statistiky prokázaly pozitivní vliv pomalu rostoucího CW na zpoždění hlasových paketů v síti, u některých statistik je přínos téměř zanedbatelný. Síť s pomalu rostoucím CW vykazuje viditelně lepší statistiky stabilnějších zpoždění snad jen u parametru Packet Delay Variation pro hlasové pakety a proto není nutné se dále touto modifikací nijak detailně zabývat.

Co se týče mobilní IP adresy, bylo předvedeno, že protokol Mobile IPv4 lze v prostředí OPNET Modeleru simulovat bez větších problémů.

Podle předpokladu implementace standardu IEEE 802.11e všeobecně zlepší statistiky přenosu pro pakety s větší prioritou a umožní tak například úspěšné provozování IP telefonie. Ve scénářích bez implementace tohoto standardu celkové zpoždění hlasových paketů mnohdy přesahovalo 0,5 sekundy, což by velice degradovalo (ne-li zcela znemožnilo) telefonní hovor. Vzájemná součinnost protokolu Mobile IPv4 a standardu IEEE 802.11e je v prostředí OPNET Modeleru možná. Obě technologie se vzájemně doplňují a v případě společného nasazení mohou být nasazeny globálně a rozšířit možnosti IP telefonie.

Simulace ukázala, že s mobilitou založenou pouze na linkové vrstvě se dá dosáhnout lepších výsledků sledovaných parametrů (což se ale dá předpokládat díky úbytku administrativy v síti a úbytku směrovačů). Ale právě již ze své podstaty tento druh mobility neumožňuje přepojení do jiné podsítě a proto je nevhodná ke globálnímu nasazení.

Během simulace protokolu Mobile IPv4 došlo také k několika problémům (popsány výše), které by pravděpodobně byly odstranitelné další prací zaměřenou přímo na jejich řešení.

7 Citovaná literatura

1. **GAST, M.** *802.11 Wireless Networks: The Definitive Guide, Second Edition.* Sebastopol : O'Reilly Media, 2005. ISBN: 978-0596100520.

2. **PRASAD, N., PRASAD, A.** *802.11 WLANs and IP Networking: Security, QoS, and Mobility.* London : Artech House Publishers, 2005. ISBN: 1580537898.

3. **Tanenbaum, Andrew S.** *Computer Networks.* New Jersey : Pearson Education, 2003.

4. **PERKINS, Charles E.** Mobile IP. *IEEE Communications Magazine.* 2002, Sv. 40, 5, stránky 66-82. Dostupný z WWW:

<http://www.ee.oulu.fi/~skidi/teaching/mobile_and_ubiquitous_multimedia_2002/Perkins.pdf>.

5. **RAAB, S., CHANDRA, M.** *Mobile IP Technology and Applications.* Indianapolis : Cisco Press, 2005. ISBN: 978-1587051326.

6. **XI, Weihua Helen, WHITLEY, Toby, MUNRO, Alistair, BARTON, Michael.** *Modeling and Simulation of MAC for QoS in IEEE 802.11e Using OPNET Modeler.* Bristol : University of Bristol, Networks & Protocols Group, CCR, Department of Electrical & Electronic Engineering.

7. **MOLNÁR, Karol, ZEMAN, Otto, SKOŘEPA, Michal.** *Moderní síťové technologie: Laboratorní cvičení, 2. revize.* Brno : VUT v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008.

8. **SKOŘEPA, M.** Podpora mobility v sítích s IPv4. *Elektrorevue - Internetový časopis.* 2007, Sv. 2007, 50, stránky 1-9.

9. **OPNET Technolopgies, Inc.** *Understanding Wireless LAN Model Internals and Interfaces, Discrete Event Simulation for R&D.* Washington D. C. : OPNETWORK, 2007.

10. **MOLNÁR, Karol.** *Zajištění kvality služeb v bezdrátových a mobilních sítích.* Brno : VUT v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008.

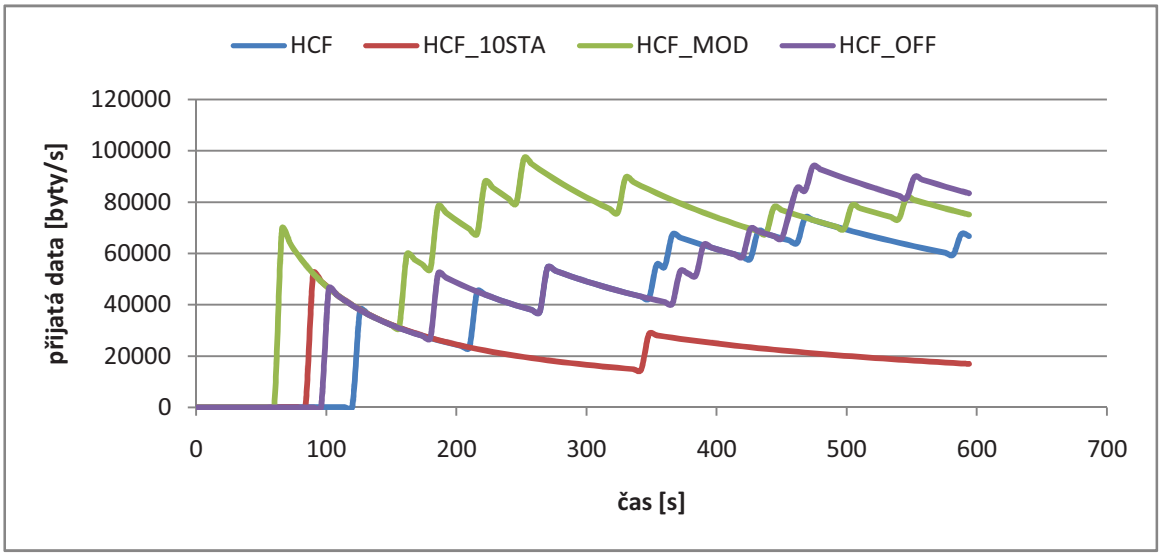
8 Seznam použitých zkratek

802.11	standard pro bezdrátové sítě
AC	*Access category;* přístupová kategorie
ACM	*Admission control mandatory;* parametr povinné kontroly přístupu
AIFS	*Arbitration IFS;* mezirámcová mezera výběru
AP	*Access point;* přístupový bod do bezdrátové sítě
BSS	*Basic service set;* základní sada služeb
CAP	*Controlled access phase;* fáze kontrolovaného přístupu
CCoA	*Colocated CoA;* MN má přímo IP adresu platnou v síti
CN	*Correspondent node;* pomocné označení PC, které komunikuje s MN
CoA	*Care of Address;* platná IP adresa MN v cizí síti
CP/ CFP	*Contention period/Contention-free period;* doba s/bez soutěžení o médium
CW	*Contention Windows;* okno soutěžení
CSMA/CA	*Carrier sense multiple access/collision avoidance;* přístup k médiu s naslouch. nosné
DCF	*Distributed coordination function;* distribuovaná koordinační funkce
DIFS	*Distributed coordination function IFS;* mezirámcová mezera pro DCF
EDCA	*Enhanced distributed channel access;* část HCF, přístup k médiu na základě soutěžení
EOSP	*End of service period;* konec obslužné doby
FA	*Foreign Agent;* směrovač v cizí síti, který je schopen ukončit tunel místo MN
FA CoA	*Foreign Agent CoA;* IP adresa rozhraní FA přidělená MN jako CoA
HA	*Home Agent;* směrovač v domácí síti, u kterého je registrována MN
HC	*Hybrid coordinator;* hybridní koordinátor
HCCA	*HCF controlled channel access;* část HCF, kontrolovaný přístup k médiu
HCF	*Hybrid coordination function;* hybridní koordinační funkce
ICMP	*Internet Control Message Protocol;* typicky pro odesílání chybových zpráv, ping
IEEE	*Institute of electrical and electronic engineers*
IP	*Internet Protocol;* Datový protokol používaný pro přenos dat přes paketové sítě
IP-in-IP	protokol použitelný pro tunelování v protokolu Mobile IPv4
IRDP	*ICMP Router Discovery Protocol;* protokol pro vzájemnou komunikaci směrovačů
ISO/OSI	referenční síťový model pro dělení sítě na 7 vrstev
LAN	*Local area network;* místní síť
MAC	*Medium access control;* vrstva modelu ISO/OSI starající se o přístup k médiu
MN	*Mobile Node;* mobilní stanice s podporou protokolu zajišťujícího mobilitu
Mobile IPv4	protokol zajišťující mobilitu v sítích založených na protokolu IPv4
PC	*Point coordinator;* centrální koordinátor
PCF	*Point coordination function;* centralizovaná koordinační funkce
PHY	*Physical layer;* fyzická vrstva ISO/OSI modelu
PIFS	*Point coordination function IFS;* mezirámcová mezera pro PCF
POLL	rámec výzvy, kterým QAP vyzívá stanici k odeslání dat
PSTN	*Packet switched telephone network;* standardní veřejná telefonní síť
QAP	*QoS enhanced AP;* AP s podporou QoS
QBSS	*QoS supporting BSS;* BSS s podporou QoS
QoS	*Quality of service;* kvalita služby

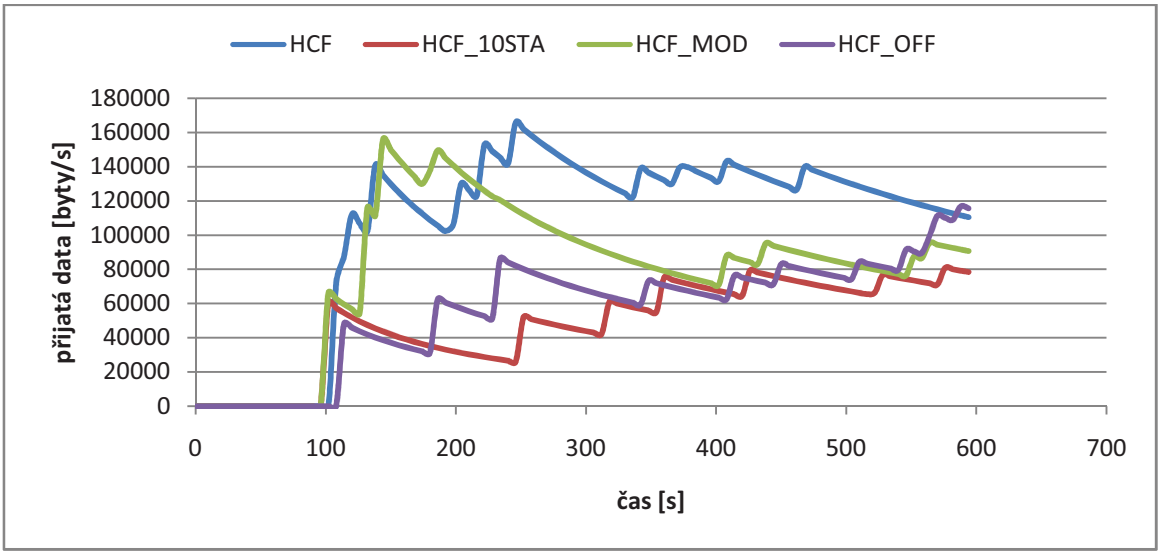
QSTA	*QoS enabled STA;* stanice podporující QoS
RRP	*Registration reply;* zpráva protokolu IRDP, odpověď na žádost o registraci
RRQ	*Registration request;* zpráva protokolu IRDP, žádost o registraci
RTS/CTS	*Request-to-send/ Clear-to-send;* rámec žádosti o výhradní přístup/rámec potvrzení
SP	*Service period;* obslužná doba
TC	*Traffic category;* kategorie provozu
TID	*Traffic ID;* identifikátor provozu
TS	*Traffic stream;* proud dat
TSID	*Traffic stream ID;* identifikátor proudu dat
TSPEC	*Traffic specification;* specifikace provozu
TTL	*Time to Live;* udává, po kolika průchodech přes směrovač bude paket zahozen
TXOP	*Transmission oportunity;* čas, kdy má stanice práva pro přenos dat
UP	*User priority;* uživatelská priorita
VoIP	*Voice over IP;* protokol pro podporu hlasové komunikace přes IP síť
VoWLAN	*Voice over WLAN;* protokol pro podporu hlasové komunikace v bezdrátových sítích
WLAN	*Wireless local area network;* bezdrátová místní síť

9 Seznam příloh

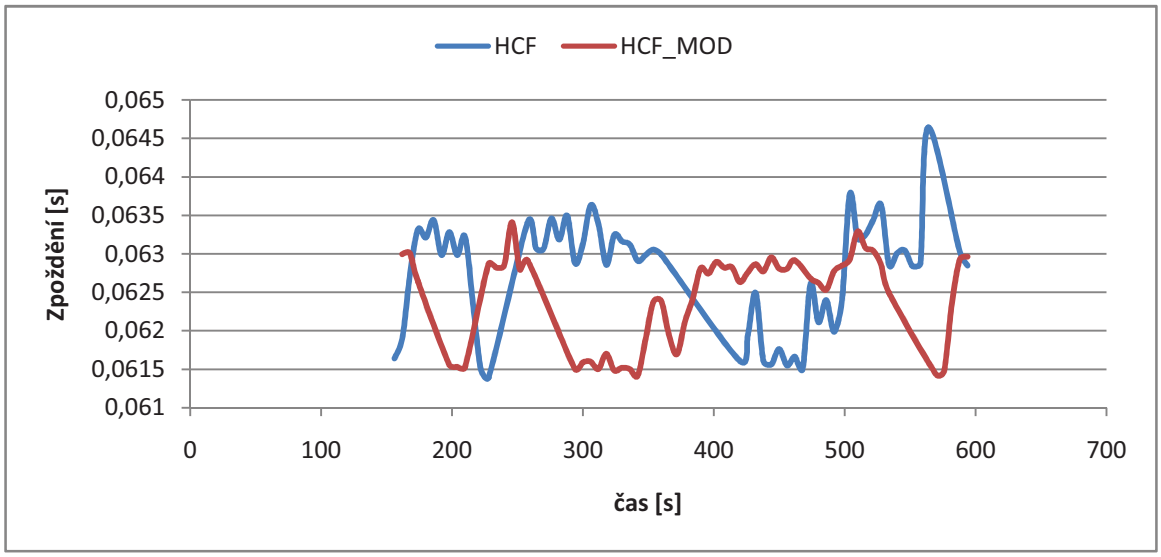
A Výsledky simulací standardu IEEE 802.11e



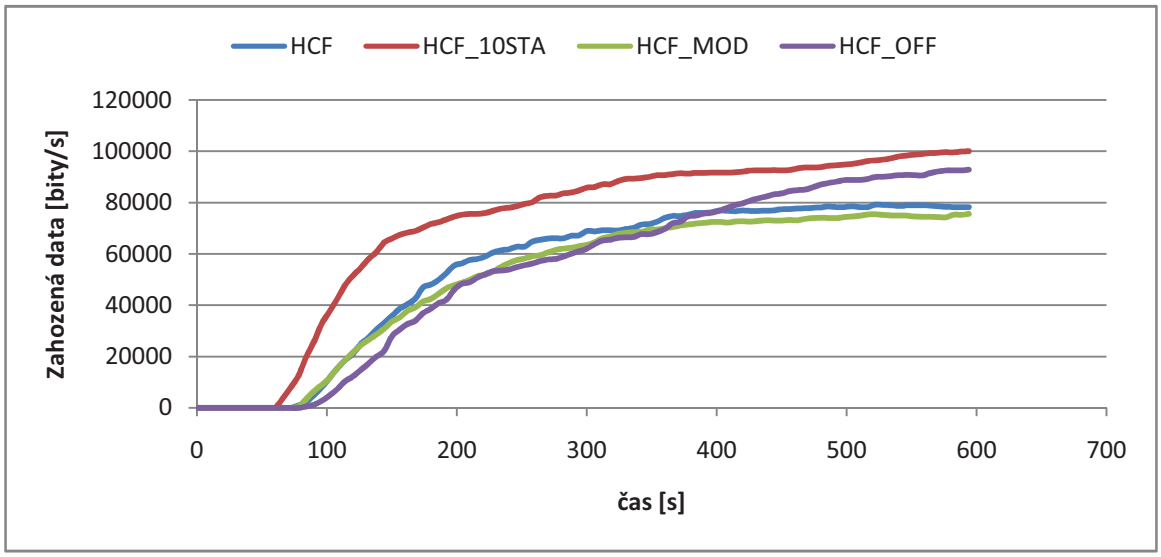
Obrázek A.1 - Data přenesená pomocí FTP



Obrázek A.2 - Data přenesená pomocí http

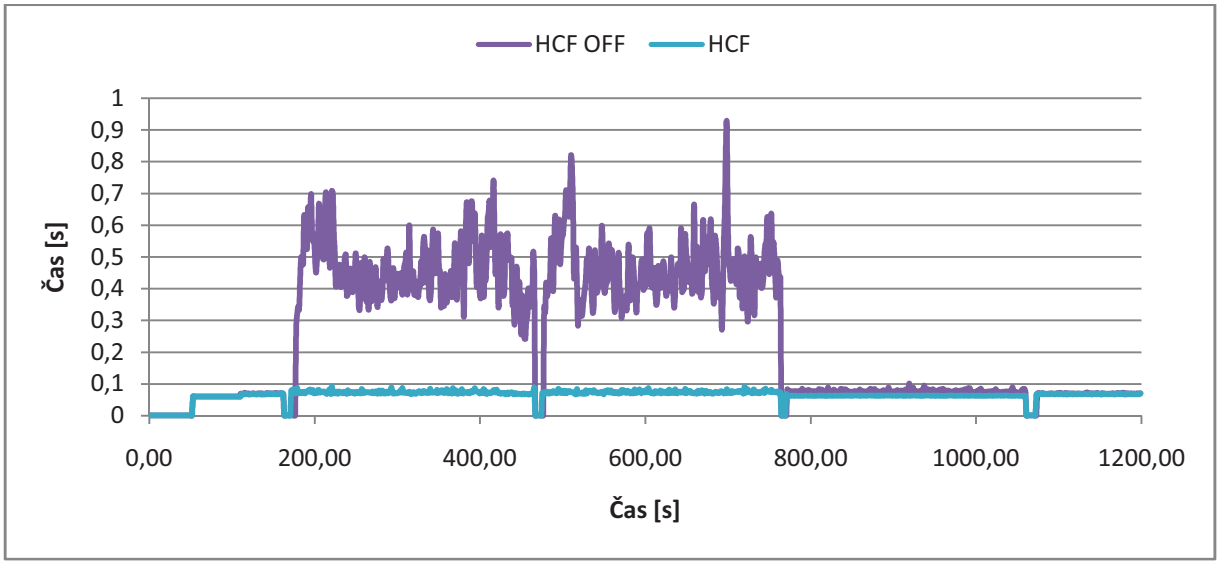


Obrázek A.3 - End to End zpoždění pro Voice na PC_1_1

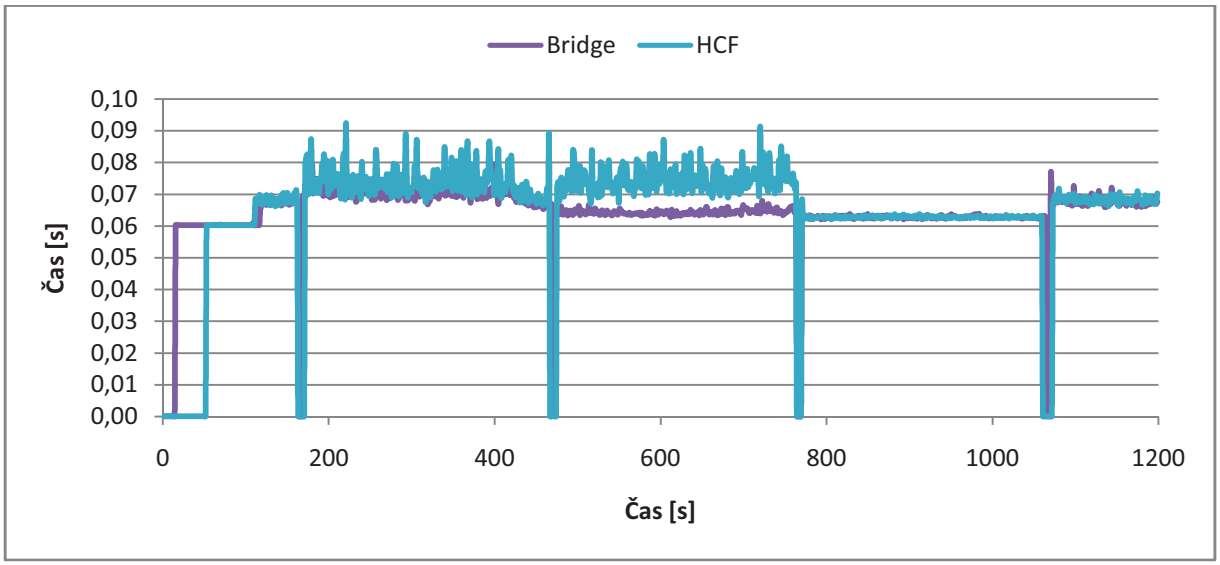


Obrázek A.4 - Data zahozená v celé síti

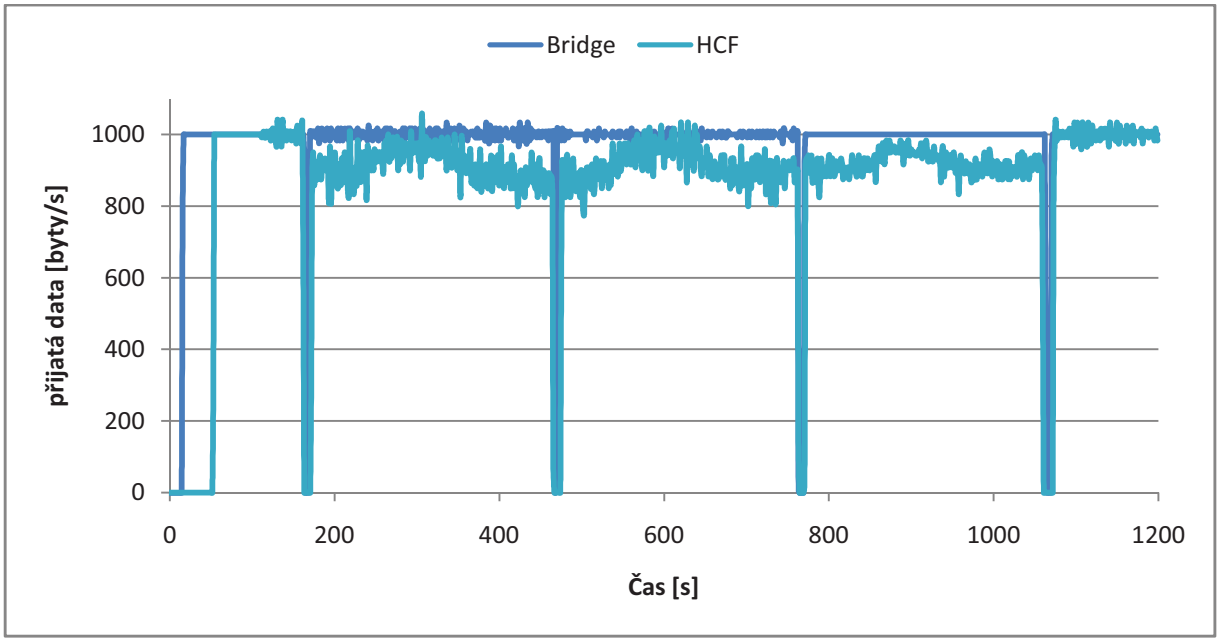
B Výsledky simulací protokolu Mobile IPv4



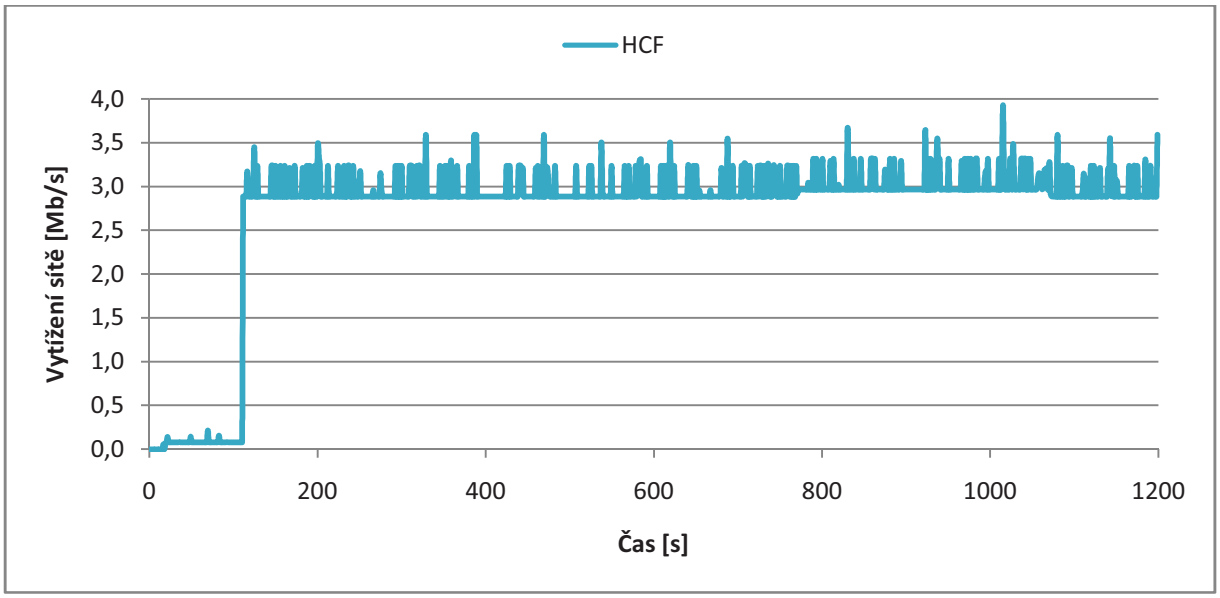
Obrázek B.1 - End to End delay pro Voice v celé síti



Obrázek B.2 - End to End delay pro Voice v celé síti



Obrázek B.3 - Přijatá hlasová data pro stanici MN



Obrázek B.4 - Celkové zatížení sítě s BSS = 3