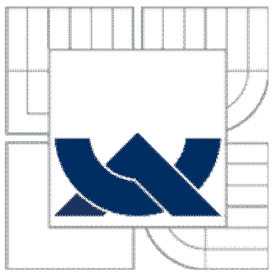
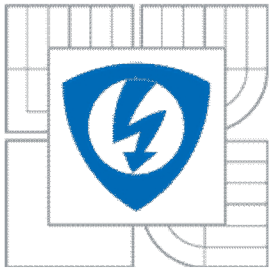


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MAPOVÁNÍ QOS POŽADAVKŮ NA SÍŤOVÉ PROSTŘEDÍ

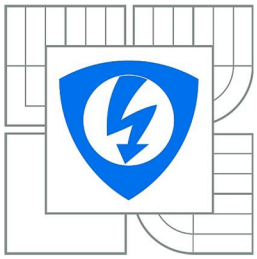
MAPPING OF QOS REQUIREMENTS ON THE NETWORK LEVEL

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE
AUTHOR
Bc. ZBYNĚK KONEČNÝ

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. TOMAŠ MÁCHA

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Zbyněk Konečný ***ID:*** 100277
Ročník: 2 ***Akademický rok:*** 2010/2011

NÁZEV TÉMATU:

Mapování QoS požadavků na síťové prostředí

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je prostudovat základní QoS mechanismy, dále IP vrstvu a architekturu IMS (IP Multimedia Subsystem). Student se bude zabývat návrhem sítí s DiffServ a IntServ doménami společně s IMS subsystémem a větším počtem koncových uživatelů. Tyto návrhy sítí a jejich následná simulace bude provedena v simulačním prostředí OPNET Modeler. Součástí bude také analýza výsledků simulací a zhodnocení mapování.

DOPORUČENÁ LITERATURA:

[1] POIKSELKA, M.; MAYER, G.; KHARTABIL, H.; NIEMI, A. The IMS: IP Multimedia Concepts and Services in the Mobile Domain. England: WILEY, 2004. 448 p. ISBN-10 0-470-87113-X.

[2] CAMARILLO, G.; GARCÍA-MARTÍN, M. A. The 3G IP Multimedia Subsystem (IMS) - Merging the Internet and the Cellular Worlds. Third Edition. England: WILEY, 2008. 618 p. ISBN-13 978-0-470-51662-1.

[3] GÓMEZ, G.; SÁNCHEZ, R. End-to-End Quality of Service over Cellular Networks. Data Services Performance and Optimization in 2G/3G. WILEY. 2005. 317p. ISBN-13 978-0-470-01180-5.

Termín zadání: 7.2.2011 ***Termín odevzdání:*** 26.5.2011

Vedoucí práce: Ing. Tomáš Mácha

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

ANOTACE

Problematikou konvergovaných sítí je dostatečné zajištění kvality služeb po celé délce komunikačního přenosu. Tato problematika je úzce spjata se službami pracujícími v reálném čase, jako jsou VoIP (Voice over Internet Protocol) a videokonference. Tyto služby vyžadují striktní dodržení kvalitativních parametrů, v opačném případě není jejich funkce zaručena. Tento problém do jisté míry řeší subsystém IMS (IP Multimedia Subsystem), který na základě sjednaných uživatelských profilů dokáže požadovanou kvalitu služeb zajistit.

Teoretická část se proto zaobírá popisem vlastní struktury tohoto systému a protokoly určenými pro signalizaci v této síti. Dále jsou popsány jednotlivé mechanismy pro podporu kvality služeb, a to jak v přístupových, tak v páteřních sítích. V následující části je vysvětlen princip ustanovení kvalitativních požadavků mezi koncovými uživateli sítě.

V praktické části jsou získané teoretické znalosti využity k návrhu a konfiguraci sítě, skládající se z různých technologií. Výsledný model je odsimulován v programu Opnet Modeler, který slouží pro návrh a testování paketových sítí. Na jednotlivých simulacích je znázorněn vliv mapování kvalitativních požadavků v jednotlivých přístupových sítích na technologie, které jsou podporovány v páteřní síti.

Výstupem práce je podrobná analýza síťové komunikace a srovnání mechanizmů pro implementaci kvality služeb. V závěru budou shrnuty výsledky dosažených simulací.

Klíčová slova: IMS, QoS, IntServ, DiffServ, VoIP

ABSTRAKT

The issue of converged networks is to ensure the sufficient quality of services along the entire length of the communication transmission. This issue is closely connected to the real-time services, such as VoIP (Voice over Internet Protocol) and videoconferencing. These services require strict adherence to quality parameters, otherwise their function is not guaranteed. This problem particulary resolves subsystem IMS (IP Multimedia Subsystem), which concluded on the basis of user profiles can provide the required quality of service.

Therefore the theoretical part deals with the description of the structure of the system and protocols designed to signal the network. Various mechanisms to support quality of services in access and backbone networks are also described. The following section explains the principle of provision of quality requirements of end-user networks.

In the practical part is this theoretical knowledge used for designing and configuration of the network consisting of various technologies. The resulting model is then simulated in Opnet Modeler program, which is used for designing and testing of packet networks. Each simulation shows the effect of mapping quality requirements in the different access network on technologies, which are supported in the backbone.

The outcome of this work is detailed network analysis and comparison of mechanisms for implementing quality of service. The conclusion summarises all simulation outcomes.

Keywords: IMS, QoS, IntServ, DiffServ, VoIP

KONEČNÝ, Z. *Mapování QoS požadavků na síťové prostředí. Brno*: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 73 s. Vedoucí diplomové práce Ing. Tomáš Mácha.

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma „Mapování QoS požadavků na síťové prostředí“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a 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 práce Ing. Tomášovi Máchovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne ....

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Diplomová práce s názvem: „Mapování QoS požadavků na síťové prostředí“ je zaměřena na problematiku subsystému IMS (IP Multimedia Subsystem) a kvalitu služeb QoS (Quality of Service). V teoretické části budou popsány jednotlivé funkční bloky architektury IMS a vrstvová struktura tohoto subsystému.

Dále budou pospány jednotlivé protokoly, které jsou nedílnou součástí této architektury. Jedná se především o protokoly SIP (Session Initiation Protocol), SDP (Session Description Protocol) a Diameter.

Dalším stěžejním bodem této práce bude vzájemné srovnání dvou mechanismů, které zajišťují požadovanou kvalitu služeb. Jedná se o technologie DiffServ a IntServ, proto je těmto službám věnovaná značná část v teoretickém úvodu.

Následující kapitola stručně popisuje simulační prostředí Opnet Modeler a jeho základní bloky, které se dají použít pro modelování rozmanitých sítí nebo vlastních protokolů.

Hlavní kapitola se zabývá konfigurací a následné simulaci vytvořeného modelu sítě. Tato síť se skládá z páteřní sítě, kde bude vzájemně propojeno linkou 10Base_T několik směrovačů, a z různých přístupových sítí. Tyto přístupové sítě budou typu UMTS (Universal Mobile Telecommunication System), Ethernet a Wi-Fi. Síť je zatížena následujícími aplikacemi: FTP (File Transfer Protocol), HTTP (Hyper Text Transfer Protocol), VoIP (Voice over Internet Protocol) a videokonference. Každá tato služba má rozdílné potřeby na šířku přenosového pásma, zpoždění, kolísání zpoždění a ztrátovost paketů. Všechny tyto služby jsou společně odsimulovány ve čtyřech scénářích. První scénář modeluje síť bez použití kvalitativních požadavků. Druhý scénář podporuje technologii DiffServ, ale pouze v páteřní síti. To znamená že jednotlivé přístupové sítě nebudou mít správně namapovány jednotlivé nosné služby k plné podpoře kvality služeb. Třetí scénář bude obsahovat plnou podporu kvality služeb. Znamená to, že kvalita služeb bude nastavena po celé komunikační trase přes různé přístupové sítě. Poslední scénář je duplikován a mírně modifikován tak, že podporuje technologie IntServ. Zde tedy bude vyjednána rezervace síťových zdrojů za pomoci rezervačního protokolu.

V závěru je do infrastruktury navržené sítě implementován subsystému IMS, který by měl zaručit registraci koncových uživatelů a vyjednání patřičné kvality služby podle profilu uloženého v databázi operátora. Ke všem zmiňovaným simulacím jsou přiloženy patřičné konfigurace a výsledky dosažené simulaci. Jednotlivé dosažené výsledky jsou v dílčích kapitolách podrobně popsány a shrnuty v závěru.

1 IMS (IP MULTIMEDIA SUBSYSTEM)

Systém IMS je nové vylepšení stávající UMTS. Toto vylepšení by mělo vést ke sjednocení a centralizaci služeb využívajících paketový přenos dat.

V UMTS existují dva základní druhy přenosu zpráv, a to paketově spínaná část a okruhově spínaná část. Jelikož je spínání okruhů neefektivní, je snaha včlenit služby této části do paketové sítě.

IMS je tedy systém, který dokáže efektivně poskytovat rozmanitou škálu služeb, např.: hlasové služby, video služby, služby s multimediálním obsahem atd. Technologie IMS je navržena tak, aby pokryla veškeré potřeby klientů a poskytovatelů, tzn. je zde velmi propracovaná QoS (Quality of Service), je kladen velký důraz na bezpečnost sítě, dále je zde možnost různých druhů účtování za poskytované služby.

Koncept IMS je dobře škálovatelný a obsahuje širokou paletu různých protokolů. Jádro sítě IMS je tvořeno skupinou SIP (Session Initiation Protocol) serverů, které komunikují s klienty za pomoci SIP protokolu přes síťový protokol IP (Internet Protocol). Služba IMS zahrnuje jak komunikaci přes pevnou, mobilní tak i bezdrátovou síť. Konkrétně se jedná o přístupy, jako jsou:

- GSM (Global System for Mobile communications),
- WCDMA (Wideband Code Division Multiple Access),
- CDMA 2000 (Code-Division Multiple Access),
- WLAN (Wireless Local Area Network),
- ADSL (Asymmetric Digital Subscriber Line),
- WiMAX (Worldwide Interoperability for Microwave Access) [1, 3].

1.1 VRSTVOVÝ MODEL IMS

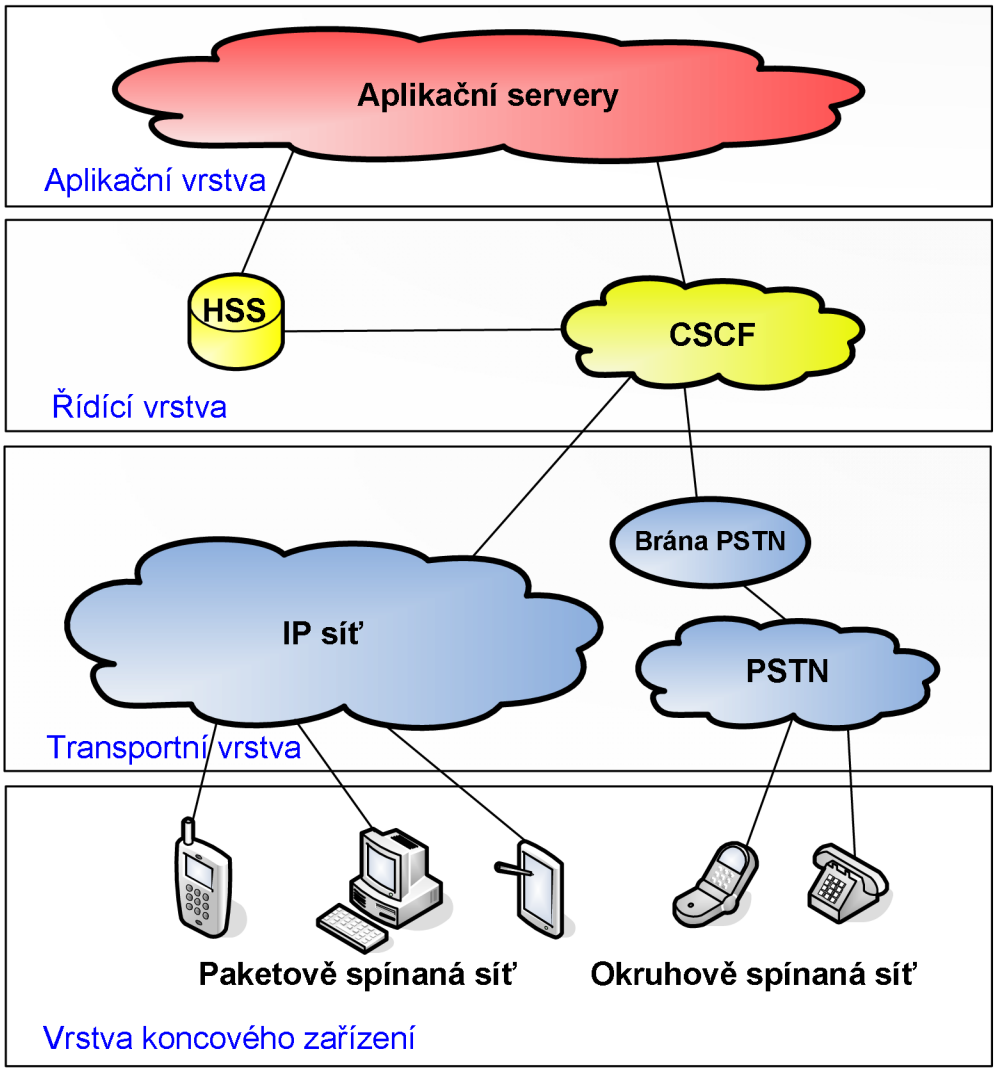
Subsystém IMS lze rozdělit do čtyř základních vrstev, které jsou vrstva koncového zařízení, transportní vrstva, řídící vrstva a aplikační vrstva. Jednotlivé vrstvy jsou znázorněny na Obr. 1.1.

1.1.1 Vrstva koncového zařízení

Tato vrstva je nejnižší vrstva celého modelu. Jak již bylo řečeno, IMS umožňuje velké spektrum přístupů do sítě. Na Obr. 1.1 jsou znázorněny dva možné přístupy do sítě. První je pro zařízení poskytující paketový přenos dat. Tyto zařízení se mohou připojit přímo do IP sítě. Druhá skupina jsou zařízení používající spínání okruhů. Zařízení tohoto typu se musí do IP sítě případně do IMS subsystému připojit přes PSTN (Public Switched Telephone Network) bránu. [1, 2].

1.1.2 Transportní vrstva

Transportní vrstva obsahuje směrovací a řídící prvky, které umožňují přenášet informace skrz IP síť. Dále pak poskytuje konverzi z analogové do digitální podoby a naopak. Transportní vrstva pracuje na IP vrstvě v referenčním modelu ISO/OSI a umožňuje připojení různorodých koncových zařízení. [1, 2].



Obr. 1.1 Vrstvový model IMS [2]

1.1.3 Řídící vrstva

O řídící vrstvě se dá říct, že je jádrem subsystému IMS. Obsahuje hlavní komponenty tohoto systému, jako jsou SIP servery např.: CSCF (Call Session Control Function), databáze HSS (Home Subscriber Server) a SLF (Subscriber Location Function). Servery CSCF se starají o registraci uživatelů, o přesměrování komunikace a o zabezpečení sítě. Naproti tomu databáze HSS obsahuje profily uživatelů, které mohou obsahovat uživatelskou IP adresu, telefonní záznamy, seznam přátel, možné nastavení QoS atd. Hlavním protokolem pracujícím na této vrstvě je SIP a Diameter. Řídící vrstva zprostředkovává tyto hlavní služby:

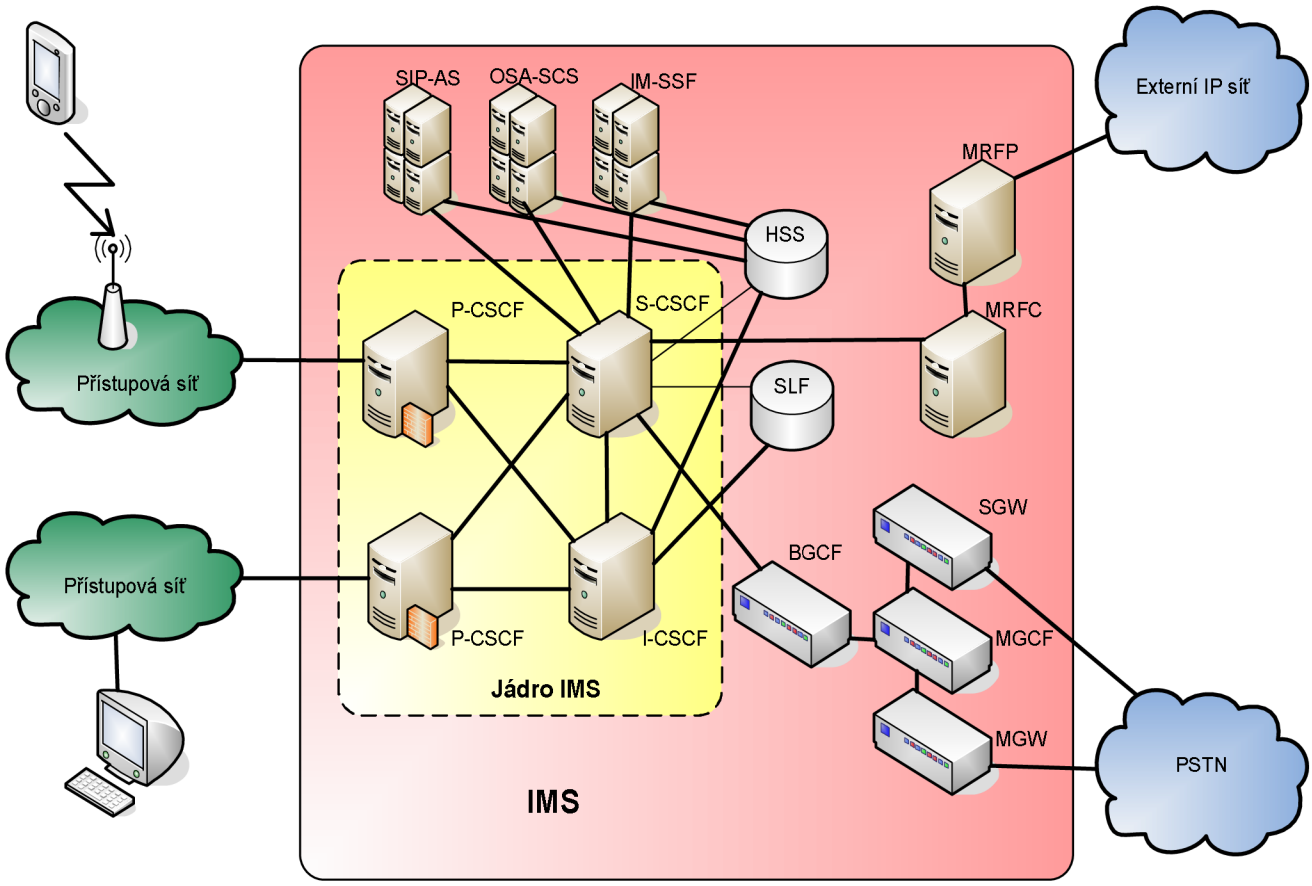
- správa mobility,
- správa údajů o platbách,
- navázání spojení,
- udržení spojení,
- ukončení spojení. [1, 2].

1.1.4 Aplikační vrstva

Tato vrstva je ve vrstvovém modelu IMS na nejvyšším místě. Na této vrstvě pracují aplikační servery, které poskytují uživatelům rozmanité služby na základě signalizačního SIP protokolu. Na jednom serveru může společně kooperovat více aplikací. např. správa videokonference, SIP server pro telefonii, služba zasílání zpráv atd. [1, 2].

1.2 ARCHITEKTURA IMS

Jednotlivé prvky architektury IMS lze rozdělit do několika skupin, které mohou obsahovat jednu či více daných entit. V subsystému se nachází databáze HSS a SIP servery se společným názvem (CSCF). Dále síť obsahuje tyto služby: aplikační servery (AS), MRFP (Multimedia Resource Function Procesor), MRFC (Multimedia Resource Function Control), bloky pro vzájemnou vnitřní komunikaci a řízení, BGCF (Breakout Gateway Control Function), MGCF (Multimedia Gateway Control Function), IM-MGW (IMS Media GateWay), SGW (Signaling GateWay). Dalšími prvky jsou podpůrné bloky jako SEG (SEcurity Gateway), PDF (Policy Decision Function), THIG (Topology Hiding Inter-working Gateway) a také bloky pro účtování. Všechny tyto prvky budou v následující části detailně popsány. Architektuta IMS je zobrazena na Obr. 1.2. [3]



Obr. 1.2 Architektuta IMS sítě [1, 4]

1.2.1 CSCF (Call Session Control Function)

Tento server bývá spolu s databází HSS označen za jádro celého systému IMS. Zkratka CSCF je souhrnný název, který obsahuje další servery dělící se podle způsobu zpracování SIP signalizace.

P-CSCF (Proxy - Call Session Control Function)

Server P-CSCF je prvním CSCF serverem, který stojí mezi IMS klientem a sítí. Z pohledu SIP architektury vystupuje jako příchozí i odchozí SIP Proxy server.

Pokud se terminál chce registrovat do dané IMS sítě, je mu přidělen P-CSCF server. Po celou dobu registrace komunikuje terminál se stejným P-CSCF serverem, který mu tedy byl přidělen při přihlášení do sítě.

Jelikož není v IP síti zaručena autentičnost zprávy, je nutné, aby existovala entita, která tuto autentičnost zajistí i skrze IP síť. Toto zabezpečení je umožněno díky protokolu IPsec. Server P-CSCF před samotným spojením s IMS terminálem zabezpečí komunikační kanál, tím zajistí integritu dat. Jakmile P-CSCF autentizuje uživatele, může začít komunikace i uvnitř IMS subsystému. Jelikož je P-CSCF považován sítí jako důvěryhodný zdroj, není již dále třeba ověřovat autentičnost zpráv i uživatele. Další schopností P-CSCF je ověřování správné syntaxe SIP zpráv. Pokud objeví chybu, danou zprávu nepropustí dál do vnitřní sítě. Tím zabrání zahlcení vnitřních prvků irelevantními zprávami.

Velice důležitou vlastností P-CSCF vzhledem k různorodé škále přístupových metod je komprese a dekomprese SIP zpráv. Jelikož je protokol SIP textově orientovaný, není nikterak omezen, co se týče objemu nesených zpráv. Komprese se používá z důvodu využití IMS služeb pro mobilní terminály, které jsou omezeny šířkou pásma radiového prostředí. Server P-CSCF tedy provede kompresi zprávy, zašle zprávu příjemci a ten ji následně dekomprimuje. Tímto se podstatně zmenší zpoždění vzniklé zasíláním dlouhých SIP zpráv.

P-CSCF může zahrnovat entitu pro rozhodování o politice PDF (Policy Decision Function). Tato služba může být tedy přímo součástí P-CSCF nebo funguje jako samostatný blok. PDF má za úkol autorizaci zdroje a řízení QoS (Quality of Service).

V rámci IMS koexistuje několik serverů P-CSCF, a to kvůli zálohování jednotlivých serverů a také kvůli větší propustnosti. [1, 3]

I-CSCF (Interrogating - Call Session Control Function)

Jedná se o dotazovací SIP server. Tento server reprezentuje kontaktní bod domovské IMS sítě. Spojení, která přicházejí do dané sítě IMS od jiného operátora, prochází přes domovský I-CSCF. Tento server se následně spojí pomocí protokolu Diameter s databází HSS, případně SLF (Subscription Locator Function), která obsahuje informace o dotazovaném účastníkovi. Následně je z HSS získána příslušná adresa serveru S-CSCF dotazovaného uživatele. Dále jsou SIP zprávy směrovány přes tento S-CSCF server. Další funkcí I-CSCF je volitelné šifrování SIP zpráv, které mohou obsahovat informace o vnitřní struktuře IMS jako je např.: počet serverů v dané doméně a jejich DNS (Domain Name System) jména. Tato funkce se nazývá THIG (Topology Hiding Inter-network Gateway) a její použití je volitelné. [1, 3]

S-CSCF (Serving - Call Session Control Function)

Server S-CSCF je centrálním bodem subsystému IMS. Na základě informací zjištěných pomocí protokolu Diameter z databáze HSS určuje vlastnosti spojení. V domovské síti operátora se může vyskytovat i více S-CSCF serverů. Jeden z důvodů výskytu více serverů je, že tento server je nejvíce vytěžován oproti ostatním IMS serverům. Zvýšením počtu serverů

dosáhneme rozmělnění provozu a zvýšení propustnosti sítě. Dalším důvodem je, že každý S-CSCF server může vykonávat jinou funkci. Hlavní funkce serveru je zpracovávání registračních požadavků a uchovávání záznamů o spojení jako je IP adresa a SIP adresa uživatele. S-CSCF dále směruje příchozí SIP zprávy k daným aplikačním serverům. Server S-CSCF také umožňuje překlad telefonního čísla na URI (Uniform Resource Identifikator) adresu a naopak. [1, 3]

1.2.2 HSS (Home Subscriber Server)

Databáze HSS je centrálním úložištěm uživatelských informací. Skládá z dvou hlavních částí: HLR (Home Location Register) a AuC (Authentication Center). Prvek HLR je domovský registr, který uchovává informace o uživatelích patřících k dané ústředně. HLR podporuje jak paketové tak okruhově spojované sítě. Naproti tomu prvek AuC slouží pro autentizaci terminálu a obsahuje tajné klíče k tomu určené. Dále AuC poskytuje službu zajištění integrity a šifrování dat mezi koncovým uživatelem a IMS subsystémem.

V HSS jsou uložena různá přístupová práva, identifikační údaje, profily a informace o poloze terminálu, a to pro každého registrovaného uživatele. Dále HSS uchovává informaci o právě přiděleném serveru S-CSCF.

Existují dva typy identifikátorů uživatele IMS subsystému. První je soukromý identifikátor, v kterém jsou uložené informace spojené s registrací uživatele a autorizací. Tyto informace používá výhradně síť. Druhým typem je veřejný identifikátor, který slouží k nastavení vzájemné komunikace. např.: oznámení připojení uživatele atd.

Zabezpečení dat uložených v domovské síti je provedeno tak, že HSS neposkytuje uložené informace S-CSCF serverům, které leží v jiné IMS síti. Tato ochrana je docílena prvky P-CSCF a I-CSCF. Komunikace mezi HSS a jinými entitami probíhá pomocí protokolu Diameter.

V případě, že se v IMS nachází více HSS, je nutné, aby existoval prvek, který bude přesně vědět, kde se jaké informace nachází. Toto zajišťuje entita SLF. [1, 3]

1.2.3 SLF (Subscriber Location Function)

Pokud se v jedné IMS doméně nachází více databází HSS, je nutno použít prvek SLF. Ten mapuje uživatelovu adresu na adresu příslušného HSS, které obsahuje potřebné informace o uživateli. Síť s SLF pak funguje tak, že severy I-CSCF, S-CSCF a nebo AS posílají dotazy na SLF místo přímo na HSS. SLF obdrží na vstupu adresu uživatele a na výstup předá informaci, v jakém HSS se uživatel nachází. Databáze SLF komunikuje s ostatními entitami pomocí protokolu Diameter. [1, 3]

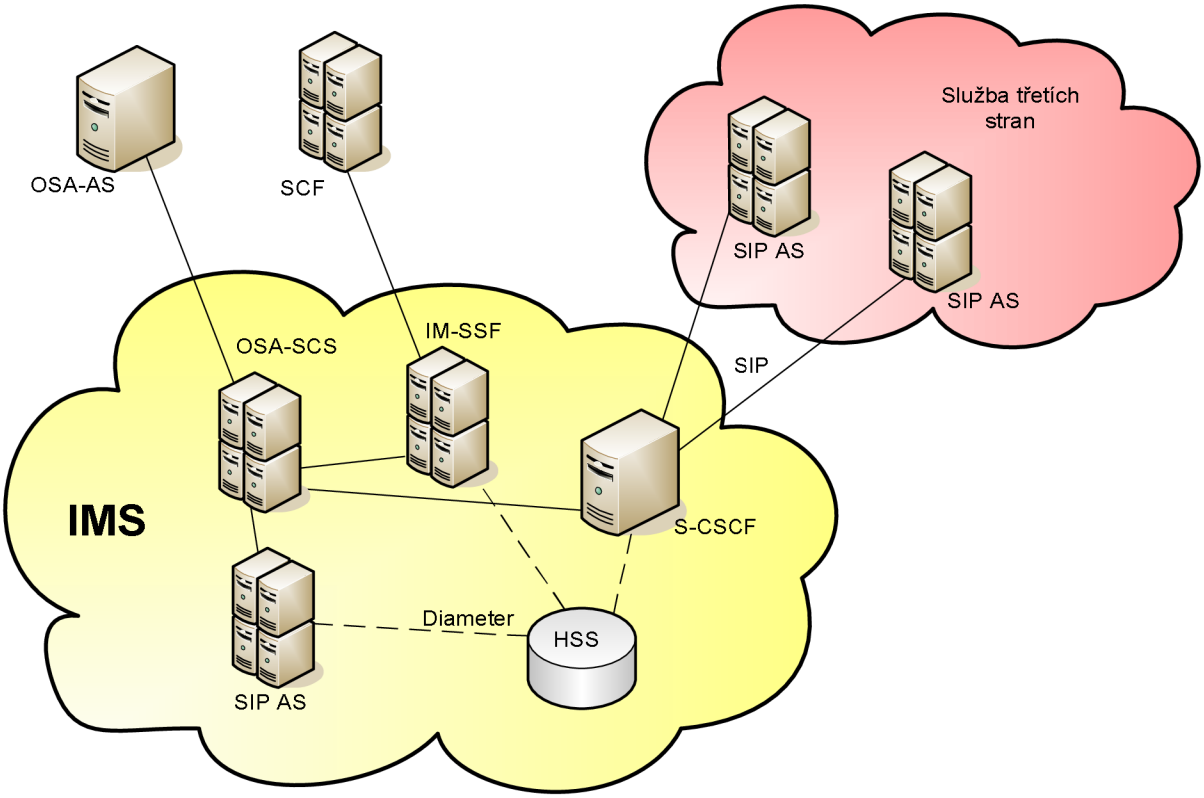
1.2.4 AS (Application Servers)

Tyto servery zajišťují v síti IMS požadované služby koncovým uživatelům. AS komunikují s prvky S-CSCF pomocí protokolu SIP a s prvky HSS komunikují protokolem Diameter. Tyto AS se mohou nacházet jak v domovské síti tak i mimo ni. V druhém případě platí již zmíněné bezpečnostní pravidlo, že AS v cizí síti nebude přímo komunikovat s domovským HSS. Topologie aplikačních serverů je zobrazena na Obr. 1.3. V IMS se nachází tři základní typy AS:

- **SIP AS** (Session Initiation Protocol Application Server) – tento server poskytuje multimediální služby koncovým uživatelům sítě IMS. Jedná se zejména o služby, které implementují protokol SIP. Ty jsou např.: multimediální konference, VoIP (Voice over Internet Protocol) atd.

- **OSA-SCS** (Open Service Access - Service Capability Server) – jedná se o server, který je schopný pomocí standardizovaného rozhraní OSA API zprostředkovávat komunikaci mezi domovskou sítí IMS a OSA aplikačním serverem, který je umístěn vně domovské sítě.

- **IM-SSF** (IP Multimedia Service Switching Function) – jak již název napovídá, jedná se o server, který přepíná funkce IMS do starší podoby komunikace GSM. Tento server tedy podporuje službu CAMEL (Customized Applications for Mobile network Enhanced Logic). Díky tomu lze propojit IMS síť se sítí GSM a tak např. směrovat příchozí hovory jak do sítě ISM tak do sítě GSM podle toho, co si uživatel zvolí. Dále je možné, že síť na základě výskytu terminálu sama zjistí, kterou službu může uživatel využívat, a podle toho rozhodne, jestli bude komunikovat s IMS terminálem nebo GSM terminálem. Řídící logika inteligentní GSM sítě se nazývá GSM (SCF – Service Switching Function). [1, 3]



Obr. 1.3 Topologie aplikačních serverů [1]

1.2.5 MRF (Media Resource Function)

Tato entita poskytuje služby v domovské síti a zahrnuje funkce pro správu a zpracování multimediálních dat. Prvek MRF je použit jen v případě, že to spojení vyžaduje. Pokud tedy aplikace žádá sloučení multimediálních dat z více toků, tak MRF tato data může sloučit a

případně překódovat. Všechny tyto konverze čili překódování videa, hlasu, textu řeší MRF v reálném čase. MRF se dále dělí na:

- **MRFC** (Multimedia Resource Function Controller) – tento prvek vystupuje vzhledem k S-CSCF jako SIP UA (SIP User Agent). MRFC řídí multimediální tok dat a poskytuje služby konference jiným multimediálním aplikacím.

- **MRFP** (Multimedia Resource Function Procesor) – tato entita poskytuje funkce pro práci s multimediálním obsahem. Tyto funkce jsou: mixování multimediálních dat z více datových toků, přehrávaní, překódování a přizpůsobení obsahu multimediálního toku. [1, 3]

1.2.6 BGCF (Breakout Gateway Control Functions)

Brána BGCF slouží jako směrovač. Jedná se v podstatě o SIP server, který podle telefonního čísla směruje data od IMS domény k uživateli připojenému do klasické telefonní sítě. Tato brána se tedy používá pouze v případě, že vzniklý hovor inicializuje strana uvnitř IMS sítě. Brána pak podle svojí směrovací tabulky najde vhodnou síť PSTN, kam hovor přepojí. [1, 3]

1.2.7 Brána PSTN (Public Switched Telephone Network) / CS (Circuit Switching)

Hlavní funkcí těchto bran je umožnit přístup do IMS sítě uživatelům používající telefonní síť PSTN nebo jinou okruhově spojovanou síť CS. Brány PSTN lze rozdělit na tři části:

- **MGW** (Media Gateway) – tato brána přímo souvisí s multimediálním obsahem datového toku. Poskytuje konverzi dat přenášených prostřednictvím protokolu RTP (Real Time Protocol) do časových slotů PCM a naopak, které používá klasická telefonní služba. Brána MGW také umožňuje překódování obsahu RTP proudu. Tato funkce se musí použít hlavně tam, kde klasická telefonní služba používá jiné kódové schéma než IMS.

- **MGCF** (Media Gateway Controller Function) – tato entita transformuje SIP signalizaci do signalizace vhodné pro síť pracující na bázi spojování okruhů.

- **SGW** (Signaling Gateway) – slouží pro převod signalizace na nižších vrstvách sítě. [1, 3]

1.2.8 PDF (Policy Decision Function)

Prvek PDF je logickou entitou, která může být umístěna přímo v severu P-CSCF nebo může existovat samostatně. Je zodpovědná za implementování služby SBLP (Service Based Local Policy). Entita PDF přímo komunikuje s P-CSCF za účelem zjištění a následného vyjednání parametrů spojení. PDF si tedy udržuje informace o relacích, které jsou navázány se serverem P-CSCF, a to sice: IP adresu, port a požadovanou šířku pásma pro přenos dat. PDF je dále propojený s bránou GGSN (Gateway GPRS Support Node) za účelem sjednání parametrů pro danou relaci. [1, 3]

2 PROTOKOLY POUŽITÉ V IMS

Druhá kapitola pojednává o protokolovém vybavení používaném v IMS. Jelikož IMS obsahuje značné množství protokolů, budou zde popsány jen ty nejpodstatnější pro danou problematiku. Tyto protokoly jsou SIP, Diameter a SDP (Session Description Protocol) protokol. Nejpodrobněji bude probrán první zmiňovaný, tedy protokol SIP, jelikož je hlavním protokolem celého systému IMS. Slouží zde k navázání, modifikaci a ukončení spojení mezi dvěma a více koncovými účastníky.

2.1 SIP (SESSION INITIATION PROTOCOL)

Protokol SIP je aplikační, textově orientovaný signalizační protokol. Používá se pro sestavení, modifikaci a ukončení relace. SIP využívá protokoly transportní vrstvy modelu ISO/OSI, a to jak TCP (Transmission Control Protocol) tak UDP (User Datagram Protocol) protokol. Standardně ale používá síťový port 5060 nebo 5061, který je určen pro zabezpečenou komunikaci. Protokol SIP pracuje jako klient-server, přičemž každé zařízení může být jak klient, tak server. Jsou zde podporovány dva typy zpráv: žádosti (request) a odpovědi (response). [5]

Tyto žádosti jsou formulovány jako určité metody, které popisují danou žádost např.: INVITE, REGISTER, ACK, CANCEL, BYE atd. Naproti tomu SIP odpovědi jsou trojciferná čísla v rozsahu 100 až 699 a jsou rozdělena do šesti tříd po stovkách. První číslice označuje, o jaký typ zprávy se jedná, a zbylé dvě tuto odpověď upřesňují.

SIP protokol není svázán s žádným konkrétním protokolem pro přenos multimediálního obsahu. Proto je uvnitř protokolu SIP zapouzdřen další aplikační protokol, který již tyto informace obsahuje. Typicky pro IMS služby je to protokol SDP pro popis multimediální relace. Dalšími protokoly obsažené v SIP zprávě jsou např.: RTP, RTCP (RTP Control Protocol), RTSP (Real Time Streaming Protocol), které se používají pro samotný přenos, řízení a kontrolu multimediálního proudu. [5]

Výhody tohoto protokolu se dají odvodit z toho, že pracuje na aplikační vrstvě. Díky tomu dokáže lokalizovat účastníka v síti, toto je možné jelikož SIP protokol provádí komunikaci typu bod-bod. Další výhoda je schopnost sledovat dostupnost volané strany a změnu jejího stavu. [5]

2.1.1 Architektura SIP

V architektuře SIP jsou definovány dva hlavní prvky: User Agent a Server.

User Agent (UA) - je koncové zařízení, které se stará o navazování komunikace s ostatními SIP prvky. Existuje velké množství UA, např.: klasický telefon, telefon reprezentovaný programem nebo různé brány do jiných sítí. UA se dále dělí na User Agent Client (UAC) a User Agent Server (UAS). Jak již bylo řečeno, model SIP komunikace pracuje na principu klient-server, tzn. UAC má za úkol inicializovat spojení a UAS na toto vybudované spojení reaguje formou odpovědí. Důležité je, že v SIP architektuře může být každé zařízení UA jak UAC tak UAS. [5]

Server – SIP servery nejsou podmínkou pro komunikaci prostřednictvím SIP protokolu. Nicméně pokud tyto servery jsou využívány, tak mají na starost spojení mezi dvěma a více uživateli. Servery v architektuře SIP se dělí na:

- **Proxy server** – tento server se stará o příjem zpráv z UA případně z jiných proxy serverů. Tyto přijaté žádosti jsou pak dále přeposílány na další proxy server případně na UA.

- **Redirect server** – jeho funkce je vyhledávat koncový UA. Funguje to tak, že přijaté žádosti od UA nebo proxy serveru prověří ve své databázi a výsledek pošle zpět stejnou trasou k UA případně proxy serveru. UA přijme odpověď od redirect serveru a následně může další žádost směrovat buď na již koncové UA nebo na další proxy server.

- **Registar server** – slouží k příjmu žádostí od UA a podle těchto informací si aktualizuje databázi koncových zařízení, která jsou připojena k dané SIP doméně. [5]

2.1.2 Formát SIP zprávy

Struktura SIP zprávy je podobná dalším textově orientovaným protokolům jako jsou HTTP (Hyper Text Transfer Protocol) nebo SMTP (Simple Mail Transfer Protocol). Formát SIP zprávy se tedy skládá ze záhlaví, pole hlaviček a vlastního těla zprávy.

- **Záhlaví** - obsahuje různá data podle toho, zda se jedná o SIP žádost nebo odpověď.

- **Pole hlaviček** - toto pole obsahuje data, která souvisí se samostatnou SIP zprávou. Informuje příjemce o tom, jakého typu jsou data v těle zprávy.

- **Tělo zprávy** – do těla zprávy může být vložena jakákoliv textová informace. V IMS je typickou zprávou zapouzdřenou v těle zprávy SIP protokol SDP. Tento protokol slouží k popisu multimediálního toku dat. [5]

2.1.3 SIP adresa

V rámci protokolu SIP je uživatel jednoznačně identifikován pomocí SIP URI (SIP Uniform Resource Identifier). Tato adresa má podobný formát jako adresa emailová. Skládá se tedy ze dvou částí. Část nacházející se před zavináčem identifikuje uživatele uvnitř domény. Druhá část za zavináčem identifikuje přímo doménu, ve které se uživatel nachází. Adresa URI může mít více tvarů, např.: telefonní číslo, IP adresa, nebo může mít textovou podobu. [5]

2.2 SDP (SESSION DESCRIPTION PROTOCOL)

Tento protokol přenáší informace důležité při navazování multimediální relace. Účelem tohoto protokolu je podat detailní informace o mediálním toku vytvářené multimediální relace. Protokol SDP také slouží k oznamování výskytu multicastového vysílání a podává podrobný popis této relace. Díky tomuto se účastník může připojit do daného multicastového vysílání. SDP může obsahovat informace názvu a účelu relace, času, po který je spojení aktivní, seznam medií v relaci, informace o potřebné šířce pásma a kontaktní informace na komunikující uživatele. Protokol SDP je textově orientovaný. Formát SDP zprávy je složen

z několika řádků v následující formě <TYP>=<HODNOTA>. Typ je zastoupen vždy pouze jedním znakem, zatímco hodnota může obsahovat více zřetězených znaků oddělených mezerou. V IMS se tento protokol používá také k vyjednání QoS. Vysílací strana informuje síť IMS o použitém médiu, přenosové rychlosti atd. IMS síť podle toho a podle profilu uživatele zvolí patřičné QoS. [1, 3, 5]

2.3 DIAMETER

Protokol Diameter je používán pro přístup do sítě a podporuje IP mobilitu. Diameter používá pouze transportní protokol TCP nikoliv protokol UDP. Funkce zabezpečení je dosáhnuta použitím protokolu TLS (Transport Layer Security) nebo IPsec (Internet Protocol security). Diameter je tzv. AAA protokol (Authentication, Authorization and Accounting), tzn.:

- **Autentizace** (Authentication) – jedná se o proces potvrzení pravé identity uživatele, a to např.: zadáním přihlašovacího jména a hesla.

- **Autorizace** (Authorization) – je to proces rozhodnutí, které služby může uživatel používat. Rozhodnutí je prováděno na základě autentizace a dále na službách, které jsou danému uživateli přiděleny.

- **Účtování** (Accounting) – jedná se o sběr účtovacích informací, jako jsou informace o poskytované službě, délce trvání této služby atd. [1]

Diameter je v IMS používán ke komunikaci databáze HSS případně SLF s ostatními komponenty IMS subsystému.

3 QOS (QUALITY OF SERVICES)

Jelikož v dnešní době podstatně roste náročnost uživatelů na poskytované služby, je nutné tyto služby poskytovat s určitou předem zvolenou spolehlivostí a stabilitou. Existuje spousta služeb, které jsou poskytovány paketovou sítí:

- www služby,
- ftp služby,
- VoIP telefonie,
- streaming videa,
- video konference aj. [6]

Tyto služby kladou různé nároky na prostředky sítě. Některé služby jsou velmi citlivé na časové zpoždění nebo na kolísání zpoždění (jitter). Například pokud bude v síti uživatel, který bude kontinuálně stahovat velké soubory třeba z ftp serveru, tak službám citlivým na časové zpoždění s menším datovým tokem bude komunikace téměř znemožněna. Je to způsobeno tím, že existuje pouze jedna společná fronta v uzlových prvcích. Tato fronta je zanesena službou, která má největší datový tok, a služby jako je např.: VoIP budou mít tak velké zpoždění, že komunikace bude neuskutečnitelná. Tento jev je řešen pomocí QoS. Je nutné rozdělit služby s podobnou náročností na vlastnosti sítě do stejných tříd. Následně potom tyto třídy hierarchicky seřadit podle priority. To bude mít za následek, že služby s největší citlivostí na časové zpoždění (služby pracující v reálném čase) budou mít největší prioritu a postupně budou řazeny třídy s nižší prioritou. Výsledná komunikace bude probíhat tak, že služby v nejnižší třídě budou pracovat jen tehdy, pokud nebude vyšší třída žádat o síťové prostředky. Samozřejmě je zařazen vhodný mechanismus, aby naopak služby s vyšší prioritou nezahltily linku natolik, že služby s nejnižší třídy nebudou moci komunikovat vůbec. [6]

Každá služba z výše uvedených služeb je jinak náročná na síťové prostředky. Pojem kvalita služeb obsahuje kombinaci různých parametrů. Ty to parametry jsou:

- **Propustnost** – je definována maximální možnou dlouhodobou zátěží na lince. Může být udávána v počtu přenesených dat nebo paketů za jednotku času.

- **Zpoždění** – je to doba, kterou potřebuje paket k tomu, aby se dostal od vysílače k přijímači. Na zpoždění má vliv mnoho prvku vyskytujících se na přenosové cestě. Typy zpoždění jsou:

  - **Propagační zpoždění** – je způsobené fyzickou vzdáleností mezi zdrojem a cílem zprávy.

  - **Proměnné zpoždění** (jitter) – je způsobeno kolísáním zpoždění. Tento jev může nastat, když je síť v určitou dobu velmi zatížena provozem a data v přepojovacích prvcích jsou uložena ve vyrovnávací paměti, zatímco v jinou dobu síť zatížena není a data nejsou nikde pozdržena.

  - **Přenosové zpoždění** - je doba, kterou potřebuje vysílač k vyslání celé datové jednotky na přenosové medium.

- **Paketizační zpoždění** – toto zpoždění vzniká při sestavování dat do paketu. Může k němu docházet jak ve vysílači, kde se celý paket tvoří, nebo v přepojovacích prvcích, kde jsou data kontrolována, případně jsou některé parametry měněny.

- **Ztráta paketu** - tento jev může nastat ve více případech, a to kdy vyrovnávací paměti síťových prvků jsou zahlceny a zbylé příchozí pakety jsou již zahazovány. Další ztráty můžou vniknout při výpadku linky. Dále může být paket zahozen v případě poškození jeho obsahu. [5, 8]

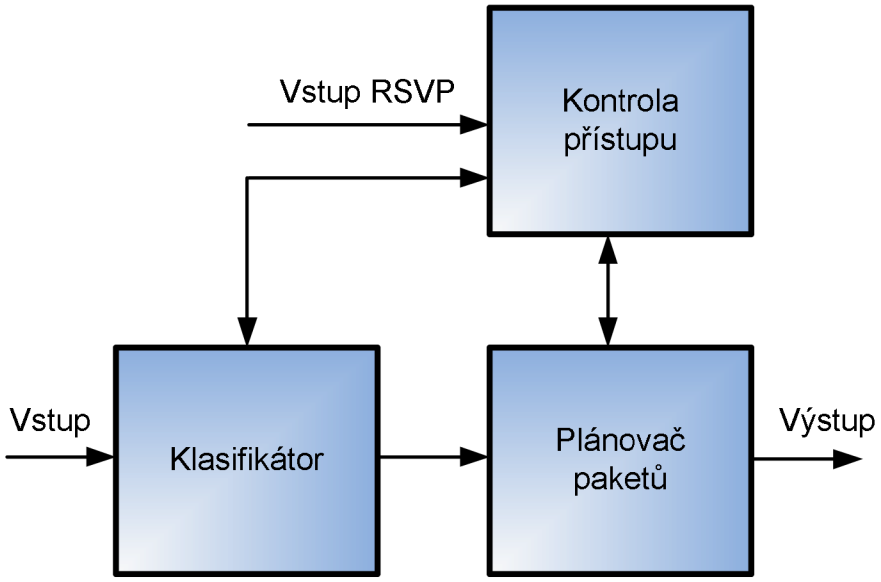
V dnešní době existují spousty páteřních a přístupových technologií a každá z nich používá jinou metodu zajištění QoS. Nyní budou rozebrány vybrané metody zajištění QoS v paketových sítích.

3.1 ZAJIŠTĚNÍ QOS V PÁTEŘNÍ IP SÍTI

Pro zajištění QoS v páteřní IP síti se používají dva základní mechanizmy. Je důležité, aby tyto mechanizmy dodržovaly všechny prvky v přenosovém řetězci QoS. V opačném případě nemůže být QoS garantována. Tyto metody jsou integrované služby (IntServ) a diferencované služby (DiffServ).

3.1.1 Integrované služby (IntServ)

Tento model pro zajištění QoS využívá toho, že parametry přenosové cesty musí být nastaveny ještě před samotným vysíláním dat. Každý prvek v síti musí tuto službu podporovat a obsahovat čtyři hlavní prvky, které společně zajistí požadovanou QoS. Jsou zobrazeny na Obr. 3.1. Těmito prvky jsou:



Obr. 3.1 Model IntServ [5]

- **Plánovač paketů** (packet scheduler) – řídí odesílání paketů podle odpovídající servisní třídy. Pracuje tam, kde jsou pakety řazeny do tříd podle priority.

Plánovač paketů potom řídí mechanizmus odesílání paketů z daných front na linku.

- **Kontrola přístupu** (admission control) – tato kontrola je spuštěna v každém uzlu sítě, který využívá technologii IntServ. Je realizována rozhodovacím algoritmem, který pak využívají směšovače nebo případně hostitelský počítač, aby rozhodl o tom, jestli nová rezervace prostředků neovlivní již stávající rezervovaný provoz.

- **Klasifikátor** (classifier) – klasifikace paketů je proces, kdy jsou pakety řazeny do odpovídajících front dle předem dohodnutých pravidel. S pakety zařazenými ve stejné třídě je zacházeno stejným způsobem.

- **RSVP** (Ressource reSerVation Protocol) – tento protokol je využíván k sestavení a udržení požadované QoS po celé komunikační trase. Je vyslán postupně ke každému směrovači, kde se snaží vyjednat příslušnou kvalitu služeb. [5, 8]

Pokud směrovač přijme RSVP paket, podrobí jej kontrole přístupu. V případě, že bude zjištěno, že priorita služby, kterou RSVP požaduje, neohrozí dříve rezervované prostředky sítě, je tato žádost předána dále. Následně musí žádost projít přes tzv. policy kontrolu. Tato kontrola určí, jestli má daný uživatel oprávnění k užití požadované QoS. Pokud jsou obě kritéria splněna, je nastaven klasifikátor a plánovač paketů, který dále obstará pro danou službu požadovanou QoS. Pokud RSVP žádost nevyhoví oběma kritériím, dojde k jejímu zamítnutí. [4, 5]

Protokol RSVP se tedy používá pro rezervaci síťových prostředků. Jeho funkce je zajistit požadovanou QoS pro jednotlivé datové toky. RSVP se snaží v každém směrovači vyjednat potřebnou kvalitu služeb. K tomuto využívá dvě hlavní zprávy, jsou to:

- **PATH** - tuto zprávu posílá zdroj, který chce vytvořit rezervaci pro danou službu. Tato zpráva v sobě nese informaci o požadované QoS a prochází všemi směrovači od zdroje k cíli. Každý směrovač má pak ve své databázi PATH stav, který obsahuje IP adresu předchozího směrovače. Tuto adresu potom využije zpráva RESV pří zpětné cestě od cíle ke zdroji. Pokud není rezervace možná, vyšle směrovač zprávu PATH ERR.

- **RESV** – tato zpráva je odpověď cílové stanice na zprávu PATH. Zpráva RESV se vrací stejnou cestou, kterou putovala zpráva PATH, a to díky PATH stavu uloženém v každém směrovači, kudy putovala zpráva PATH. Pokud není rezervace možná, pošle směrovač nebo cílový prvek zprávu RESV ERR. Rezervace je úspěšně ustanovena, pokud zpráva RESV dorazí zpátky k odesílateli. Protokol RSVP využívá směrovací tabulky směrovačů, nejedná se ovšem o směrovací protokol. [5,8]

Pro ukončení rezervace je doporučeno použít zprávu Teardown, není to ale nutné. Spojení se totiž samo rozpadne, pokud není rezervace obnovena. Pro ukončení spojení se používají dvě zprávy, a to:

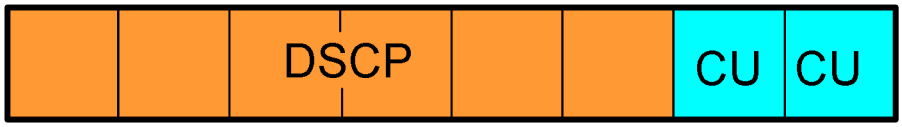
- **PATH TEAR** – tato zpráva provede odstranění PATH stavu ze všech směrovačů na dané přenosové cestě.

- **RESV TEAR** – tato zpráva se používá k odstranění rezervace ze všech směrovačů na dané přenosové cestě. [4, 5]

3.1.2 Diferencované služby (DiffServ)

Tato služba pracuje tak, že jednotlivé datové toky řadí do tříd podle jejich nároků na síť. S každou třídou je potom zacházeno odlišně podle dané priority, zatímco s pakety umístěnými ve stejné třídě je zacházeno stejně. Každý odeslaný paket je označen značkou, která určí, do jaké třídy patří. Jakmile takový paket přijme síťový prvek, určí jeho prioritu právě podle této značky. Na rozdíl od integrovaných služeb si nemusí jednotlivé síťové prvky uchovávat informace o parametrech jednotlivých spojení. Jediné, co si udržuje v paměti, jsou metody zacházení s danými třídami, které reprezentují značky uvnitř IP paketu. [5, 8]

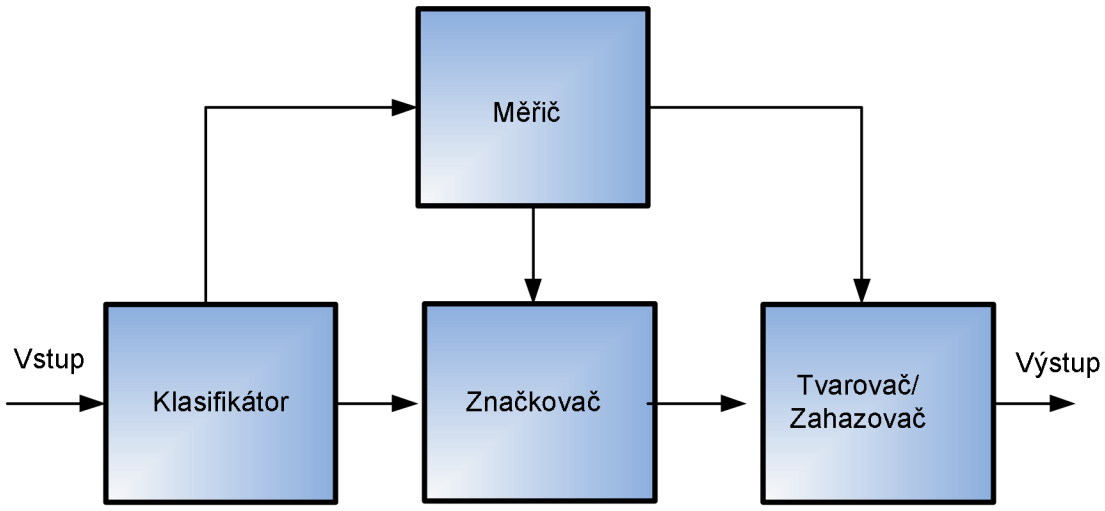
Služba DiffServ využívá pole TOS, které je umístěno v hlavičce IP paketu. Toto pole mělo původně sloužit k zpracování paketu ve směrovači, nebylo však běžně používáno. Díky tomu mohla toto pole využít služba DiffServ. Při použití této služby se používá nové označení, a to DS (podle názvu DiffServ). Toto pole má délku 8 bitů, přičemž je využíváno prvních šest bitů s označením DCSP (DiffServ Code Point), zbylé dva bity nejsou zatím nevyužity a označují se CU (Currently Unusued). Pole DSCP může nabývat hodnot od 0 až po 63, toto je určeno typem aplikace. Strukturu pole DS můžeme vidět na Obr. 3.2. [5, 8]



Obr. 3.2 Struktura pole DS [4]

Podle značky DSCP je s paketem v síti zacházeno. Je definováno chování uzlu PHB (Per Hop Behavior), což je předem definované kritérium síťové politiky uvnitř DiffServ domény. Znamená to, že podle politiky dané domény je zacházeno v uzlech sítě s paketem nezávisle na ostatních síťových prvcích. [5, 8]

Síťová politika DiffServ je založena na tzv. dohodě o úrovni služby SLA (Service Level Agreement). Tato dohoda je ujednána mezi poskytovatelem sítě a jejími uživateli. SLA popisuje, které DS služby poskytuje se zárukou QoS a které naopak nepodporuje s garancí. Dohodu SLA upřesňuje TCA (Traffic Conditioning Agreement). Toto upřesnění udává přesné parametry každé úrovně, jako jsou: propustnost, ztrátovost paketu, zpoždění, DS značení atd.



Obr. 3.3 Model DiffServ [5]

Provoz v DiffServ je řízen čtyřmi hlavními prvky, které jsou zobrazeny na Obr. 3.3. Tyto prvky jsou:

- **Klasifikátor** (classifier) – klasifikátor vybírá postupně pakety a zachází s nimi podle obsahu pole DSCP, toto se označuje jako BA (Behaviour Aggregate), nebo podle kombinace více parametrů jako jsou: cílová a zdrojová IP adresa, DS pole, ID protokolu atd. Tento způsob se nazývá MF (Multi-Field Calssification). BA se provádí, pokud paket přichází již označen od jiného síťového prvku. V opačném případě se používá MF. Při přechodu paketu do jiné DiffServ domény může hraniční směrovač značku ponechat nebo ji změnit.

- **Měřič** (meter) – tento prvek měří dočasné vlastnosti datového proudu vybraného klasifikátorem a porovnává ho s profilem TCA. Zjištěné hodnoty posílá do značkovače a tvarovače.

- **Značkovač** (marker) – značkovač má za úkol nastavovat nové hodnoty DS podle hodnoty zjištěné měřičem. Značkovač může značkovat všechny pakety nebo jen vybrané.

- **Tvarovač** (shaper) – tvarovač podle dopravního profilu TCA zpomaluje či urychluje přijaté pakety. Tvarovač disponuje určitou pamětí, do které přechodně ukládá např. zpožděné pakety. V případě, že paměť je již plná, jsou další pakety zahozeny.

- **Zahazovač** (dropper) – zahazuje pakety, aby byl výsledný tok v souladu se specifikací TCA. [5, 8]

3.2 ZAJIŠTĚNÍ QOS V BEZDRÁTOVÝCH SÍTÍCH

V předchozí kapitole byly popsány metody zajištění kvality služeb především v páteřních sítích. Tato služba musí být ovšem podporována po celé komunikační trase. Pokud by tomu tak nebylo, nebylo by možné zajistit požadovanou QoS v plném rozsahu. Musel se tedy vyřešit problém jak zajistit požadovanou kvalitu služeb u jednotlivých používaných technologií. Výše popsané metody zajištění QoS v páteřních sítích pracují na síťové vrstvě referenčního modelu ISO/OSI. Proto bylo zapotřebí navrhnou mechanizmy, které pracují na nižších vrstvách tohoto modelu a přitom spolupracují s již zavedenými technologiemi. Zde tedy budou popsány způsoby zajištění QoS u technologií Wi-Fi a UMTS.

3.2.1 QoS v technologii Wi-Fi

Sítě WLAN jsou založeny na náhodné metodě vícenásobného přístupu s detekcí nosné neboli CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). U standardů Wi-Fi jsou přístupové metody označovány jako koordinační funkce. Jsou definovány dva typy koordinačních funkcí, a to funkce distribuované a centralizované. V rámci distribuované koordinační funkce DCF (Distributed Coordination Function) mohou stanice mezi sebou soutěžit o přístup k médiu. [4, 9]

Na rozdíl od DCF představuje centralizovaná koordinační funkce PCF (Point Coordiantion Fuction) přístupovou metodu bez soutěžení. Nevýhoda této metody je, že klient před samotným použitím této služby musí být registrován k danému přístupovému bodu. Přístupový bod potom během intervalu bez soutěžení se táže všech registrovaných klientů, jestli mají data k odeslání. Z výše uvedeného plyne, že tato metoda může pracovat pouze ve spolupráci s funkcí DCF. [4, 9]

Důležitou roli v komunikaci prostřednictvím Wi-Fi hrají tzv. čekací doby, které se označují pojmem mezirámcová mezera. Jedná se o dobu, kdy musí vysílač čekat před samotným zahájením pokusu o vysílání. Existují tři základní čekací doby, přičemž jejich délka ovlivňuje pravděpodobnost toho, že stanice získá přístup na médium, a proto čekací doba přímo ovlivňuje prioritu řízení přístupu. Toto prioritní řízení se však používá hlavně pro oddělení řídících a uživatelských dat. Koordinační funkce PCF a DCF tedy využívají ty to typy mezirámcových mezer:

- **SIFS** (Short Interframe Space) – jedná se o nejkratší dobu, a tak zajišťuje největší pravděpodobnost přístupu k médiu. Používá se u rámců s největší prioritou.

- **DIFS** (Distributed Coordination Function Interframe Space) – jedná se o dobu, používanou v DCF. Stanice v tomto režimu musí po uvolnění média čekat minimálně právě tuto dobu, a pak až může začít soutěžení o médium.

- **PIFS** (Point Coordination FunctionInterframe Space) – je středně dlouhý čekací interval, který je využíván v módu PCF. [4, 9]

U technologie Wi-Fi se dále využívá mechanismus s explicitní rezervací přenosového média. Tato metoda se používá pro zvýšení pravděpodobnosti úspěšného přenosu rámce.Toho je docíleno vyhrazením celého média jedné stanici. Stanice, která vyžaduje výhradní přístup, vyšle zprávu RTS (Request to Send), která obsahuje předpokládanou dobu trvání přenosu dat včetně řídících zpráv. Po odvysílání této žádosti, je okolním stanicím

známa doba po kterou se nemají pokoušet o přístup na médium. Jakmile je žádost RTS přijata cílovou stanicí, vyšle tato stanice zprávu CTS (Clear to Send). Tento rámec naopak přijmou všechny uzly v dosahu této stanice a také se po danou dobu nepokusí připojit na médium. Po výměně těchto řídících zpráv následuje zaslání požadované informace a spojení je ukončeno zprávou ACK. Tohoto řešení se zpravidla používá jen ve specifických situacích, např. problém skrytého uzlu nebo při potřebě rezervace média pro přenos dlouhého rámce. [4, 9]

Všechny výše zmiňované metody, ale nerozlišují prioritu provozu, takže nejsou schopny bez potřebného rozšíření plně podporovat QoS. Zmiňovaným rozšířením je standard IEEE 802.11e. Tento standard rozšířil stávající dvě koordinační funkce. Vznikly tedy funkce EDCF (Enhanced DCF), která může pracovat pouze během doby se soutěžením a HCF (Hybrid Coordination Function), která vychází z volitelné funkce PCF a může pracovat jak v době bez soutěžení tak v době se soutěžením, kde však využívá pro svou funkci metodu EDCF. Díky těmto novým koordinačním funkcím byly vyvinuty dvě nové přístupové metody, a to EDCA(Ehanced Distributed Channel Access) a HCCA (HCF Controlled Channel Access). [4, 9]

EDCA představuje nový rozšířený distribuovaný přístup k mediu. Tento mechanismus na základě zvolené kategorie provozu alokuje potřebnou šířku pásma. Existují zde čtyři kategorie provozu, do kterých je mapováno osm prioritních úrovní viz. Tab. 3.1. Tato tabulka nám zobrazuje provázanost prioritních úrovní v pevných sítích s kategoriemi přístupu v bezdrátové síti. Dalším důležitým parametrem je TXOP (Transmission Oportunity), který udává časový interval, ve kterém bude možné přenést rámec. Jednotlivé kategorie přístupu mezi sebou soutěží právě o TXOP. Tento časový interval má přesně danou dobu trvání, kterou příslušné stanice získají z přístupového bodu pomoci vysílaného rámce beacon. Dané kategorie přístupu jsou odvozeny od čekacích intervalů AIFS (Arbitration Interframe Space). Tento interval se prodlužuje se snižující se prioritou provozu a zkracuje s rostoucí prioritou provozu. Tím je dáno, že rámce s vyšší prioritou mají větší pravděpodobnost odvysílání. Dále je možné nastavit pro každou kategorii zvlášť hodnoty parametrů CW_{min} a CW_{max}. Při tomto nastavení velikosti okna platí stejná podmínka jako u nastavení AIFS, čili větší okno pro kategorii s nižší prioritou, aby bylo docíleno menší pravděpodobnosti odvysílání rámce. [4, 9]

Tab. 3.1 Mapování priorit na kategorie přístupu [4]

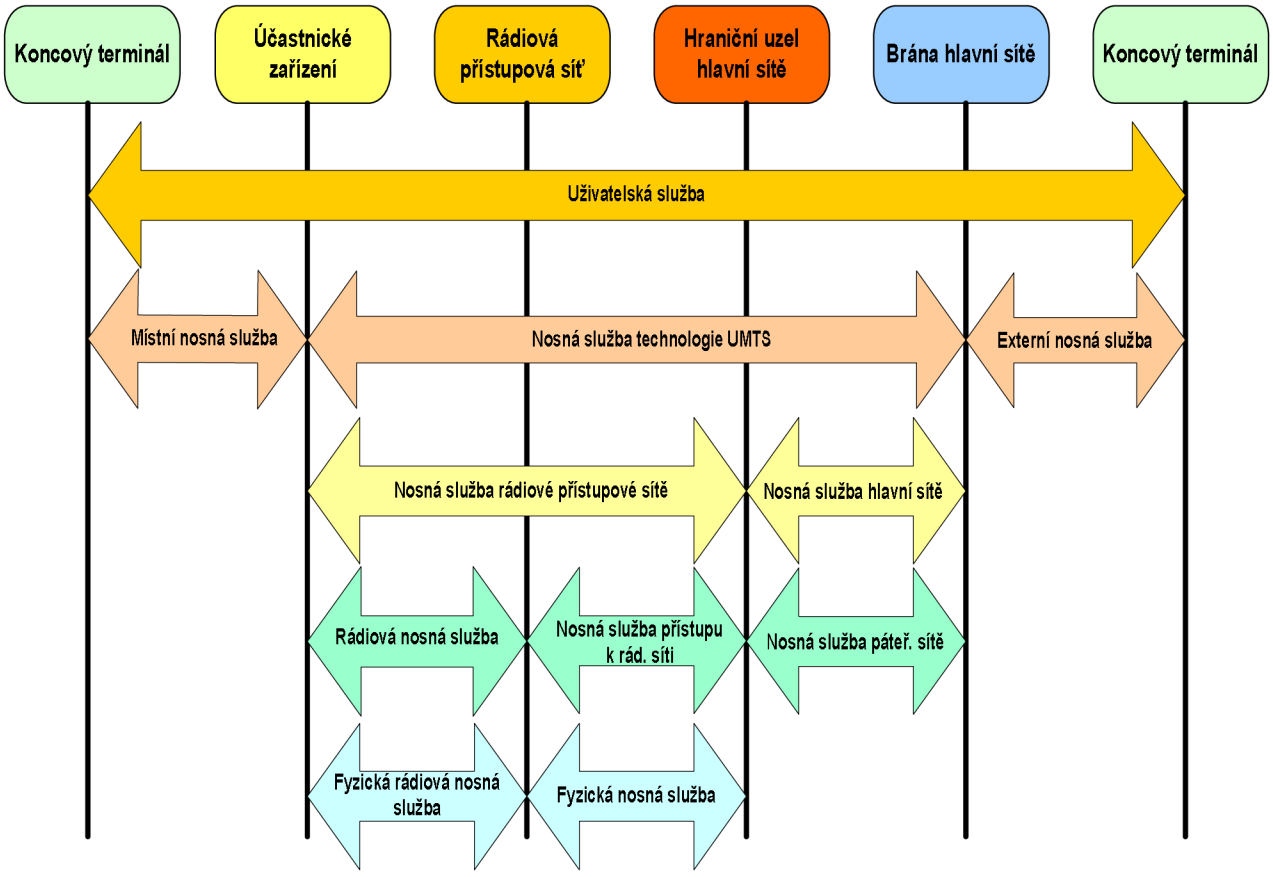
Priorita (0-7)	Kategorie přístupu	Služby
1,2	0	přenos na pozadí
0,3	1	best effort
4,5	2	video
6,7	3	hlas

Naproti předchozímu mechanizmu HCCA vychází z centralizované koordinační funkce PCF, přičemž nabízí propracovanější podporu kvality služeb. QoS je zde uplatněna pomoci různých vysílacích dob, které ve výsledku rozdělí přenosový kanál podle nastavené priority. HCCA na rozdíl od EDCA je schopen zaručit absolutní garanci zpoždění a doby přenosu. Je to způsobeno vyšší prioritou tohoto přístupu a také možností pracovat v době bez soutěžení i se soutěžením o přístupový kanál. Zde již nestačí pouhá registrace stanic, jak tomu bylo u metody PCF. Je zde zapotřebí sdělit přístupovému bodu přesné požadavky na síťové prostředky. Centrální prvek se podle toho rozhodne, jestli je možné tyto požadavky splnit nebo jestli bude muset danou relaci odmítnout. [4, 9]

3.2.2 QoS v technologii UMTS

V dnešní době je většina pevných datových sítí založena na protokolu TCP/IP, pracujícím nad linkovou vrstvou, která je v nejvíce případech zastoupena technologií Ethernet. Proto se v těchto sítích poměrně dobře zajišťuje QoS a další služby, jelikož celá takto propojená síť je standardizována jednou organizací IETF (Internet Engineering Task Force). Naproti tomu, již není tak snadné propojit zmiňovanou pevnou síť s mobilními či méně používanými technologiemi a udržet zde QoS, jelikož na jejich vzniku se podíleli různé organizace. V případě sítě UMTS se jedná o organizaci 3GPP (3rd Generation Partnership Project). Jelikož v dnešních sítích existuje spousta používaných technologií standardizovaných různými organizacemi, je třeba správně mezi sebou provázat jednotlivé technologie používaných standardů. Aby bylo možné zajistit požadované QoS, je nutné, aby celá síť (přístupová i transportní) tuto službu podporovala. Je tedy třeba, aby prioritní mechanizmy použité v jedné technologii byly správně a co nejefektivněji namapovány na prioritní mechanizmy technologie jiné.[4, 11]

Na Obr. 3.4 je znázorněna referenční architektura pro zajištění QoS v mobilní síti UMTS. Je zde znázorněno jak uživatelská služba je postupně dělena na dílčí nosné služby pracující v jednotlivých částech sítě. Externí nosná služba může představovat klasickou IP síť (internet). Je žádoucí správně mapovat prioritní mechanizmy z nosné služby technologie UMTS právě na tuto klasickou IP síť. Dále v rámci nosné služby technologie UMTS existují další nosné služby, kde je také třeba mapovat jednotlivé prioritní mechanizmy mezi sebou a tím zajistit end-to-end QoS, tedy kvalitu služby pro celkovou uživatelskou službu. [4, 11]



Obr. 3.4 Referenční architektura jednotlivých služeb zajišťujících QoS v síti UMTS [4, 11]

Při zajišťování QoS v síti UMTS je nutné dbát na odlišné metody zajištění kvality služeb v každé části této sítě. Je zapotřebí použít translátory, které následně patřičně mapují prioritní třídy jedné služby na prioritní třídy služby sousední. Tímto způsobem a dílčím mapování QoS v každé části sítě se podaří zajistit požadovanou kvalitu služby podél celé komunikační trasy. Jelikož jsou v každé části sítě postupně prioritní třídy měněny na třídy, které jsou podporovány dílčí nosnou službou, je tedy zapotřebí, aby existovaly mechanismy řízení pro dodržení sjednaných parametrů. Těmito mechanizmy jsou klasifikátory, tvarovače a kontrola parametrů provozu. Pomoci těchto mechanizmů jsou jednotlivé provozy seřazeny do odpovídajících prioritních tříd a je prováděno měření, jestli nebyly přesáhnuty sjednané parametry provozu. V případě, že byly, může dojít v rámci tohoto provozu k tvarování případně i zahazování některých paketů, aby byl dodržen předem sjednaný profil. Provoz, který splnil veškeré požadavky je dále patřičným způsobem označen a jsou mu poskytnuty dané síťové zdroje. [4, 11]

Síť UMTS disponuje těmito třídami služeb pracujících na nosné službě UMTS:

- **Konverzační třída** - Tato třída se uplatňuje pro služby v reálném čase s největší náchylností na časové zpoždění a na kolísání zpoždění. Typickými představiteli jsou videokonference a VoIP. Jak bylo řečeno, tato třída má největší prioritu a z toho plyne, že je přednostně odbavena v síťových uzlech.
- **Streamovací třída** - Tato třída je také určena pro služby v reálném čase, ale již méně náchylné na časové zpoždění nebo jitter. Na rozdíl od konverzační třídy jsou zde data přenášena pouze jedním směrem od serveru k uživateli. Typickými představiteli je streamované video nebo hudba. Jelikož je video přenášeno obvykle UDP protokolem, není možná žádná kontrola doručení. Proto musí být kvalita doručení garantovaná streamovací třídou. Zpoždění a jitter je vyrovnáváno až na straně příjemce ve vyrovnávací paměti, přičemž malé ztráty paketů jsou díky vhodnému kódování a lidskému vnímání zanedbatelné.
- **Interaktivní třída** - Tato třída, jak již z názvu vypovídá, je určena k interakci mezi serverem a uživatelem. Typicky se používá pro prohlížení internetový stránek. Tato služba je typická pro TCP protokol. Funguje na principu žádosti a odpovědi. Rychlost této komunikace je závislá na mnoha faktorech ale v našem případě na rychlosti linky a také na požadavcích vyšších tříd. Přenos paketů musí být bezchybný, což zajišťuje protokol TCP.
- **Třída služeb na pozadí** - Tato třída nemá prakticky žádné požadavky na zpoždění. Její provoz je závislý na provozu ostatních tříd. V případě velkého provozu vyšších tříd je tato třída a služby v ní zpomaleny nebo úplně přerušeny. Příkladem těchto služeb je FTP, email aj. Důležitým požadavkem této třídy je chybovost, která musí být co nejnižší. Opět je zde použit protokol TCP a jiné protichybové mechanizmy. [6]

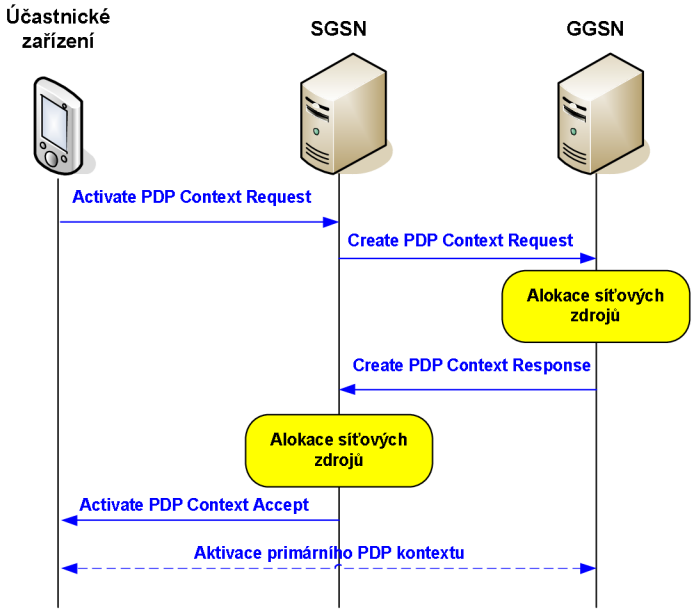
3.2.3 Sestavení spojení a stanovení QoS v mobilní síti pomoci IMS

Při sestavování spojení mezi klienty, kteří chtějí danou službu provozovat, je nutné již při sestavování této relace dohodnout požadovanou kvalitu služby. QoS se potom vztahuje pouze k této relaci a ostatní služby, které daný klient využívá, můžou mít odlišné kvalitativní požadavky.

Jak již bylo popsáno výše, v IMS je nositelem zprávy týkající se multimediálního obsahu relace protokol SDP. Na základě těchto informací již síť dokáže získat informace o požadavcích na síťové zdroje. Příklad informace, kterou obsahuje protokol SDP je:

m=video 51372 RTP/AVP 98 99
a=rtpmap:98 H263-1998/90000
a=rtpmap:99 H261/90000

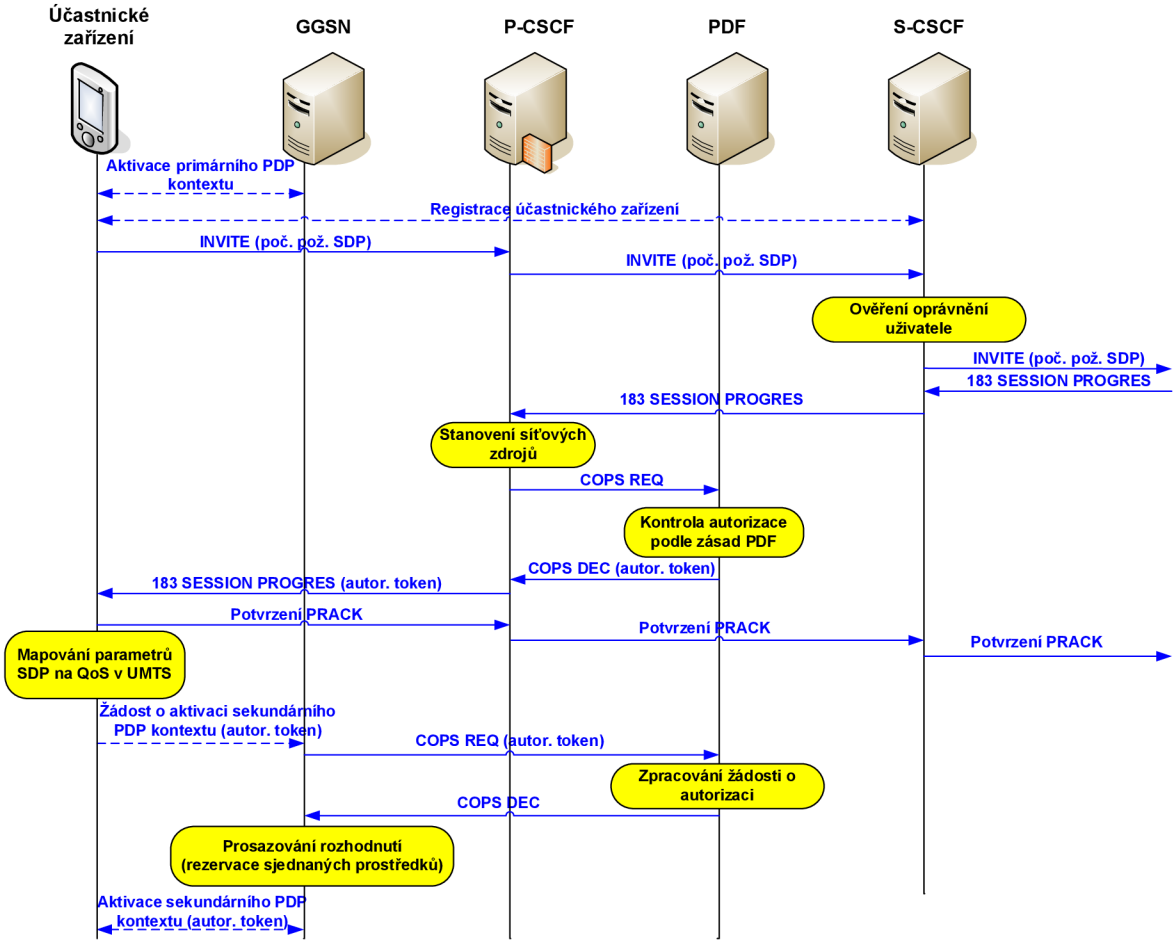
Zpráva tedy obsahuje informaci o tom, že jsou data přenášena protokolem RTP na portu 51372 a obsahují dva video toky, přičemž první používá kodek H.263 a druhý H.261. [4]



Obr. 3.5 Aktivace primárního PDP kontextu [4, 10, 11]

V případě sítě UMTS se navázání spojení provádí ve dvou základních krocích. Tyto kroky jsou sestavení primárního PDP (Packet Data Protocol) kontextu a následně sestavení sekundárního PDP kontextu. PDP je protokol používaný pro přenos dat v rámci mobilní síťové infrastruktury. Tento kontext je vazba mezi koncovým zařízením a prvkem sítě GGSN. Aktivace primárního PDP kontextu se uskutečňuje tak, že koncové zařízení zašle zprávu do SGSN (Serving GPRS Support Node). Tato zpráva obsahuje APN (Access Point Name), které odpovídá adrese požadovaného GGSN uzlu, přes který bude následně sestaveno spojení s externí IP sítí. Tato zpráva také nese informace o zvoleném QoS v rámci sítě UMTS. Jakmile SGSN překontroluje zprávu a ověří zdalipak má daný uživatel přístup na požadované GGSN přepošle zprávu na zvolený hraniční GGSN uzel. GGSN překontroluje, jestli disponuje potřebnými síťovými zdroji a pokud ano zašle odpověď zpět SGSN. Uzel SGSN dále také ověří zdalipak má potřebné síťové zdroje a následně je rezervuje. Dále pak vytvoří rádiovou nosnou službu s nadefinovanými parametry přes rádiovou přístupovou síť. Jakmile obdrží účastnické zařízení zprávu o sestavení kontextu, byl tímto krokem sestaven primární PDP kontext viz. Obr. 3.5.[4, 10, 11]

Dále pak zmiňované GGSN pošle registrační zprávu danému P-CSCF serveru, který vyhledá patřičný S-CSCF pomocí domovského I-CSCF serveru. Jakmile S-CSCF potvrdí registraci účastníka zašle zprávu o potvrzení do P-CSCF a ten potvrdí registraci danému koncovému zařízení. P-CSCF si uloží s kterým S-CSCF serverem uživatel komunikuje a dále všechna komunikace je přímo spojována s tímto serverem. V tomto kroku byla tedy úspěšně dokončena registrace účastnického zařízení k IMS systému viz. Obr. 3.6. [4, 10, 11]



Obr. 3.6 Aktivace sekundárního PDP kontextu [4, 10, 11]

V následujícím kroku účastnické zařízení zašle zprávu *INVITE,* prostřednictvím protokolu SIP do zvoleného S-CSCF. Tato zpráva také obsahuje SDP protokol, který následně udává jaké QoS je požadováno pro danou relaci. Uzel S-CSCF ověří pomocí databáze HSS jestli má účastník právo na dané síťové prostředky, tato komunikace není v obrázku znázorněna. Pokud je vše v pořádku je zpráva *INVITE* poslána dále k protějšímu účastnickému zařízení. Samozřejmě u cílového zařízení probíhá analogická kontrola oprávnění k požadavkům na síťové zdroje u jeho domovských serverů. Jakmile je provedena kontrola oprávnění cílového terminálu a vše proběhne v pořádku, je zaslána zpráva *183 Session Progress*, která obsahuje zprávu SDP nesoucí informace o možnostech tohoto terminálu. Domovský P-CSCF volajícího účastníka si z této zprávy odvodí požadavky na síťové prostředky. Dále pak P-CSCF žádá PDF o potvrzení požadavků na danou kvalitu služby. Pokud jsou splněny všechny podmínky tak PDF vydá autorizační token, který slouží k identifikaci následujícího datového toku. Toto potvrzení je dále zasláno zprávou *Session Progress* volajícímu účastníkovi. [4, 10, 11]

Následně účastnické zařízení zašle žádost o aktivaci sekundárního PDP kontextu. Tato žádost nese i zmiňovaný autorizační token. Po převzetí této zprávy uzlem GGSN pošle tento uzel pomoci PEP (Policy Enforcement Point) zprávu k PDF. Tato zpráva obsahuje zmiňovaný autorizační token, díky němuž dojde v PDF k autorizaci daného datového toku. Tímto dojde k nastavení vyjednané QoS a jejímu přiřazení v GGSN k danému datovému toku. Podobným způsobem dojde k autorizaci relace i na straně volaného účastníka. [4, 10, 11]

4 OPNET MODELER

Program Opnet Modeler je simulační program, který zjednodušuje práci při tvoření paketových sítí. V dnešní době jsou tyto simulační programy velmi ceněny. Jelikož budovat rozsáhlou síť, aniž bychom měli jistotu o funkčnosti této sítě, by bylo velmi neefektivní a nákladné. K tomuto účelu slouží program Opnet Modeler. Pomoci tohoto nástroje lze navrhnout různé paketové sítě a následně simulovat provoz a analyzovat výsledky dané simulace. Tento program je součástí balíčku programů americké firmy Opnet (Optimum Network Performance).

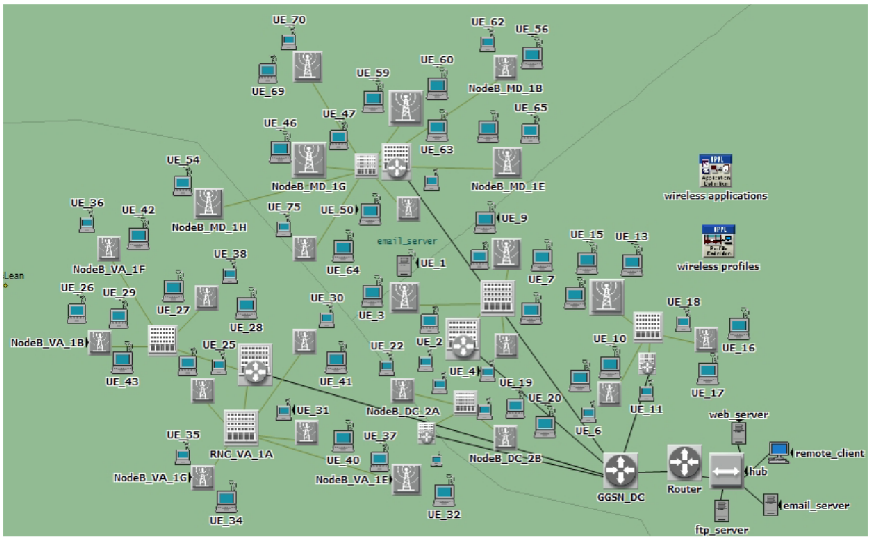
Velkou výhodou tohoto programu je možnost sledovat průběhy datové komunikaci v různých rozmezích doby trvání, což je velmi efektivní, není třeba čekat dlouhou dobu na výsledek simulace. Opnet Modeler je graficky orientovaný nástroj, což urychluje a zefektivňuje práci vývojáře. Při odsimulování určité sítě se dají z množství grafů detailně shlédnout výsledné naměřené hodnoty. Tyto grafy se potom dají exportovat do programu Microsoft Excel, kde se dají dále upravovat. Velké plus Opnetu je v jeho rozsáhlých knihovnách, které mají otevřený kód a dají se dále upravovat. Je zde i velmi dobře provedená nápověda, která obsahuje spousty tutoriálů. [6]

Opnet Modeler obsahuje množství editorů, které umožňují modelovat různé sítě a měnit parametry s různým stupněm abstrakce. Nejčastěji se používají tři základní druhy editorů:

- editor projektů (Project editor),
- editor uzlů (Node editor),
- editor procesů (Process editor). [6]

4.1 PROJECT EDITOR

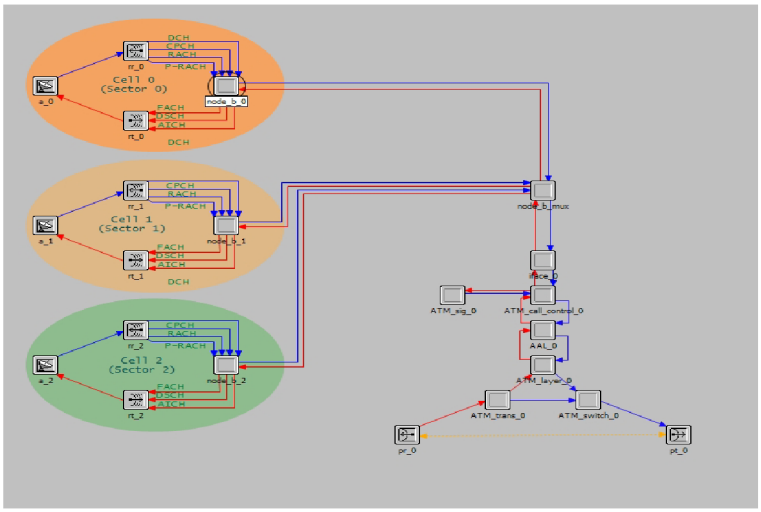
Tento editor slouží k budování topologie sítě s následnou možností analýzy komunikaci v této síti. Síť obsahuje jednotlivé uzly a odkazy na objekty, které se dále dají konfigurovat. Objekty si může návrhář sítě sám vytvořit nebo použít stávající objekty z rozsáhlých knihoven. Projektový editor má v sobě implementovány mapy světa. Díky nim je síť možno namodelovat přímo do dané lokality. Pro vytvoření různých konfigurací stejné sítě slouží tzv. scénáře, které umožňují duplikovat danou síť a dále ji konfigurovat. Schéma Projekt editoru je na Obr. 4.1. [6]



Obr. 4.1 Schéma Projekt editoru [6]

4.2 NODE EDITOR

Nachází se na nižší úrovni než je projekt editor. Tento editor ukazuje vnitřní strukturu daného síťového prvku a jeho vzájemné vztahy mezi funkčními modely a volanými funkcemi.

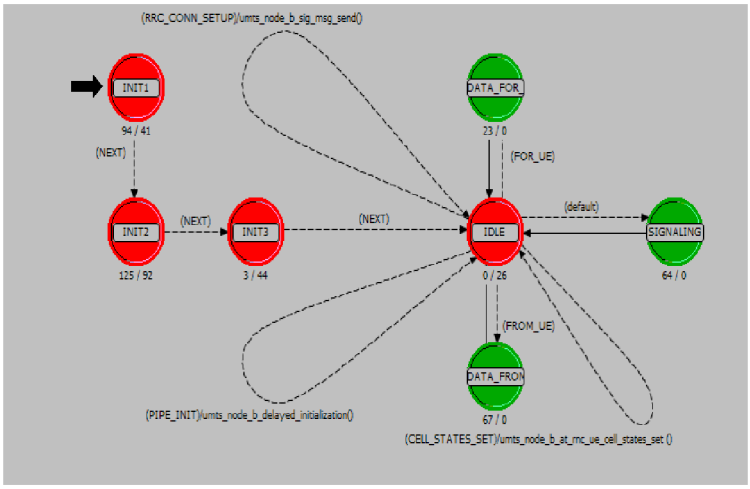


Obr. 4.2 Schéma Node editoru 3 sektorového Node B [6]

V této struktuře jsou vidět modely uzlů, které jsou spolu propojeny datovými cestami. Modely představují různé aplikace, protokolové vrstvy a dále fyzické prostředky jako jsou porty, paměti či sběrnice. Schéma Node editoru je na Obr. 4.2. [6]

4.3 PROCESS EDITOR

V hierarchii editorů stojí na nejnižší úrovni. Proces editor je ukončený stavový automat. Stavy a procesy jsou znázorněny v grafických diagramech. Tyto stavy obsahují kód napsaný v jazyce C/C++, dále je možno jednotlivé stavy měnit tak, že je do nich naprogramován vlastní kód. Schéma Process editoru je na Obr. 4.3. [6]

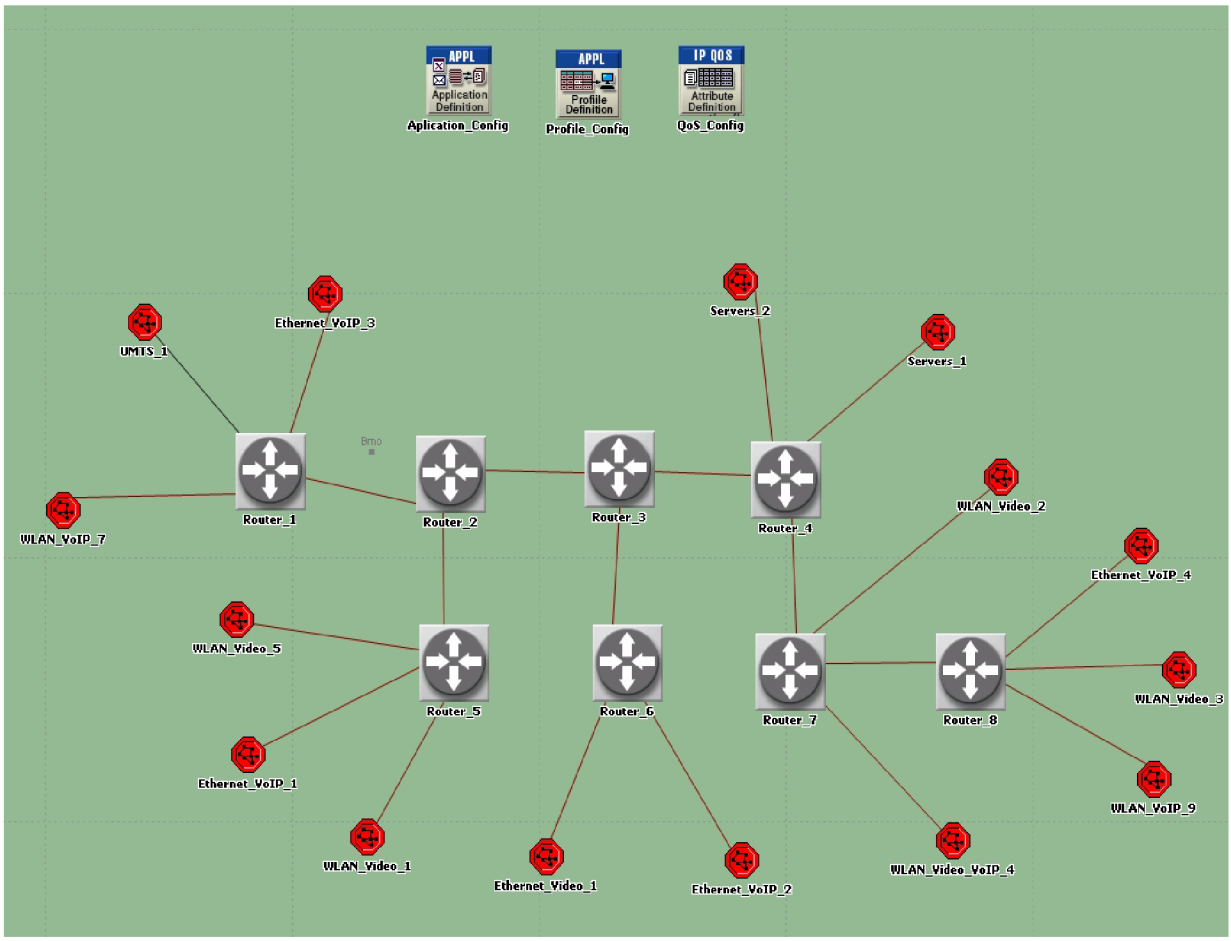


Obr. 4.3 Schéma Process editoru [6]

5 SIMULACE V PROSTŘEDÍ OPNET MODELER

V praktické části byl v simulačním prostředí Opnet Modeler navrhnut model experimentální sítě, která je zobrazena na Obr. 5.1. V této síti byly odsimulovány různé druhy provozu s rozdílnou náročností na kvalitu služeb.

Zobrazený model se skládá z několika směrovačů, které tvoří páteřní linku a propojují jednotlivé subsítě. Typ linky mezi jednotlivými směrovači a koncovými uživateli byl zvolen 10Base_T s maximální přenosovou rychlostí 10Mb/s. Výjimku tvoří dvě linky k subsítím Servers, kde byla použita linka 100Base_T s přenosovou rychlostí až 100Mb/s. Vytvořená síť se skládá ze třech rozdílných přístupových sítí, kterými jsou Ethernet, Wi-Fi a UMTS. Jednotlivé subsítě tedy obsahují výše popsané přístupové sítě a také FTP a HTTP servery.



Obr. 5.1 Model simulované sítě

Každá síť má zcela jiné požadavky na šířku pásma. V prostředí Opnet Modeler je maximální přenosová rychlost přístupové části UMTS sítě 320kb/s. Wi-Fi síť disponuje rychlostí 11Mb/s a Ethernet byl zvolen s rychlostí 100Mb/s. Jako první byl odsimulován scénář bez podpory QoS a bylo pozorováno chování sítě v závislosti na počtu uživatelů a hustotě provozu.

5.1 KONFIGURACE PARAMETRŮ JEDNOTLIVÝCH ČÁSTÍ MODELU PRO SCÉNÁŘ BEZ PODPORY QOS

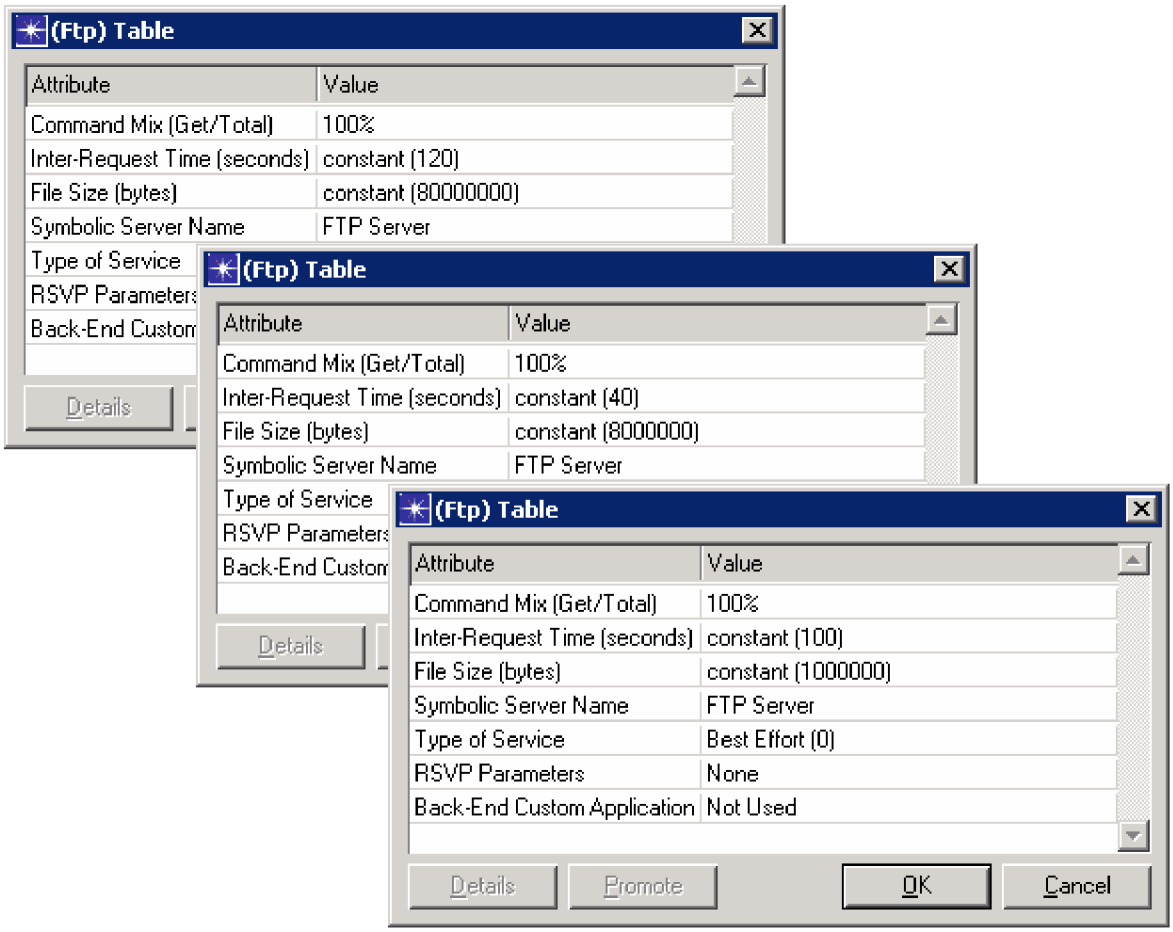
Zde bude přesně popsáno nastavení jednotlivých částí sítě. Jelikož nástroj Opnet Modeler disponuje velmi detailním nastavením každého prvku, budou zde popsány pouze parametry, které bylo nezbytné nastavit pro danou problematiku. Ostatní parametry zůstanou s výchozími hodnotami tak, jak byly předdefinovány. V dalších scénářích budou popsány pouze parametry, které bude třeba změnit pro simulaci dané problematiky. Zbylé nastavení zůstane stejné jako v tomto scénáři bez podpory QoS.

5.1.1 Konfigurace Application config

V tomto bloku jsou nadefinovány veškeré aplikace používané v síti. Pro demonstraci provozu byly vybrány tyto aplikace: FTP, HTTP, VoIP a videokonference. Dále bude popsána konfigurace jednotlivých aplikací.

Konfigurace Application config pro FTP aplikaci

Zde je popsáno nastavení parametrů pro FTP aplikaci. V simulované síti byly zvoleny tři FTP aplikace s rozdílnými parametry, které jsou zobrazeny na Obr. 5.2. Zobrazeny jsou postupně shora FTP_app_1 až FTP_app_3.

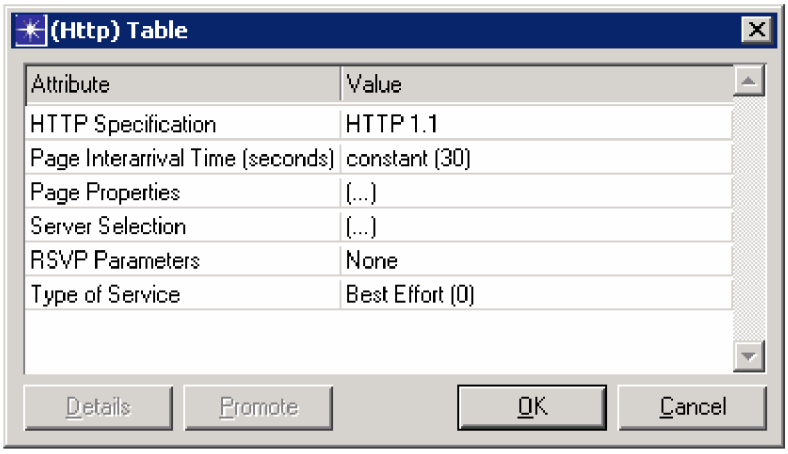


Obr. 5.2 Konfigurace Application config pro FTP

- **Command Mix (Get/Total)** – vyjadřuje procentuální poměr mezi přijatými a odeslanými daty.
- **Inter Request Time (seconds)** – je to čas mezi dvěma žádostmi na FTP server.
- **File Size (bytes)** – jedná se o velikost souboru, který bude přenášen sítí.
- **Type of Service** – jedná s o určení kvality služeb QoS.

Konfigurace Application config pro HTTP aplikaci

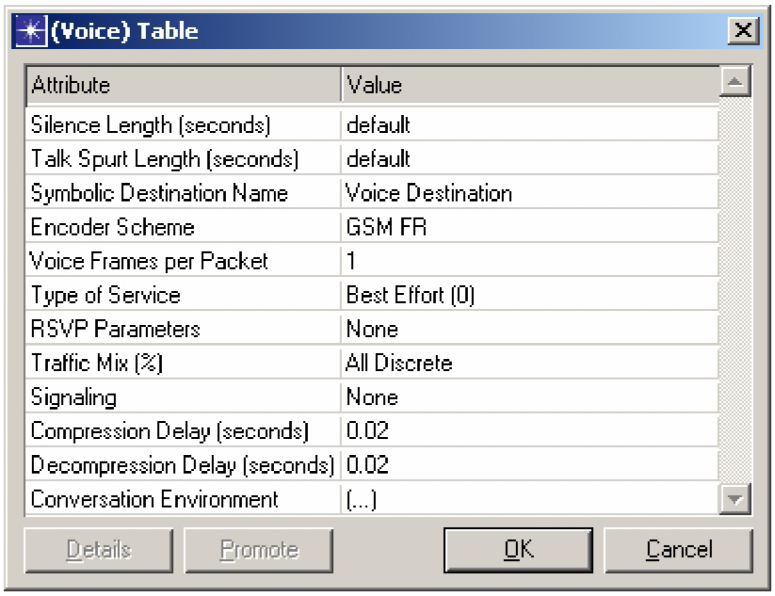
- **HTTP Version –** udává název používané verze protokolu.
- **Page Interarrival Time (seconds)** – je doba mezi dvěma požadavky na http server.
- **Type of Service** – jedná s o určení kvality služeb QoS.



Obr. 5.3 Konfigurace Application config pro HTTP

Konfigurace Application config pro VoIP aplikaci

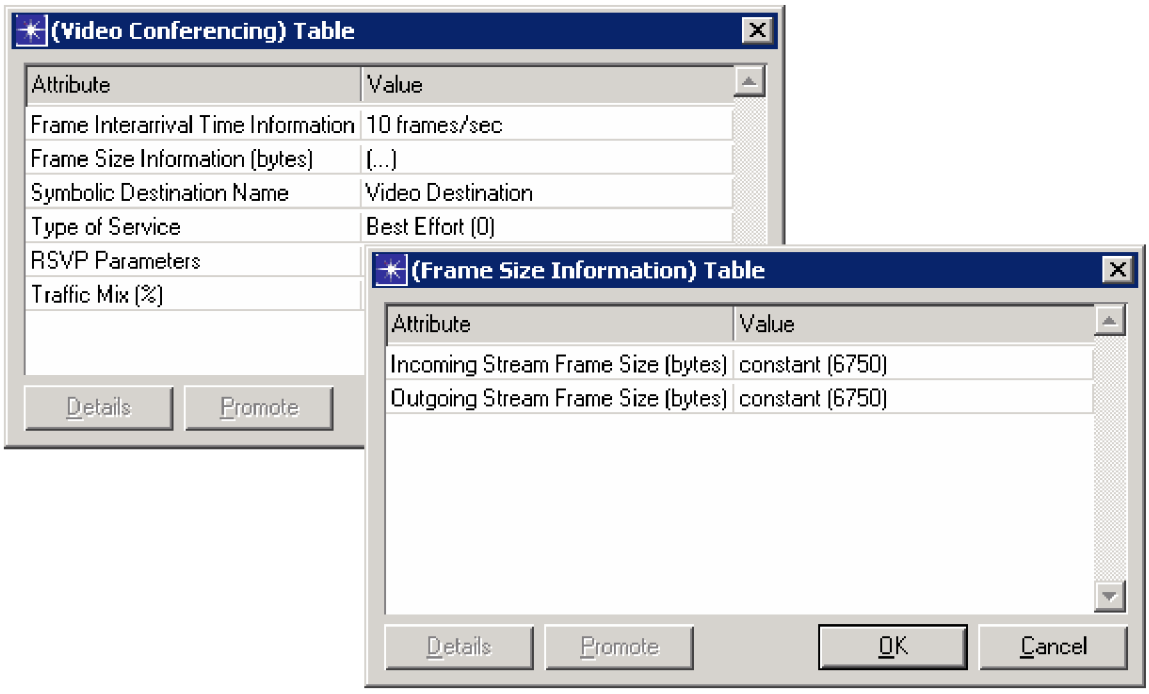
- **Encoder Scheme** – jedná se o kódové schéma použité pro zakódování řeči do digitální podoby. Byl použit GSM FR kodek s přenosovou rychlostí 13,2 kb/s.
- **Type of Service** – jedná s o určení kvality služeb QoS.



Obr. 5.4 Konfigurace Application config proVoIP

Konfigurace Application config pro videokonferenci

- **Frame Interarrival Time Information** – jedná se o nastavení počtu přenesených snímků za sekundu.
- **Frame size Information** – toto nastavení udává rozlišení videa.
- **Type of Service** – jedná se o určení kvality služeb QoS.



Obr. 5.5 Konfigurace Application config pro videokonferenci

5.1.2 Konfigurace Profile config

Tento konfigurační blok slouží pro nastavení profilu definované aplikace. Nastavení samotné aplikace pro simulaci nestačí. Je nutné, aby bylo nadefinováno, kdy má být aplikace spuštěna, jak dlouho bude trvat a po jaké době se bude opakovat. Toto nastavení nám umožní vytvořený profil, který bude následně svázán k dané aplikaci. Následující parametry popisují dané profily.

- **Start Time Offset (seconds)** - zde je nastaven čas spuštění dané aplikace od začátku spuštění profilu.
- **App. Duration** – tato hodnota vypovídá o délce trvání dané aplikace.
- **Start Time** – je to doba, kdy při spuštění simulace má být spuštěn profil.
- **Prof. Duration** – tento čas je zodpovědný za dobu trvání profilu. U všech profilů je tento čas nastaven na „End of Simulation".
- **Inter-repetiton Time (seconds) –** je to čas mezi dvěma aplikacemi.

Konfigurace Profile config pro FTP

Jsou vytvořeny tři FTP aplikace a čtyři FTP profily. Je tomu tak proto, aby byla každá aplikace spuštěna v jiný čas. Tímto způsobem docílíme rovnoměrného nárůstu zátěže linky. Nastavení FTP profilu je znázorněno na Obr. 5.6. Tab. 5.1 znázorňuje, která aplikace je svázána s kterým profilem, a dále pak čas začátku profilu a aplikace.

Tab. 5.1 Nastavení Profile config pro FTP

Profile	Application	Start Time Offset [s]	Start Time [s]	App. Duration [s]
FTP_prf_1	FTP_app_1	5	10	End of Profile
FTP_prf_2	FTP_app_2	240	10	End of Profile
FTP_prf_3	FTP_app_1	400	10	End of Profile
FTP_prf_4	FTP_app_3	40	10	End of Profile

Konfigurace Profile config pro HTTP

Aplikace HTTP je obsažena v simulované síti jenom jedna a má nastaveny tyto parametry viz. Tab. 5.2.

Tab. 5.2 Nastavení Profile config pro HTTP

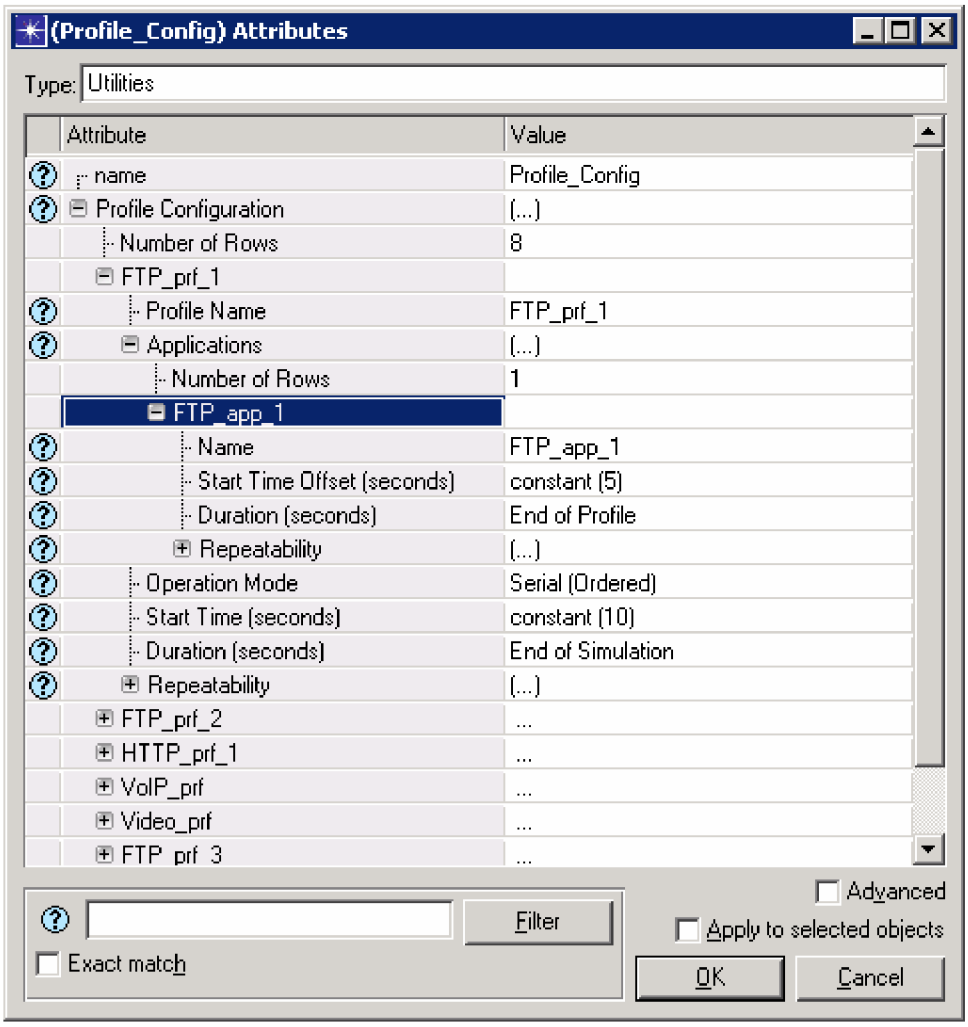
Profile	Application	Start Time Offset [s]	Start Time [s]	App. Duration[s]
HTTP_prf_1	HTTP_app_1	50	10	End of Profile

Konfigurace Profile config pro VoIP

Parametry pro tuto aplikaci jsou znázorněny v Tab. 5.3.

Tab. 5.3 Nastavení Profile config pro VoIP

Application	Start Time Offset [s]	Start Time [s]	Inter-repetition Time [s]	App. Duration [s]
VoIP_app	120	10	120	180



Obr. 5.6 Konfigurace Profile Config pro FTP

Konfigurace Profile config pro videokonferenci

K této aplikaci jsou přiřazeny dva profily z důvodu časového rozestupu mezi spuštěním aplikace. Nastavení jednotlivých parametrů je zobrazeno v Tab. 5.4.

Tab. 5.4 Nastavení Profile config pro videokonferenci

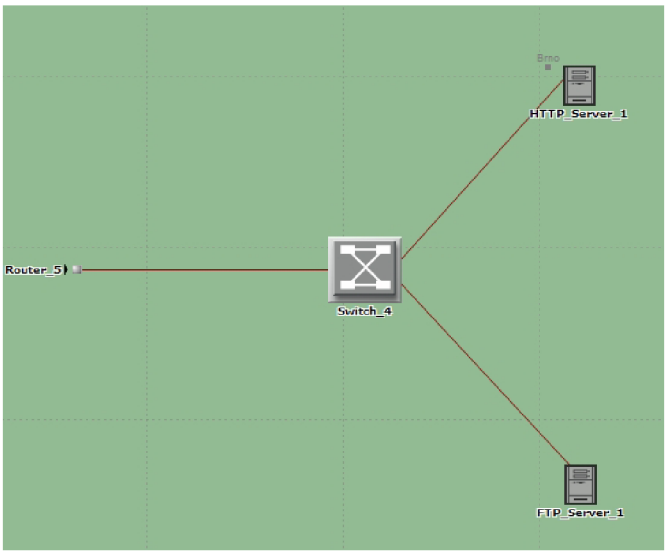
Profile	Application	Start Time Offset [s]	Start Time [s]	Inter-repetition Time [s]	App. Duration [s]
Video_prf	Video_app	180	10	120	260
Video_prf_2	Video_app	300	10	120	260

5.1.3 Konfigurace jednotlivých subsítí

Zde bude popsáno nastavení jednotlivých subsítí a pomocí tabulek bude znázorněn směr komunikace mezi koncovými uživateli.

Konfigurace serverů

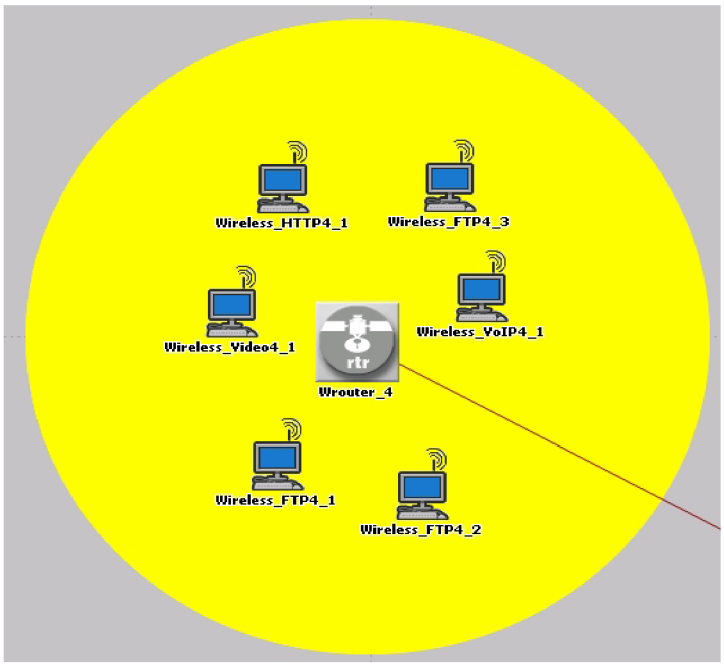
V každé subsíti Servers_1 a 2 jsou dva servery Obr. 5.7. Nastavení HTTP a FTP serverů spočívá v přiřazení dané aplikace k zvolenému serveru. V subsíti Servers_1 se nachází FTP_Server_1 a má přiřazenou aplikaci FTP_app_1 a HTTP_Server_1 s aplikaci HTTP_app_1. V druhé subsíti Servers_2 je FTP_server_2 s aplikací FTP_app_2 a FTP_server_3 s přiřazenou aplikací FTP_app_3.



Obr. 5.7 Subsíť Servers_1

Konfigurace WLAN sítě

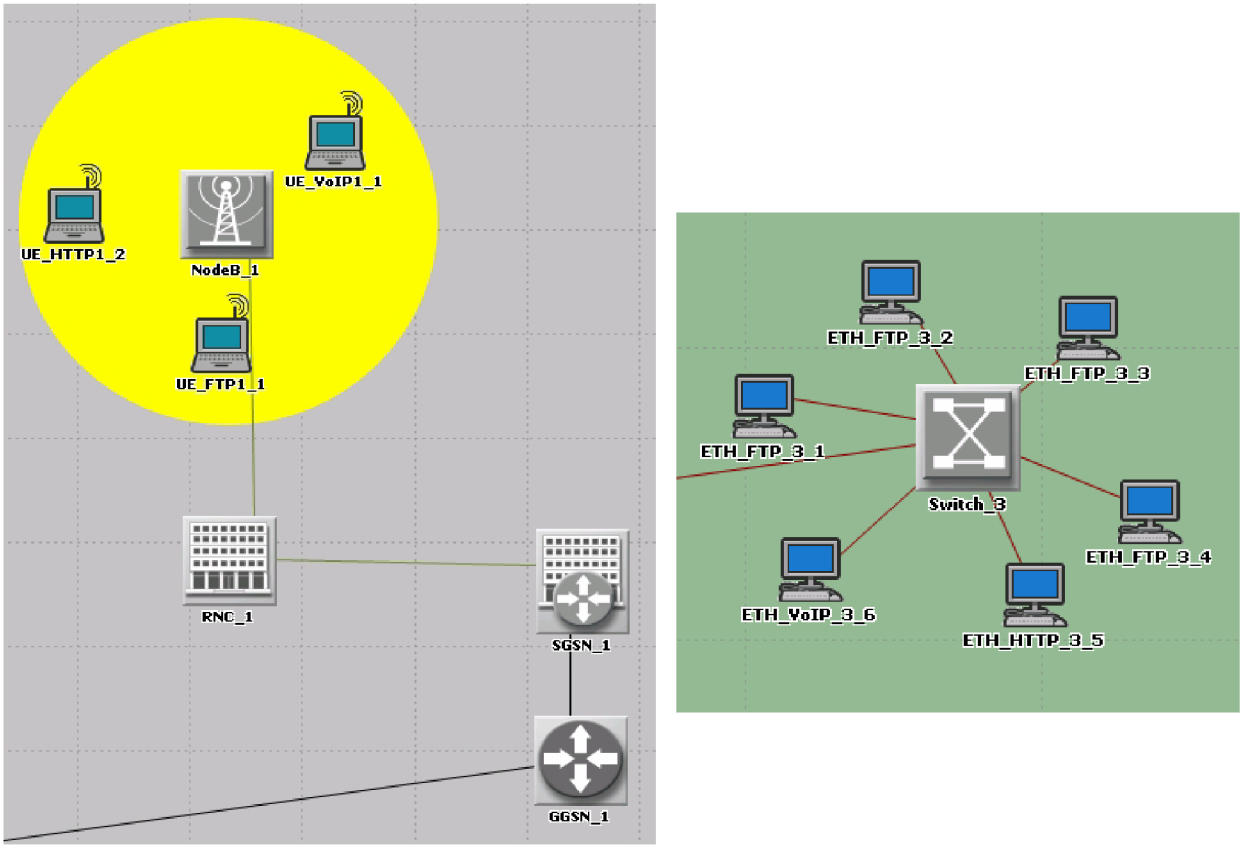
Každá subsíť WLAN obsahuje jeden Wi-Fi směrovač a různý počet stanic. Zde bylo nutné nakonfigurovat stejné SSID (Service Set Identifier) pro koncové stanice a daný směrovač. Topologie sítě WLAN je zobrazena na Obr. 5.8



Obr. 5.8 Subsíť WLAN

Konfigurace UMTS sítě

V síti UMTS je třeba nakonfigurovat RNC (Radio Network Controller). Zde je nutné nastavit parametry pro různé třídy QoS. Jelikož byly nejprve všechny aplikace testovány v nejnižší třídě Background, byly zatím nastaveny pouze parametry v této třídě.



Obr. 5.9 Subsíť UMTS a subsíť Ethernet

Hlavní parametr, který byl potřeba nakonfigurovat, byl čas podržení paketu v bufferu před samotným odesláním. Toto nastavení se muselo provést, jak ve směru uplink, tak ve směru downlink. Hodnota tohoto parametru tedy **Transmission Time Interval** byla nastavena na 10 sekund. Toto nastavení bylo nutné provést kvůli službě VoIP, která při vyšších hodnotách tohoto intervalu přestala fungovat.

U koncové stanice bylo třeba nastavit maximální přenosovou rychlost. U služby VoIP a HTTP bylo tedy nastaveno **Maximum Bit Rate Uplink** a **Downlink** na hodnotu 64kb/s. Služba FTP měla tento parametr nastaven na hodnotu 256kb/s. Topologie sítě UMTS je na Obr. 5.9.

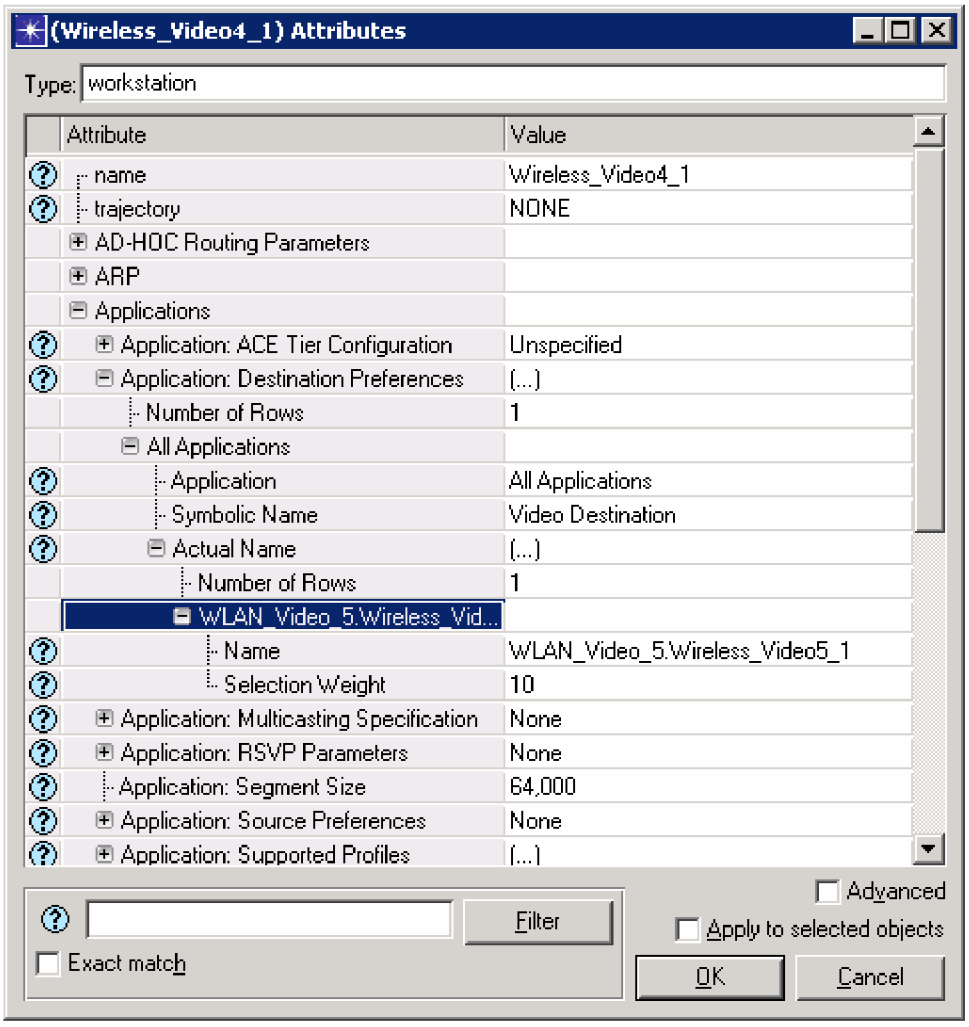
Konfigurace Ethernet sítě

V této síti se vždy nachází přepínač a několik koncových stanic, jak je znázorněno na Obr. 5.9. Každá stanice má nadefinovanou jinou službu, kterou používá. Vždy ale obsahuje alespoň jednu stanici využívající službu pracující v reálném čase.

Konfigurace koncových stanic a komunikace

Konfigurace koncových stanic spočívá v nastavení daných profilů a aplikací. V případě komunikace klient-to-server se na klientovi nastaví profil, pomocí kterého bude používat vybranou aplikaci. Serveru se naopak přiřadí aplikace, kterou bude provozovat a nabízet okolním koncovým zařízením.

Pokud se ovšem jedná o komunikaci peer-to-peer, tedy rovný s rovným jako je tomu v případě VoIP nebo videokonference, je třeba nastavit více parametrů. V případě volajícího účastníka je třeba nastavit daný profil a také cílovou stanici, tzn. volaného účastníka. Tato adresace se provádí podle tzv. klientských adres, které jsou nastaveny u každé koncové stanice. V případě volaného účastníka se nastaví podporovaná aplikace a opět adresa protější strany. Toto nastavení je znázorněno na Obr. 5.10. Položku **Symbolic Name** je třeba nastavit na název využívané služby. Je tomu tak proto, že kdyby koncový uživatel využíval více služeb současně, je třeba definovat, se kterou službou chce daný uživatel komunikovat.



Obr. 5.10 Konfigurace koncového uživatele

Směr komunikace mezi jednotlivými koncovými stanicemi a servery je znázorněn třemi tabulkami. První tabulka znázorňuje komunikace mezi subsítěmi Ethernet, Wi-fi a UMTS a servery HTTP a FTP. V tabulce Tab. 5.5 je tedy vidět, s kterým serverem daná stanice komunikuje. Toto komunikační schéma je platné pro všechny subsítě v navrženém modelu.

Tab. 5.6 zobrazuje komunikaci mezi klienty služby VoIP. První číslice za názvem koresponduje s číslem subsítě. Druhá číslice vyjadřuje číslo koncové stanice v dané subsíti. Názvy jednotlivých subsítí vždy obsahují kromě technologie, kterou používají, i název služby nebo služeb pracujících v reálném čase, které tato subsíť obsahuje společně se službami FTP a HTTP.

Tab. 5.7 znázorňuje komunikace mezi videoterminály. Označení číslic je stejné jako v předchozím bodě.

Tab. 5.5 Komunikace mezi FTP a HTTP klienty a servery

Ethernets/Servers	FTP_Server_1	FTP_Server_2	FTP_Server_3	HTTP_Server_1
ETH_FTP_1	x	-	-	-
ETH_FTP_2	-	x	-	-
ETH_FTP_3	x	-	-	-
ETH_FTP_4	-	-	x	-
ETH_HTTP_5	-	-	-	x
Wireless_FTP_1	x	-	-	-
Wireless_FTP_2	-	x	-	-
Wireless_FTP_3	x	-	-	-
Wireless_HTTP_1	-	-	-	x
EU_FTP_1	-	-	x	-
EU_HTTP_2	-	-	-	x

Tab. 5.6 Komunikace mezi VoIP klienty

Volající/Volaný	Wireless_VoIP4_1	ETH_VoIP4_6	ETH_VoIP3_6	Wireless_VoIP9_1
UMTS_EU1_1	x	-	-	-
ETH_VoIP1_6	-	x		-
ETH_VoIP2_6	-	-	x	-
Wireless_VoIP7_1	-	-	-	x

Tab. 5.7 Komunikace mezi videoterminály

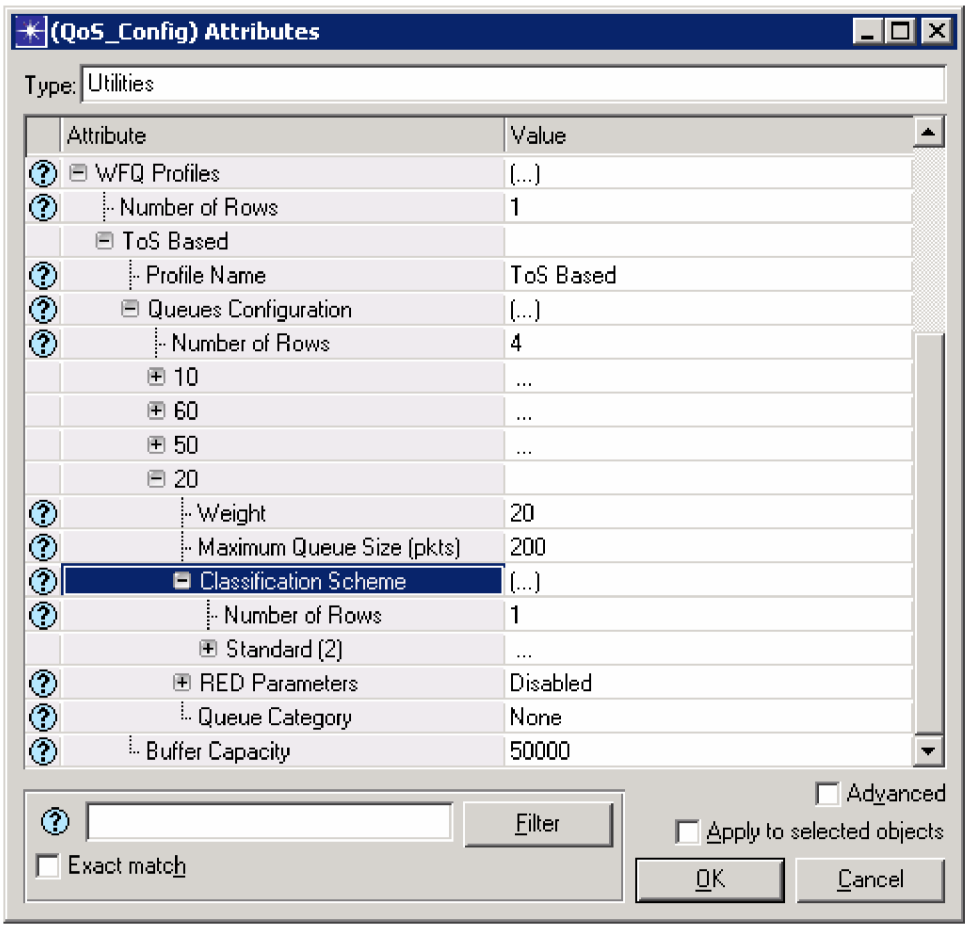
Volající/Volaný	Wireless_Video1_1	Wireless_Video3_1	Wireless_Video4_1
Wireless_Video2_1	x	-	-
ETH_Video1_1	-	x	-
Wireless_Video5_1	-	-	x

5.2 KONFIGURACE PARAMETRŮ SCÉNÁŘE S PODPOROU QOS POUZE V PÁTEŘNÍ SÍTI POMOCÍ SLUŽBY DIFFSERV

V tomto scénáři budou popsány změny v konfiguraci oproti předchozímu scénáři týkající se nastavení DiffServ domény v páteřní síti. To znamená, že pakety budou označeny příslušnými značkami a všechny směrovače v síti s nimi budou zacházet podle předem nakonfigurovaných podmínek. V tomto scénáři tedy nebudou správně namapovány QoS požadavky jednotlivých nosných služeb v přístupových sítích.

5.2.1 Konfigurace QoS Config

V tomto bloku je na výběr mezi několika metodami řízení odesílání paketů. Těmito metodami je možné nastavit různé zacházení s různě prioritizovanými datovými toky. Byla vybrána metoda WFQ (Weighted Fair Queuing), tedy systém front s váženou spravedlivou obsluhou. Tento systém diferencuje datové toky podle váhových koeficientů, které jsou jim přiděleny. Tyto koeficienty odpovídají přiřazené šířce pásma frontám u jednotlivých síťových prvků. To znamená, že služby patřící do fronty s větším váhovým koeficientem mají větší pravděpodobnost odeslání než fronty s menším váhovým koeficientem. Nastavení fronty typu WFQ je znázorněno na Obr. 5.11.



Obr. 5.11 Konfigurace WFQ fronty

Byly zvoleny čtyři fronty, jelikož ve vytvořeném modelu jsou provozovány čtyři služby. Jednotlivá nastavení těchto front je znázorněno v Tab. 5.8.

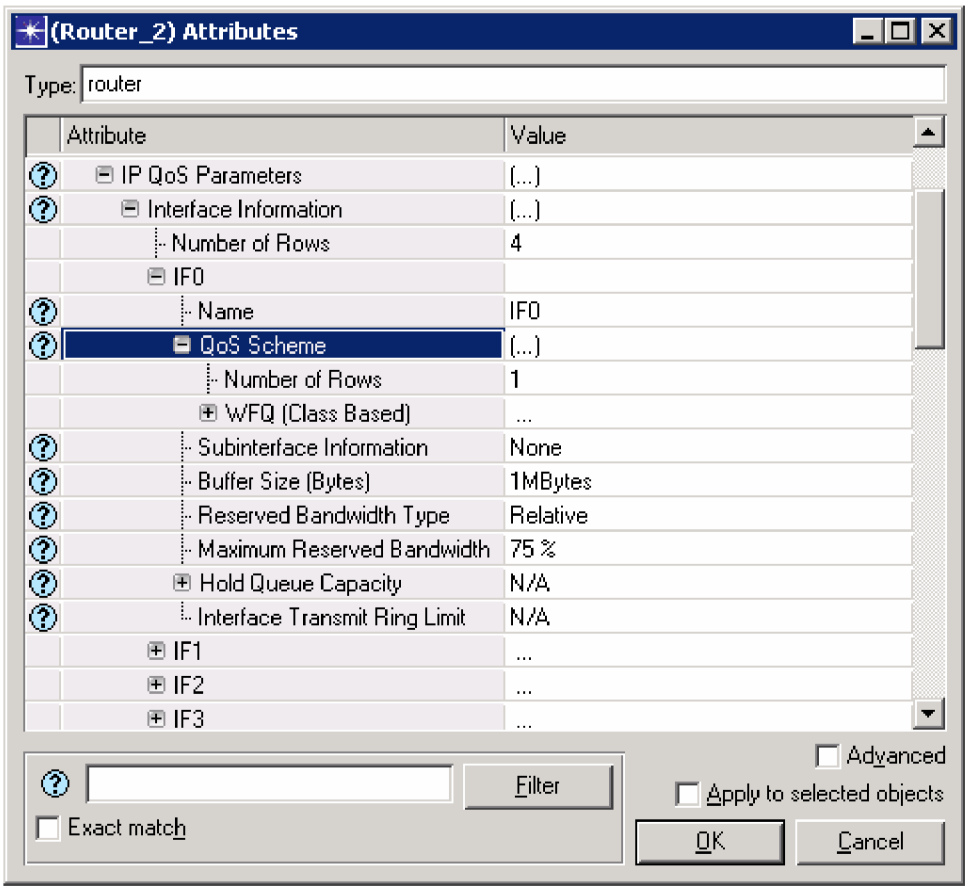
- **Profile Name** - zde se zvolí název vytvořeného profilu.
- **ToS Based** – bylo vybráno dělení do tříd podle pole ToS.
- **Weight** - jedná se o váhu, která vyjadřuje poměr šířky pásma přidělené každé frontě.
- **Maximum Queue Size (pkts)** - jedná se o velikost paměti přiřazené každé frontě.
- **Classification Scheme** - zde je přiřazen jednotlivým frontám typ služby, kterou budou podporovat.

Tab. 5.8 Nastavení jednotlivých front u metody WFQ

Weight	Aplication	Maximum Queue Size (pkts)	Classification Scheme
10	FTP	100	Best Effort
20	HTTP	200	Standard
50	Video	1000	Interactive Voice
60	VoIP	500	Interactive Multimedia

5.2.2 Konfigurace směrovačů a koncových stanic

Aby jednotlivé směrovače byly schopny zacházet podle výše definovaných pravidel s pakety různých tříd, je třeba správně nakonfigurovat jejich rozhraní. Konfigurace směrovače je znázorněna na Obr. 5.12. Toto nastavení je nutné provést pro všechny připojená rozhraní směrovače, které jsou součástí DiffServ domény. Stejné nastavení bude provedeno i u všech koncových stanic. Jelikož ale QoS není podporováno po celé komunikační trase, nebude mít zatím na průběh spojení vliv.

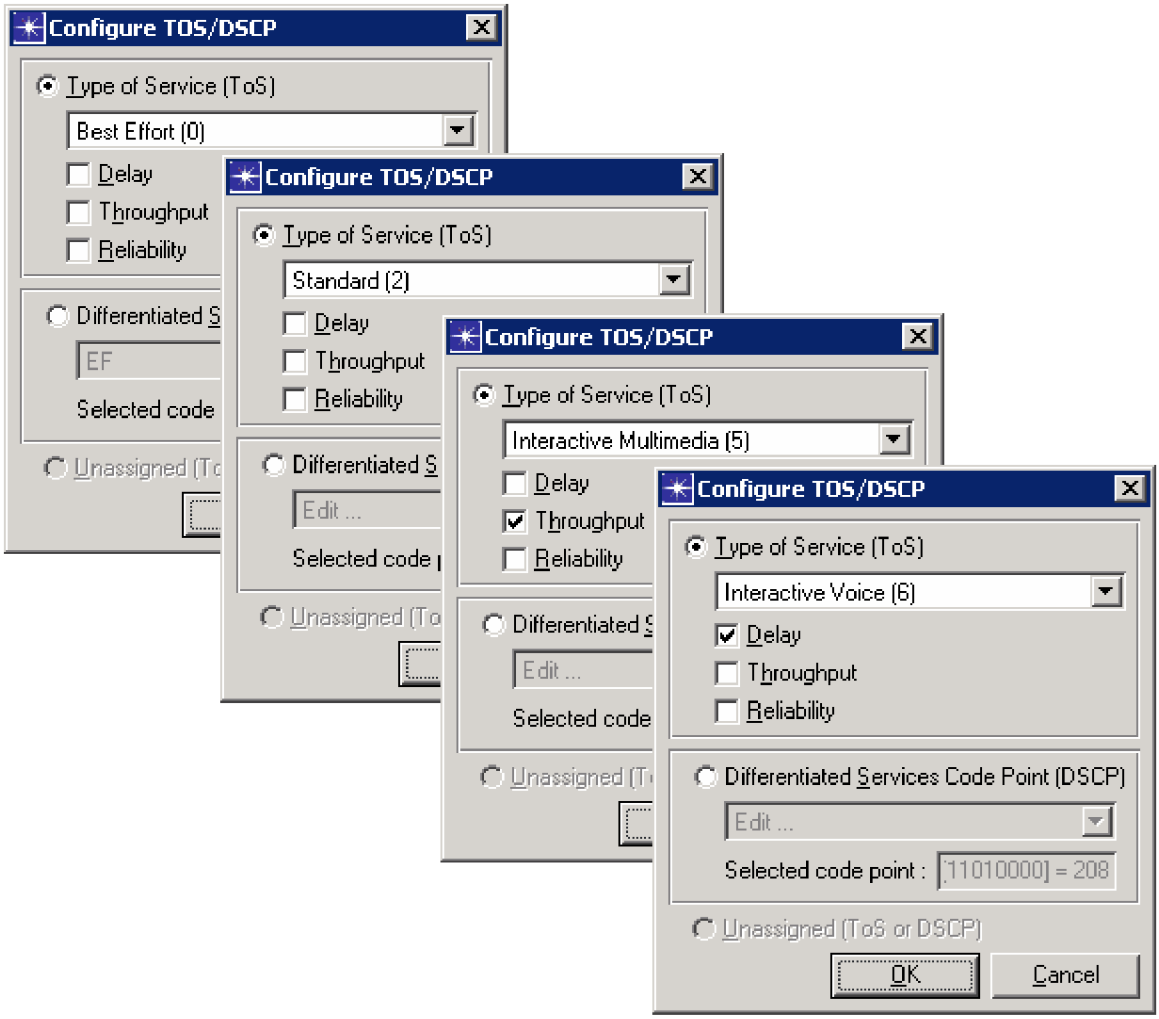


Obr. 5.12 Konfigurace DiffServ na směrovači

- **Type** – v tomto poli jsou obsaženy různé metody zacházení s datovými toky, které jsou provázány s nastavením v QoS Config.
- **Name** – zde je podle zvolené metody **Type** na výběr mezi dříve vytvořenými profily.

5.2.3 Konfigurace Application Config

V tomto scénáři je třeba změnit nastavení Aplication Config tak, aby jednotlivé aplikace byly označeny příslušnou značkou odpovídající jejich náročnosti na síťové prostředky. Toto označení společně s výše popsaným nastavením síťových prvků zajistí požadovanou QoS v páteřní síti. Nastavení jednotlivých tříd je zobrazeno na Obr. 5.13. Pořadí těchto obrázků odpovídá prioritě tříd. Zleva se jedná o třídu přiřazenou FTP, dále pak HTTP, Videokonferenci a službě VoIP.

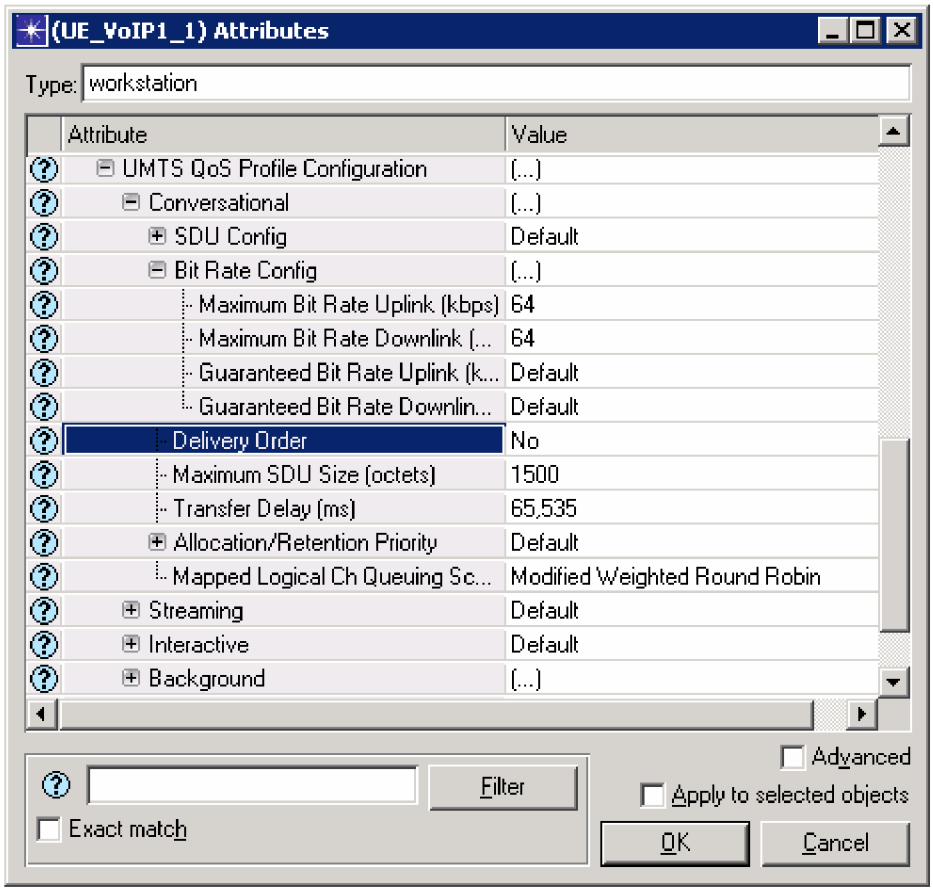


Obr. 5.13 Konfigurace jednotlivých tříd v Aplication Config

5.2.4 Konfigurace subsítě UMTS

Jelikož v tomto scénáři jsou již přiřazeny jednotlivým službám třídy provozu, je nutné nastavit v subsíti UMTS jednotlivé parametry pro každou třídu. Zde vznikl problém, jelikož tento scénář měl podporovat pouze kvalitu služeb v rámci DiffServ domény. Nebylo však možné tento postup dodržet, protože v simulačním nástroji Opnet Modeler se při přiřazení kvalitativních tříd aplikacím automaticky mapují tyto třídy do kvalitativních tříd používaných v UMTS. Proto je nutné nadefinovat u koncových stanic maximální přenosovou rychlost pro danou třídu **Maximum Bit Rate Uplink** a **Downlink.** Toto nastavení je znázorněno na Obr. 5.14. Znamená to, že pro VoIP byla nastavena rychlost 64kb/s, a to v konverzační třídě. Pro službu HTTP byla zvolena také rychlost 64kb/s, ale v interaktivní třídě, a pro službu FTP byla zvolena rychlost 256kb/s v třídě služeb na pozadí. Dále je nutné nastavit V RNC parametr

Transmission Time Interval na 10s v konverzační třídě. Důvod a popis tohoto nastavení byl popsán v kapitole 5.1.3.3.



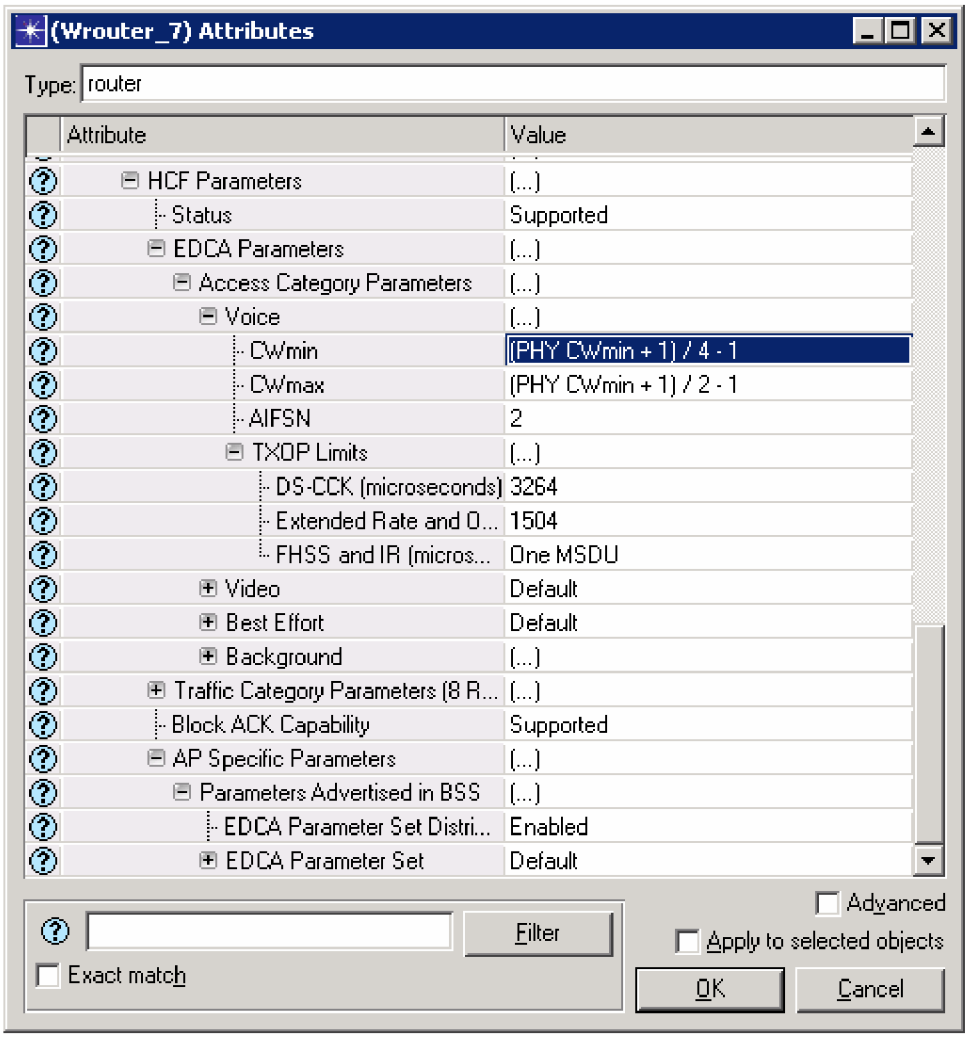
Obr. 5.14 Konfigurace koncové stanice v subsíti UMTS

5.3 KONFIGURACE PARAMETRŮ SCÉNAŘE S PODPOROU QOS PO CELÉ KOMUNIKAČNÍ TRASE POMOCÍ SLUŽBY DIFFSERV

Tento scénář bude obsahovat již kompletní konfiguraci nutnou pro dodržení kvality služeb po celé komunikační trase. To znamená, že zde bude popsána konfigurace jednotlivých přístupových sítí tak, aby bylo docíleno požadované QoS. V předchozí kapitole bylo vysvětleno, proč bylo nutné nakonfigurovat subsíť UMTS, proto zde bude popsána pouze konfigurace Wi-Fi subsítě a nastavení UMTS sítě zůstane nezměněno.

5.3.1 Konfigurace směrovačů a koncových stanic ve Wi-Fi subsíti

V předchozích scénářích nebylo potřeba používat žádné mapování služeb z DiffServ domény na služby, které jsou používány v sítích Wi-Fi. Jak je vidět v tabulce Tab. 3.1, Wi-Fi síť používá k namapování osmi QoS tříd definovaných v DiffServ doméně do čtyř tříd, které používá technologie Wi-Fi. Toto namapování povolíme tím, že na příslušném Wi-fi směrovači zvolíme **HCF Parameters** na **Supported** viz Obr. 5.15. V poli **EDCA Parameters** jsou zmiňované čtyři třídy QoS. Hodnoty obsažené v těchto třídách byly ponechány ve výchozím nastavení, jelikož výsledky vykazovaly hodnoty srovnatelné s teoretickým základem.



Obr. 5.15 Konfigurace Wi-Fi směrovače

- **HCF parameters** – při volbě **Status** na hodnotu **Supported** je podporován distribuovaný přístup k médiu EDCA.
- **EDCA Parameters** – zde jsou nastaveny jednotlivé třídy EDCA.
- **CWmin** – jedná se o minimální délku okna soutěžení.
- **CWmax** – jedná se o maximální délku okna soutěžení.
- **AIFSN** –představuje mezirámcovou mezeru před vysláním dat o určité prioritě.
- **TXOP Limits** – zde jsou nastaveny hodnoty délky trvání vysílacího intervalu pro různé technologie.
- **Parameters Advertised in BSS** – zde musí být u přístupového bodu, tedy Wi-Fi routeru nastaveno **Enable** u parametru **EDCA Parameters Set Distributed.** Tím bylo poveleno odesílání informací o délce TXOP a dalších hodnotách směrem ke koncovým stanicím v rámci beacon.

U koncových stanic je toto nastavení stejné s rozdílem, že poslední jmenovaný parametr je nastaven na hodnotu **Dislabled**, jelikož žádná stanice nepracuje v režimu přístupového bodu, není třeba rozesílat informace o bližším nastavení v rámci beacon.

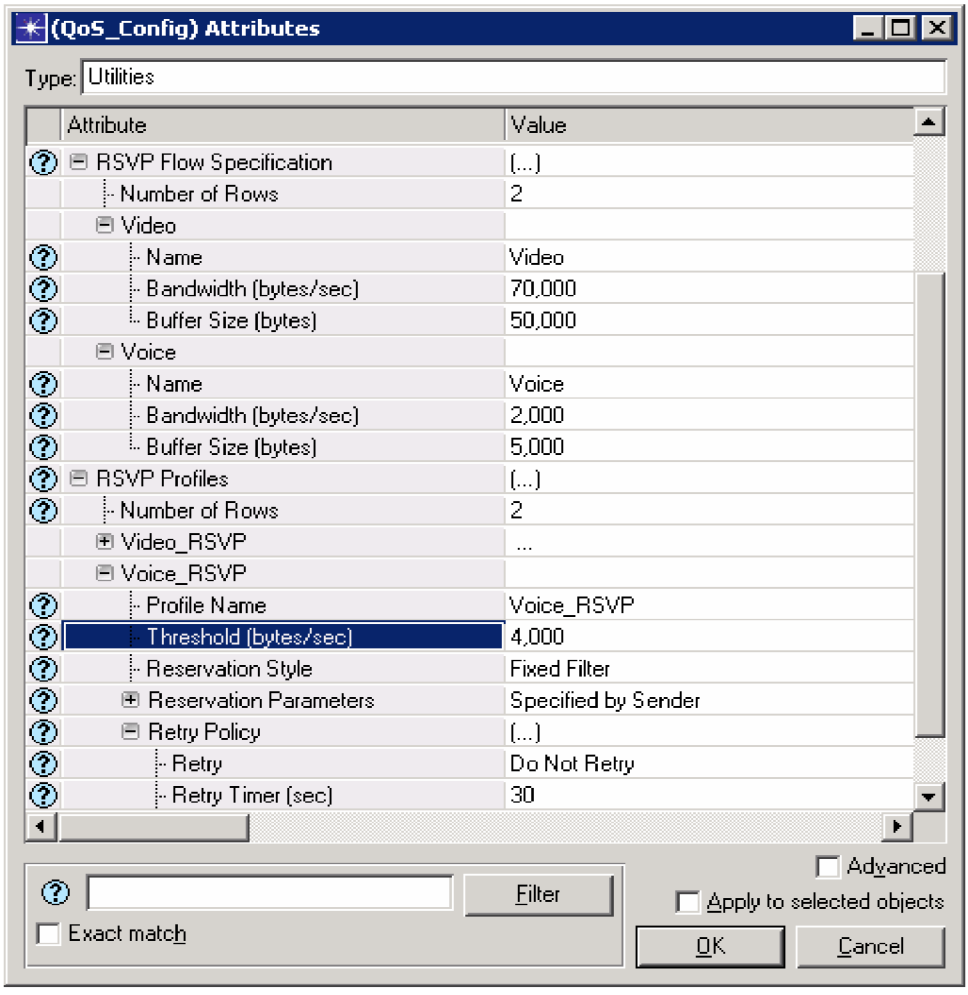
V subsíti Ethernet není třeba nic konfigurovat, jelikož nedisponuje žádnou rozdílnou technologii, kde by bylo třeba definovat mapování kvalitativních požadavků. Vše tedy zůstane stejné jako v předchozím scénáři.

5.4 KONFIGURACE PARAMETRŮ SCÉNAŘE S PODPOROU QOS PO CELÉ KOMUNIKAČNÍ TRASE POMOCI SLUŽBY INTSERV

V tomto scénáři bude popsána konfigurace nutná pro sestavení spojení pomoci RSVP protokolu čili pomocí tzv. IntServ služby. Jak již bylo popsáno v teoretické části, služba IntServ pracuje na principu vyjednání síťových zdrojů před samotným vysíláním uživatelských dat. Je tedy nutné nakonfigurovat RSVP protokol a dále podporu tohoto protokolu ostatními prvky v síti.

5.4.1 Konfigurace QoS Config

V tomto bloku jsou nakonfigurovány parametry pro RSVP protokol. Jedná se zejména o rezervovanou šířku pásma, velikost vyrovnávací paměti, druh rezervace atd. Jsou zde tedy vytvořeny profily, které jsou následně nastaveny u aplikací v **Application Config** a dále přímo u koncových stanic. Zvolené nastavení pro služby VoIP a videokonference jsou znázorněny na Obr. 5.16. Hodnoty byly voleny podle definice aplikací s malou rezervou. U videa je přenosová rychlost 67500B/s a u VoIP je tato rychlost 1650B/s.

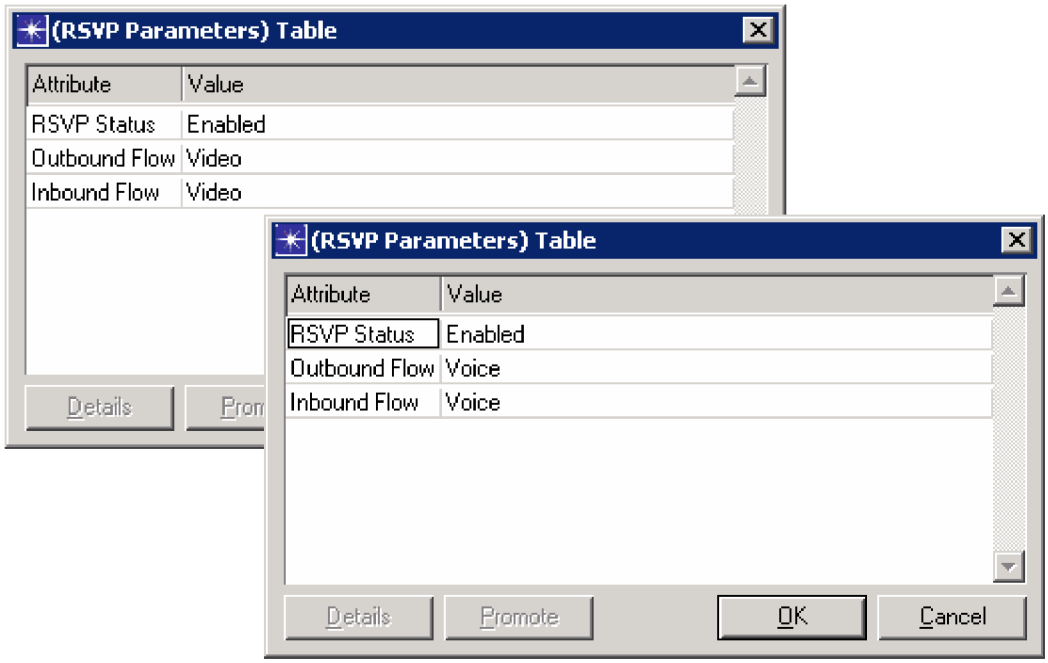


Obr. 5.16 Konfigurace RSVP protokolu

- **Bandwidth (bytes/sec)** – udává zvolenou šířku rezervovaného pásma.
- **Buffer size (bytes)** – jedná se o velikost rezervované vyrovnávací paměti v přepojovacích prvcích.
- **Threshold (bytes/sec)** – jde o rezervační práh, určující minimální hodnotu nutnou pro rezervaci prostředků.
- **Reservation Style** – zde je na výběr mezi více druhy rezervace, byla vybrána rezervace typu **Fixed Filter**, která znamená samostatnou rezervaci prostředků pro odesilatele.
- **Retry Timer (sec)** – udává interval, kdy jsou potvrzovány již rezervované zdroje, aby nedošlo k uzavření komunikačního kanálu.

5.4.2 Konfigurace Application Config

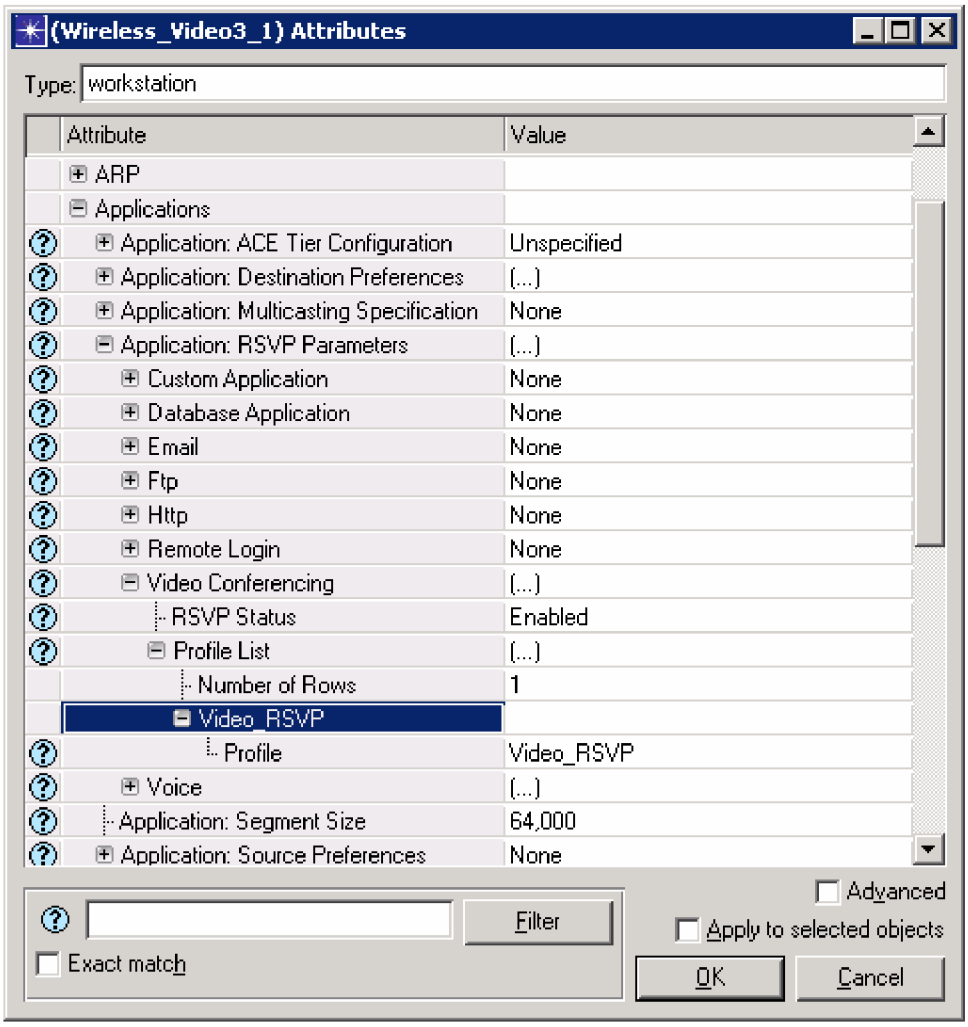
Zde bylo nutné nastavit hodnotu pole **RSVP Parameters.** Znamenalo to provázat vytvořené RSVP profily s aplikacemi, které mají dané rezervace používat. Dále musel být **RSVP status** změněn na **Enabled.** Zmiňovaná konfigurace je zobrazena na Obr. 5.17. Toto nastavení přiřadí dané aplikaci nastavené hodnoty rezervačního protokolu, které se týkají přímo aplikací, jako jsou šířka rezervovaného pásma, vyrovnávací paměti atd.



Obr. 5.17 Provázání vytvořených RSVP profilů s aplikacemi

5.4.3 Konfigurace koncových stanic

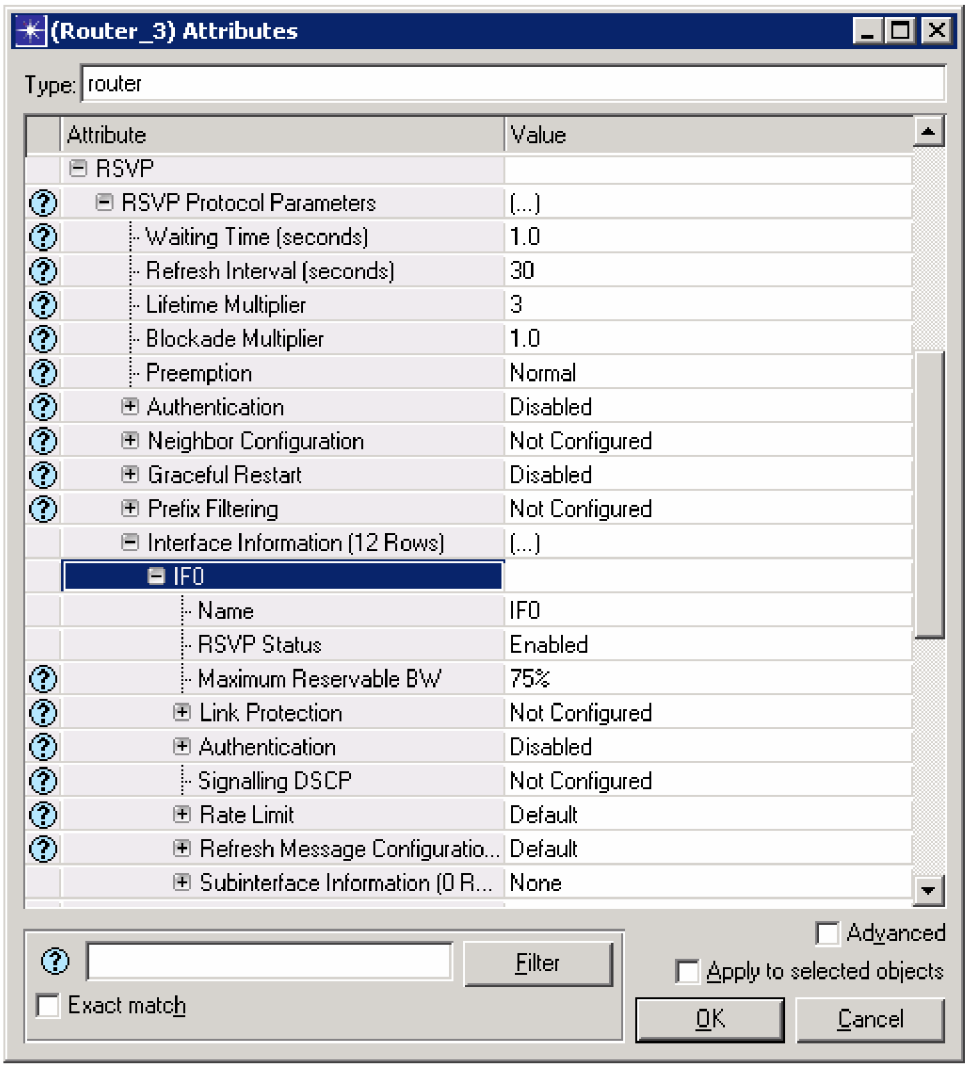
U koncových stanic bylo nutné nastavit **RSVP status** na hodnotu **Enabled.** A dále vybrat profil, který bude použit. V předchozí kapitole bylo popsáno provázání aplikace s profilem RSVP. Zde se nesvazuje profil s konkrétní aplikací, ale nastavuje se, která aplikace bude používat jaký styl a parametry rezervace. Jedná se o nastavení samotného rezervačního protokolu. Toto nastavení je znázorněno na Obr. 5.18.



Obr. 5.18 Konfigurace RSVP u koncových stanic

5.4.4 Povolení RSVP protokolu u směrovačů a koncových stanic

Dále je nutné nakonfigurovat u všech uzlů používajících rezervační protokol podporu RSVP protokolu a nastavit na všech používaných rozhraních RSVP status na hodnotu Enable. Dále byla zvolena maximální šířka pásma, kterou může RSVP protokol rezervovat pro své potřeby. Tato šířka pásma byla zvolena s ohledem na provoz služeb, které nevyžadují rezervaci prostředků. Jsou to služby FTP a HTTP. Hodnota Maximum Reservable BW byla tedy zvolena na 75 procent. Aby protokol RSVP a sním svázaná rezervace prostředků jednotlivých prvků sítě fungovala, je nutné u všech používaných rozhraní nadefinovat frontu typu WFQ. Konfigurace RSVP je stejná na stanicích i na směrovačích a je zobrazena na Obr. 5.19.



Obr. 5.19 Povolení podpory u směrovačů a koncových stanic

5.5 SIMULACE VYTVOŘENÉ SÍTĚ

Nyní se již budeme věnovat samotné simulaci sítě. Jsou vytvořené čtyři scénáře. První s názvem Best Effort znázorňuje chování sítě bez podpory QoS. Všechny aplikace mají tedy k dispozici stejné fronty v přepojovacích prvcích a nedochází zde k žádnému upřednostňování datových toků citlivých na zpoždění, kolísání zpoždění atd. Druhý scénář je označen jako QoS_DiffServ. Zde je QoS nastavena pouze v páteřní síti. Tedy je vytvořená DiffServ doména, ale QoS není správně namapováno do jednotlivých sítí až na UMTS síť, která již QoS má nastaveno z důvodů popsaných v konfigurační části. Další scénář se nazývá QoS_DiffServ_Access_Network. Jedná se o scénář, kde je QoS nastavena po celé komunikační trase a všechny kvalitativní služby jsou zde správně namapovány. Poslední scénář je označen jako QoS_IntServ. Zde je kvalita služeb zprostředkována pomoc rezervačního protokolu RSVP.

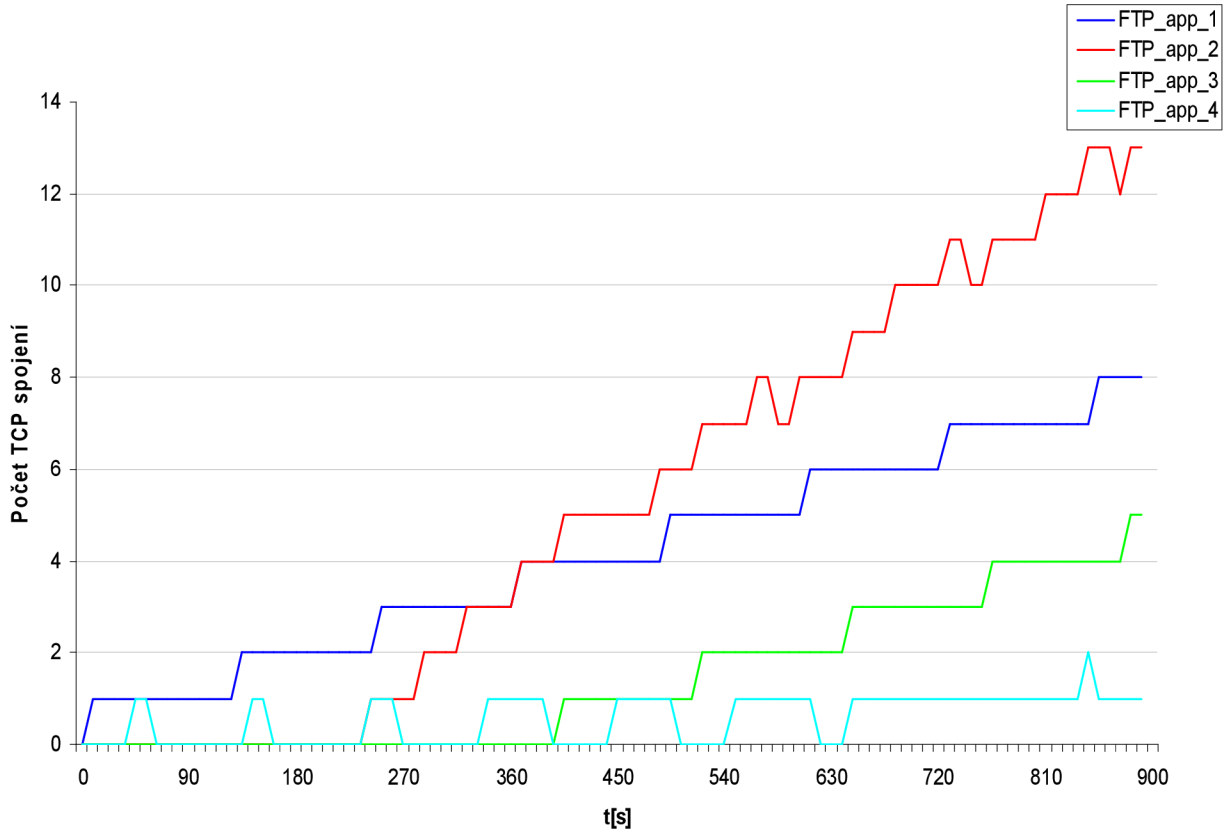
Ve všech těchto scénářích budou sledovány vybrané koncové stanice a provoz na ostatních stanicích bude fungovat jako zátěž linky. Doba simulace byla zvolena 15 minut, a to s ohledem na výpočetní výkon počítače, na kterém byla síť simulována. V namodelované síti pracují čtyři aplikace: FTP, HTTP, VoIP a videokonference. Každá tato aplikace je jinak náročná na šířku přenosového pásma, časové zpoždění a kolísání zpoždění.

5.5.1 Aplikace FTP

Tato služba funguje na aplikační vrstvě modelu TCP/IP. Jako transportní protokol používá protokol TCP. Pro přenos signalizace využívá TCP port číslo 21 a pro vlastní přenos dat používá port číslo 20. Jmenovaná aplikace pracuje na principu klient-to-server, tzn. server poskytuje data a klient s těmito daty pracuje.

Služba FTP není nikterak náročná na šířku pásma, časové zpoždění či kolísání zpoždění. Naproti tomu musí být požadovaná data přenesena bezchybně. K tomu například slouží právě protokol TCP, který před samotným přenosem dat naváže spojení s koncovým uživatelem a tím dokáže reagovat na případné výpadky nebo zatížení sítě. Tyto situace řeší podle toho, co zapříčinilo nepřijetí paketu na straně přijímače. TCP může buď zpomalit vysílání datového toku nebo opakovat vysílání ztraceného segmentu dat. Z toho plyne, že tato služba by pracovala díky své flexibilitě při použití QoS v nejnižší třídě.

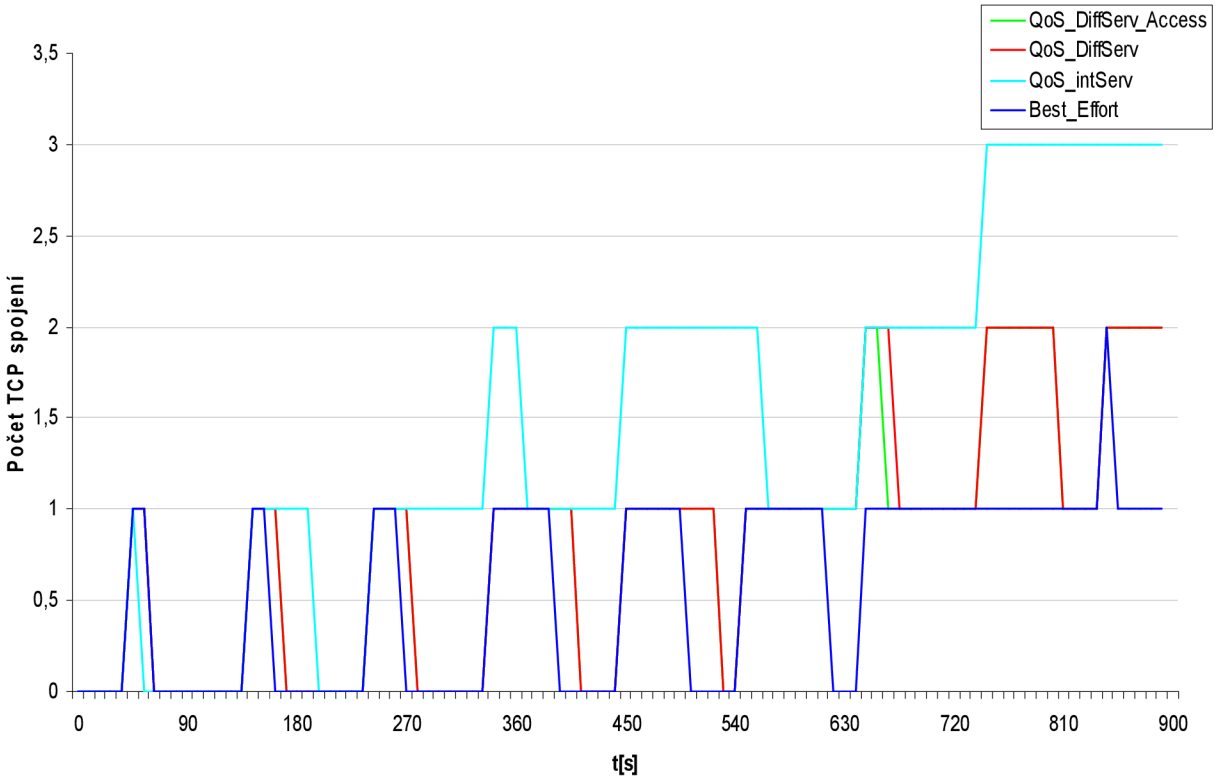
Ve vytvořeném modelu sítě je větší počet FTP klientů. Který klient komunikuje s jakým serverem, je vidět v Tab. 5.5. Jak bylo popsáno výše, jsou použity tři FTP aplikace a čtyři FTP profily. Čas spuštění jednotlivých aplikací je zobrazen v Tab. 5.1. Tento čas byl volen k názornému ukázání vlivu postupného nárůstu zatížení linky na služby náchylné na časové zpoždění.



Obr. 5.20 Počet TCP spojení u aplikace FTP

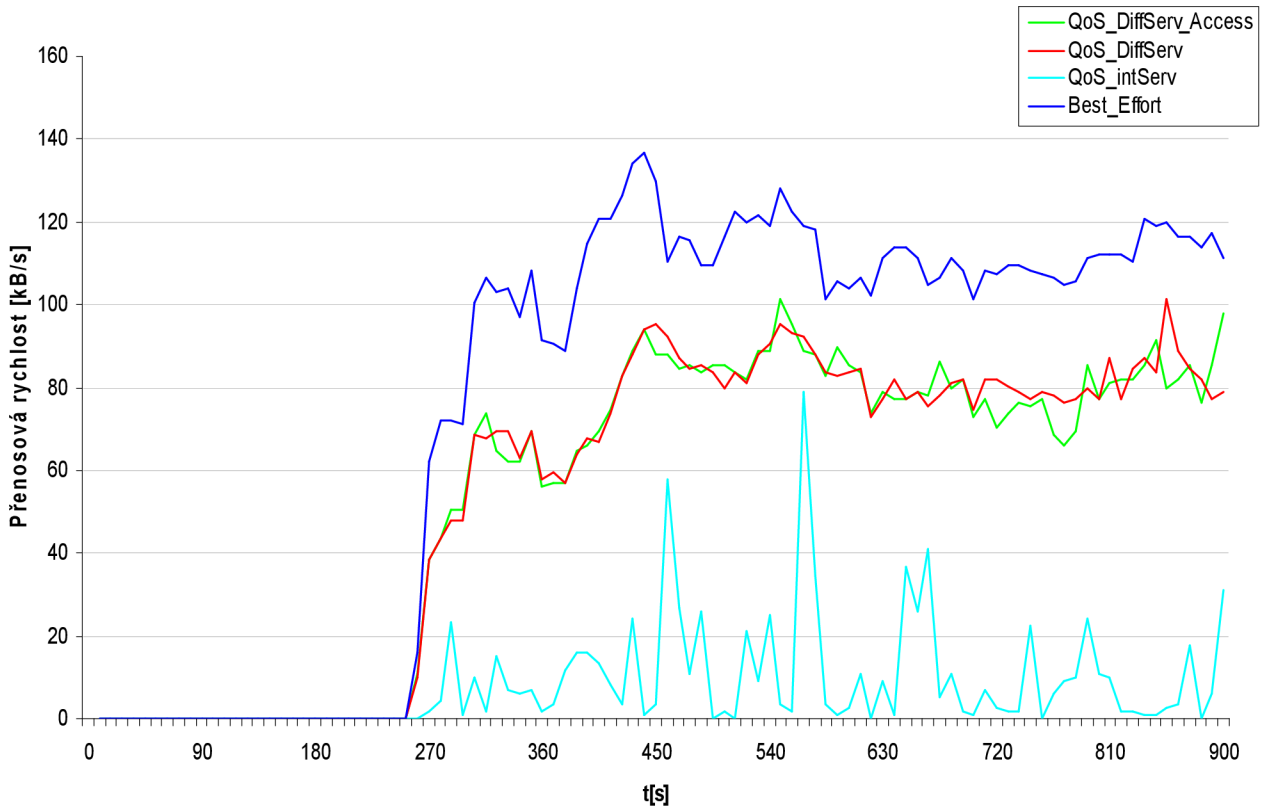
Na Obr. 5.20 je pro příklad růstu zátěže znázorněn počet TCP spojení ve scénáři bez podpory QoS u subsítě Ethernet_VoIP_2. Je vidět, že aplikace FTP_app_4 má podstatně méně TCP spojení než ostatní FTP aplikace. Je tomu tak proto, že soubory které, jsou přijímány ze serveru, nemají tak velkou velikost jako u ostatních aplikací a interval mezi dalším požadavkem na FTP server je dostatečně dlouhý. Avšak i při takovémto nastavení dojde v případě vysoce zatížené sítě k omezení šířky pásma a díky tomu k prodloužení doby

stahování souboru z FTP. Následkem toho je, že i zde dojde k nárůstu TCP spojení, avšak jen v jednom případě. Dá se ovšem předpokládat, že při delší době simulace by i zde došlo k početnému nárůstu TCP spojení. Aplikace FTP_app_3 je nakonfigurována tak, že interval mezi dvěma požadavky na server je kratší než dojde k plnému nahrání souboru na stanici. Proto dojde také k postupnému nárůstu TCP spojení na FTP server. Aplikace FTP_app_2 má nastaven nejkratší interval mezi požadavky na server a z grafu je tedy patrné, že asi po 40 sekundách dojde k dalšímu požadavku. To má za následek rychlý nárůst TCP spojení a také velké zatížení sítě. Aplikace FTP_app_1 začne vysílat asi 10 sekund po spuštění profilu a stahuje ze serveru data s největší velikostí a má nakonfigurován nejdelší interval mezi žádostmi na server. Toto postupné nastavení startu FTP aplikací bylo zvoleno kvůli nastavení postupně vzrůstající zatížení sítě. A jak bude později ukázáno, díky tomuto nastavení bude zřetelné, jak postupně vzrůstá zpoždění u aplikací pracujících v reálném čase.



Obr. 5.21 Srovnání počtu TCP spojení při různém nastavení QoS u aplikace FTP_app_3

Na Obr. 5.21 je znázorněn počet TCP spojení mezi FTP aplikací FTP_app_3 a FTP serverem ve stejné subsíti jako tomu bylo u předchozího grafu. Zde je znázorněna zatíženost sítě při různém QoS pomocí počtu vytvořených TCP spojení. V případě služby Best Effort, jak již bylo řečeno výše, je vidět, že s postupnou zátěží sítě vzrůstá i doba přenášení souboru ze serveru na stanici. V případě scénáře QoS_DiffServ a QoS_DiffServ_Access můžeme pozorovat, jak se doba přenosu souborů zvětšila a došlo i k nárůstu počtu TCP spojení. Je tomu tak proto, že při zařazení služeb do QoS tříd nemá již služba FTP tak velkou šířku pásma, která je pronajata přednostně službám pracujícím v reálném čase. Při scénáři QoS_IntServ došlo ještě k většímu potlačení šířky pásma, jelikož při použití rezervačního protokolu RSVP dojde k vyhrazení virtuálního okruhu pro služby pracující v reálném čase. Tím se podstatně zmenší šířka pásma, kterou můžou aplikace bez vyhrazeného provozu využívat.



Obr. 5.22 Průběh komunikace FTP_app_2 při různém QoS

Z grafu na Obr. 5.22 je vidět vliv různého nastavení kvality služeb v síti. V případě scénáře Best Effort je vidět, že FTP aplikace má k dispozici největší šířku pásma ale na úkor aplikací pracujících v reálném čase, jak bude později ukázáno.

V případě scénáře QoS_DiffServ a QoS_Diffserv_Access můžeme vidět podobné výsledky. Je to kvůli tomu, že zobrazená FTP služba pracuje v síti Ethernet. To má za následek to, že zde není uskutečněno mapování z technologie DiffServ na jiné přenosové technologie tak, jak tomu je např. u služby Wi-Fi. Důležité ale je, že při těchto scénářích dojde k poklesu přenosové rychlosti FTP aplikace. Je tomu tak proto, že jsou upřednostněny aplikace, které mají větší prioritu v rámci technologie DiffServ.

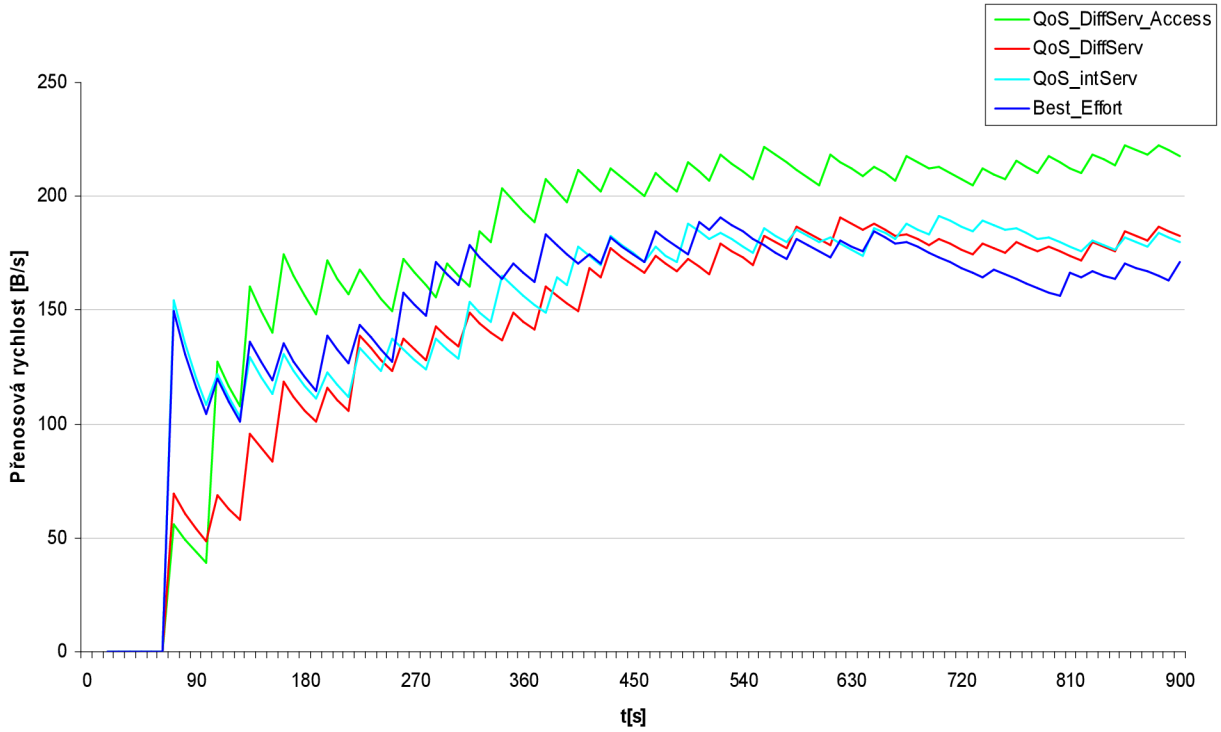
U scénáře QoS_IntSevr můžeme pozorovat nejmenší přenosovou rychlost, je to způsobeno rezervací síťových prostředků protokolem RSVP. Díky tomu mají aplikace, které nemají tento protokol nastavený, podstatně menší šířku přenosového pásma na rozdíl od služeb pracujících v reálném čase, které mají tuto šířku pásma permanentně vyhrazenou až do ukončení spojení.

5.5.2 Aplikace HTTP

Aplikace HTTP je textově orientovaný aplikační protokol určený pro přenos hypertextových formátů psaných např. v HTML kódu. Jako transportní protokol používá (stejně jak služba FTP) protokol TCP. Server HTTP naslouchá přicházejícím žádostem na portu 80. Komunikace na bázi protokolu HTTP funguje na principu žádost-odpověď. Hlavním rozdílem oproti službě FTP je, že tento protokol je tzv. interaktivní. To znamená, že takováto

komunikace je již více náchylná na časové zpoždění, jelikož uživatel vyžaduje odpověď ze serveru prakticky okamžitě. Na rozdíl od FTP, protokol HTTP nepotřebuje tak velkou šířku pásma. Kolísání zpoždění službu HTTP také nijak neomezuje.

Z grafů na Obr. 5.23 jsou vidět průběhy průměrné přenosové rychlosti u aplikace HTTP v subsíti WLAN_Video_1. Byla zvolena průměrná hodnota zobrazení, jelikož klasické zobrazení by bylo dosti nepřehledné a podalo by neodpovídající výsledky. Z grafu je tedy patrné, že při nakonfigurování end-to-end QoS má HTTP aplikace větší šířku pásma než při ostatních provozech. Ve scénáři QoS_IntServ byla služba HTTP ponechána ve stejném nastavení, jako je tomu u scénáře QoS_DiffServ. Tedy služba byla řazena do patřičných tříd až v páteřní síti. Je tomu tak proto, že protokol RSVP je vhodný pouze pro aplikace pracující v reálném čase. Pokud by byl nastaven rezervační protokol u každé služby typu HTTP, došlo by velmi rychle k vyčerpání celé dostupné šířky pásma reservačním protokolem a další komunikace by byla již odmítnuta.



Obr. 5.23 Průběh komunikace HTTP_app_1 při různém QoS

5.5.3 Aplikace VoIP

VoIP telefonie se začala rozvíjet s rozmachem paketové komunikace. Hlavním rozdílem oproti klasické telefonii je, že tato služba komunikuje na základě paketové služby, tedy tzv. spínání paketů, kdežto klasická telefonie využívá spínání okruhů. Komunikace této služby probíhá tak, že vysílací stanice musí obsahovat zařízení, které převede analogový řečový signál do digitální podoby. Čili je zapotřebí signál vzorkovat, kvantovat a následně kódovat do binární soustavy. Dále jsou data zabezpečena proti chybám a přizpůsobena na vysílací kanál. Po přenesení dat je signál inverzním způsobem zpracován a předán příjemci. U tohoto druhu komunikace vzniká zmiňovaným způsobem velké zpoždění. Dále tato služba pracuje na UDP protokolu, tudíž nelze nijak detekovat a následně znovu poslat ztracené pakety. Navíc tato komunikace nemá tak jako u klasické telefonie trvale vyhrazený vysílací kanál. Jelikož

tedy služba pracuje ve sdíleném prostředí, je jí třeba ze zmiňovaných důvodů zajistit nějakou prioritu před ostatními časově nezávislými přenosy dat.

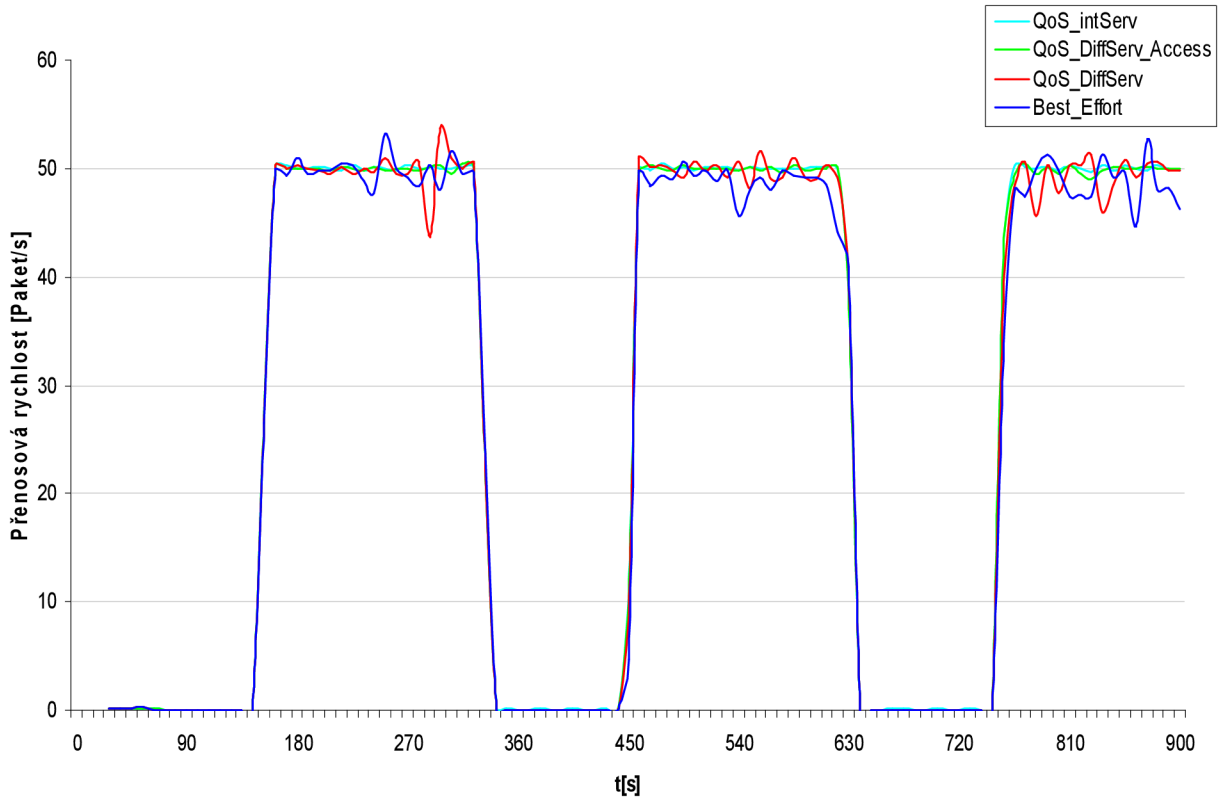
Tab. 5.9 QoS parametry pro službu VoIP [7]

Parametry/Kvalita	dobrý	akceptovatelný	neuspokojivý
Zpoždění [ms]	0 - 150	150 - 300	> 300
Kolísání zpoždění [ms]	0 - 20	20 - 50	> 50
Ztrátovost [%]	0 - 0,5	0,5 - 1,5	> 1,5

Služba VoIP nemá velké nároky na šířku přenosového pásma. Zvolený GSM kodek má přenosovou šířku pásma na aplikační vrstvě 13,2kb/s. Naopak tato služba je velmi citlivá na včasné doručení a na kolísání zpoždění. Tab. 5.9 ukazuje limitní hodnoty důležitých QoS parametrů pro VoIP aplikaci.

Na Obr. 5.24 jsou zobrazena přijatá data mezi uživateli Wireless_VoIP_9 a Wireless_VoIP_7. Můžeme pozorovat změny v čase, a to i při změnách kvalitativních požadavků. Jak bylo zmíněno dříve, FTP aplikace byly odstupňovány tak, aby zátěž postupně s časem rostla. To je dobře vidět z průběhu komunikace v scénáři Best Effort. Při prvním hovoru nebyl rozkmit přenosové rychlosti tak velký jako v druhém a třetím hovoru, kde byl pokles přenosové rychlosti oproti prvnímu hovoru dosti znatelný.

Při použití kvality služeb v páteřní síti ve scénáři QoS_DiffServ je vidět, že rozkmit již není tak velký, ale stále je znatelný. Je to způsobeno tím, že provoz je řazen do kvalitativních tříd až v DiffServ doméně, ale uvnitř přístupové sítě Wi-Fi není kvalita nijak zajištěna. Provoz v těchto sítích používá pouze náhodnou přístupovou metodu CSMA/CA, která nezjišťuje žádné diferencované zacházení se službami náročnými na kvalitativní parametry.

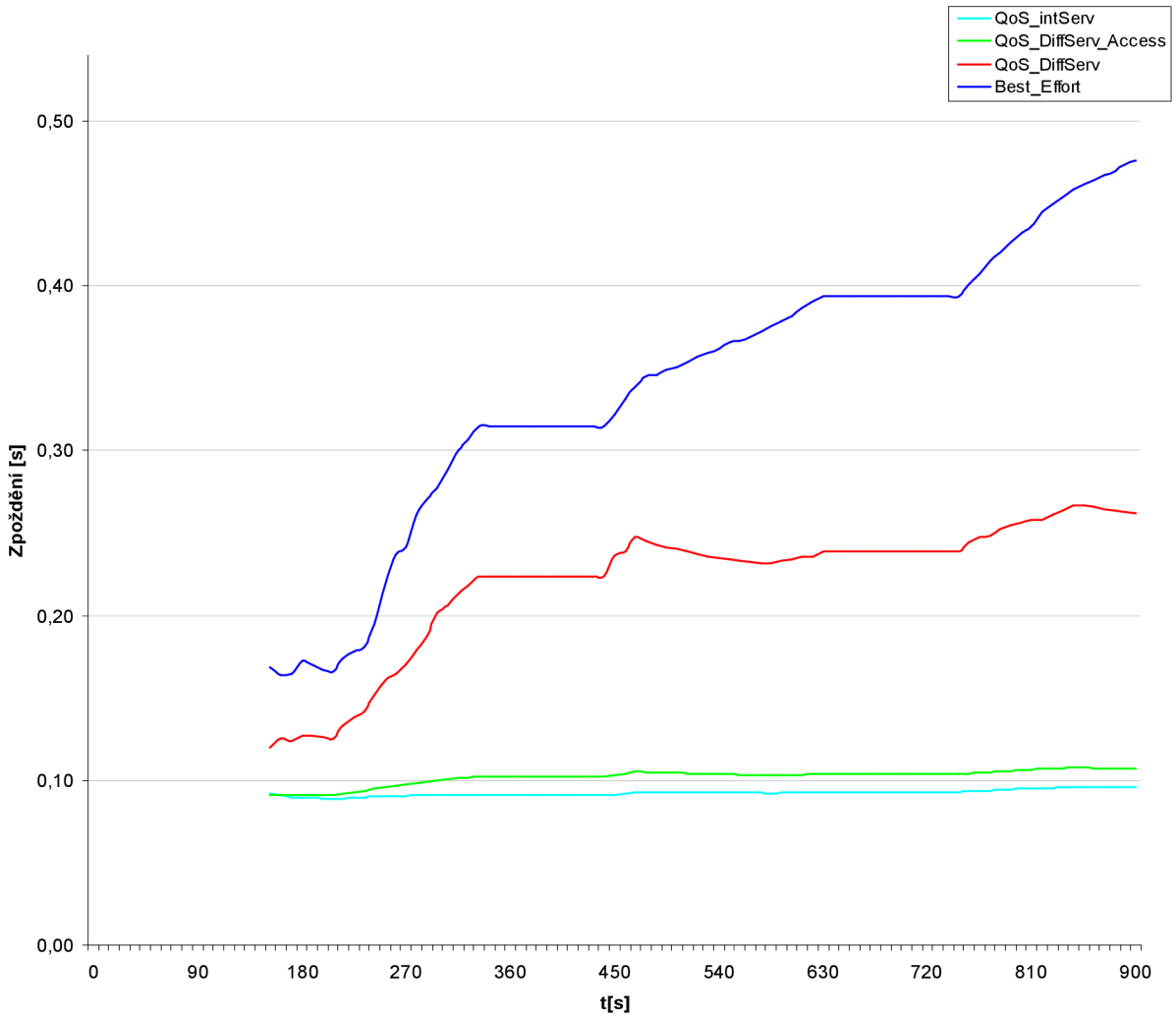


Obr. 5.24 Průběh komunikace mezi dvěma VoIP klienty při různé QoS

Křivky pro scénáře QoS_DiffServ_Access a QoS_IntServ se skoro překrývají a, jak můžeme vypozorovat z grafu, jsou průběhy stálé a nijak nekmitají.

V případě QoS_DiffServ_Access je již i v Wi-Fi síti implementovaná přístupová metoda EDCA, která již příchozí i odchozí provoz řadí do jedné ze čtyř patřičných QoS tříd. Přesná funkce EDCA je popsána v kapitole 3.2.1.

Ve scénáři QoS_IntServ byl nakonfigurován RSVP rezervační protokol, který v průběhu VoIP komunikace opakovaně zasílal každých 30 sekund RSVP zprávy, sloužící k udržení vyhrazeného spojení mezi VoIP uživateli. Původní snaha byla implementovat RSVP protokol do Wi-Fi subsítě pomocí funkce HCCA. To znamená, že by si komunikaci s koncovými uživateli řídil sám přístupový bod. Postupně by se dotazoval stanic, jestli mají data k odeslání. Pokud ano, udělil by jim oprávnění vysílat a přidělil určité vysílací okno. Toto nastavení by bylo vzhledem k charakteru služby IntServ nejvhodnější. Nicméně bylo zjištěno, že Opnet Modeler tuto funkci nepodporuje, a pod označením HCF používá metodu EDCA. Z těchto důvodů byla služba IntServ mapována stejně jak DiffServ do tříd pomocí služby EDCA.



Obr. 5.25 Srovnání zpoždění pro službu VoIP při různé QoS

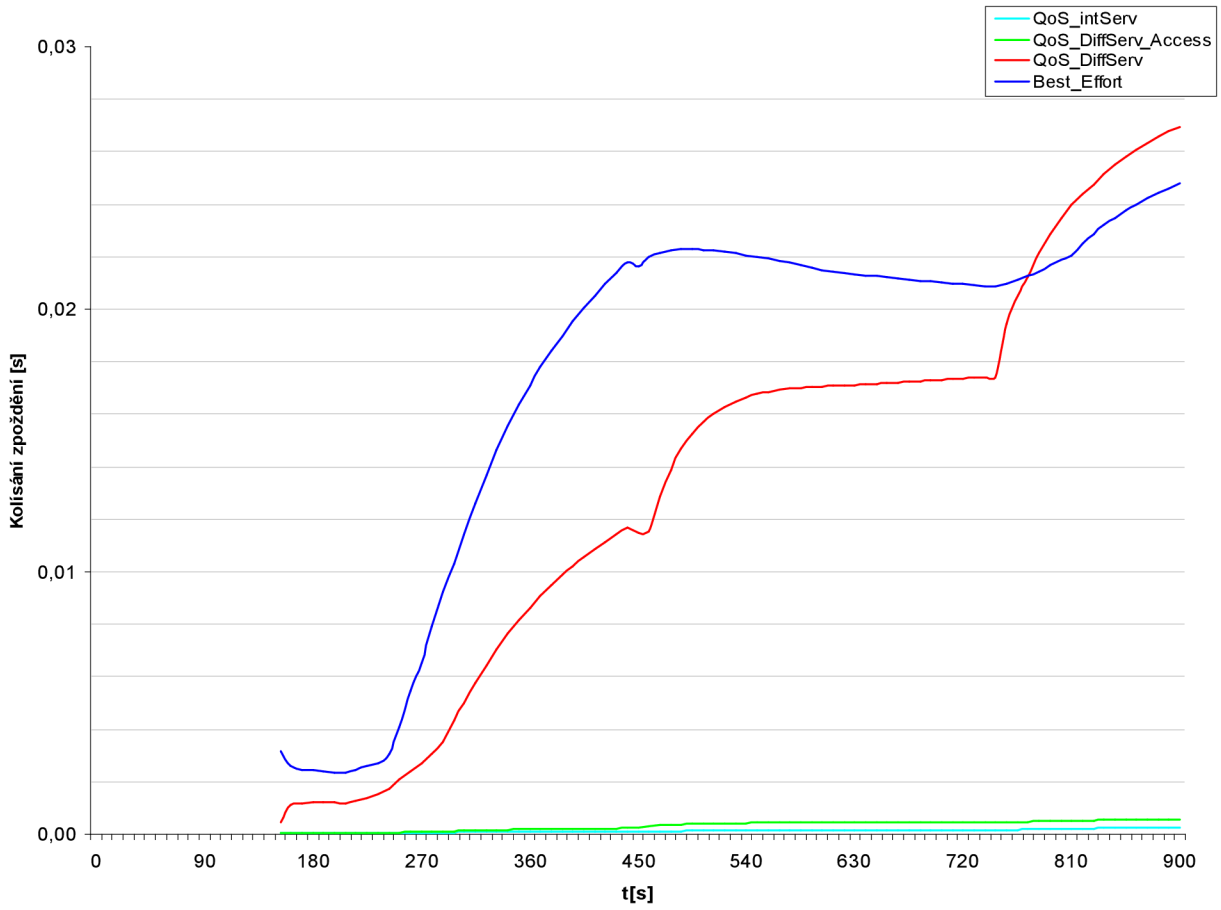
Graf Obr. 5.25 zobrazuje průměrné zpoždění pro různé kvalitativní třídy provozu. V případě scénáře Best_effort je zpoždění největší a s postupem času stále narůstá. Můžeme

vidět, že v čase 340 sekund dojde k překročení maximálního povoleného zpoždění pro VoIP, které je 300ms. Dále zpoždění narůstá až k hodnotě cca 500ms. Jedná se však o průměrné zpoždění, okamžité zpoždění může narůstat i do vyšších hodnot. Je tedy patrné, že služba VoIP nemůže bez podpory QoS absolutně pracovat správně, případně může fungovat jen v málo zatížené síti.

Scénář QoS_DiffServ vykazuje již podstatně lepší vlastnosti. V tomto scénáři se zpoždění pohybuje v rozmezí 120 až 250ms, a to odpovídá klasifikaci akceptovatelného spojení. Ale v případě ještě více zatížené sítě by pravděpodobně i toto zpoždění vzrostlo nad 300ms. Takovéto spojení by již bylo neuspokojivé.

V případě scénáře QoS_DiffServ_Access je již kvalita hovoru dle tabulky Tab. 5.9 klasifikována jako dobrá. Zpoždění se pohybuje kolem hodnoty 100ms a nevykazuje velké tendence se zátěží rapidně vzrůstat.

V posledním QoS_intServ je zpoždění nejmenší oproti ostatním. Je přibližně o 20ms menší než při použití služby DiffServ po celé komunikační trase. Je to způsobeno vyhrazením komunikačního kanálu od zdroje vysílání k příjemci. Toto zarezervování zdrojů je velmi podobné službám v klasické telefonii - tedy při přepínání okruhů. Zde je také rezervace ustanovena pro celou dobu komunikace a prostředky jsou rezervovány, i když nejsou v tomto kanále přenášena žádná data.



Obr. 5.26 Srovnání kolísání zpoždění pro službu VoIP při různé QoS

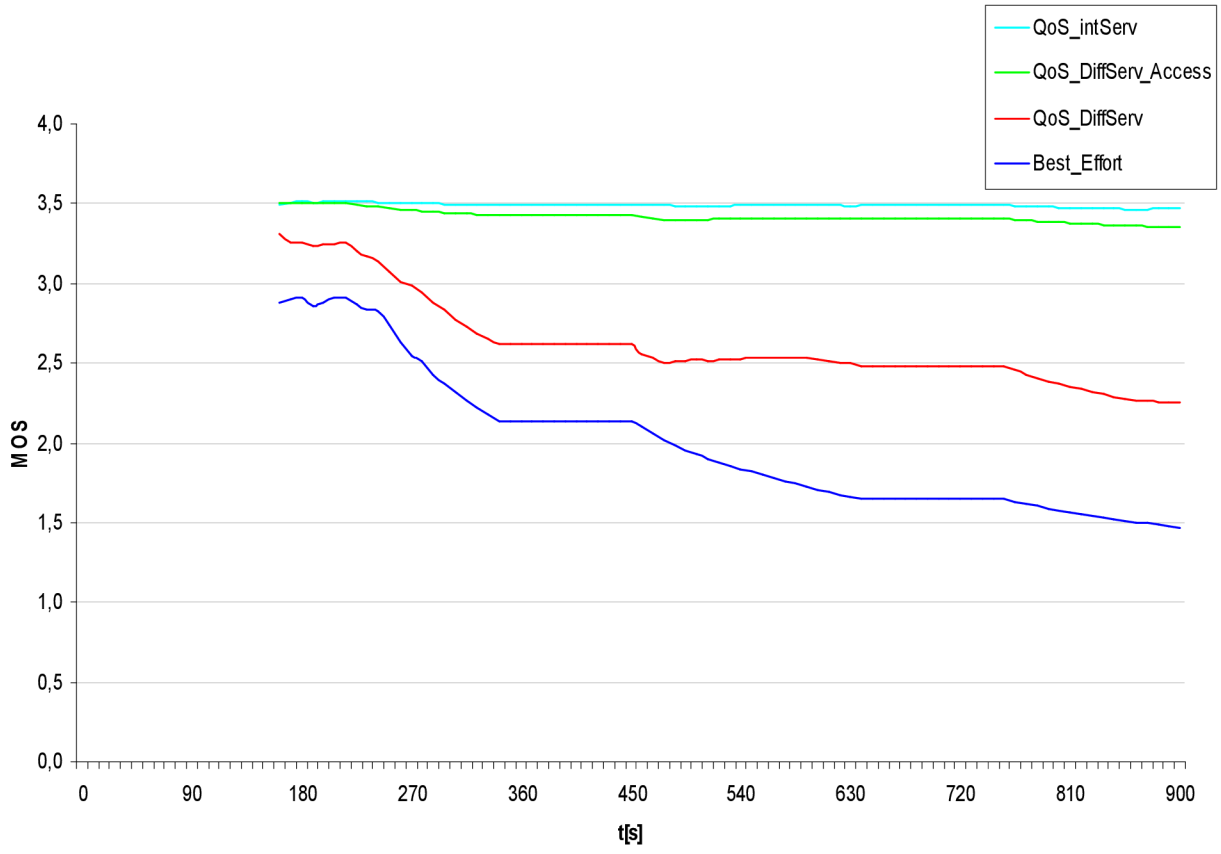
Graf Obr. 5.26 znázorňuje průměrné kolísání zpoždění. Zde je vidět, že tento parametr v simulované síti nemá natolik fatální důsledky jako zpoždění. Pouze v případě velkého

zatížení linky je vidět, že se hodnota kolísání zpoždění dostala do hodnocení kvality jako akceptovatelná. Nicméně kdyby byla délka simulace nastavena na větší hodnotu, měl by tento parametr stále vzestupnou tendenci a komunikace by byla také znemožněna. Kolísání zpoždění je způsobeno rozdílnou délkou průchodu paketu sítí. To znamená, pokud jsou požadavky na FTP a HTTP servery častější, bude paket s VoIP daty čím dál tím více pozdržen ve vyrovnávacích pamětech směrovačů a tím bude toto kolísání zpoždění zvyšovat svoji hodnotu.

V grafu průměrného kolísání zpoždění jsou zobrazeny hodnoty pro různé třídy služeb. V případě scénáře Best_Effort se toto kolísání zpoždění v průběhu simulace zvětšuje až na hodnotu 24ms. Tato hodnota je klasifikovaná jako akceptovatelná. Výsledek je ale poměrně zkreslená zprůměrňováním hodnot v tomto grafu. Kdyby ale byl zobrazen graf bez zprůměrňovaných hodnot, výsledky by byly dosti nepřehledné. Proto byly voleny průměrné hodnoty, které podávají přehledné výsledky, i když jsou zatíženy chybou. Dále je toto zobrazení vhodné pro porovnání jednotlivých kvalitativních tříd.

Ve scénáři QoS_DiffServ je toto kolísání zpoždění menší a pohybuje se průměrně kolem hodnoty 150ms, což je klasifikováno jako dobré. Je tedy vidět, že i špatně nastavené mapování QoS, respektive použití QoS pouze v páteřní síti, vede k lepším výsledkům než u scénáře Best_Effort.

V případě scénářů QoS_DiffSev_Access a QoS_IntServ jsou hodnoty klasifikované jako dobré a maximálně nabývají hodnot 1ms. To dokazuje, že správné nastavení QoS vede k podstatně lepším výsledkům než v případě částečné podpory nebo vůbec žádné podpory QoS. Scénář s podporou IntServ opět i zde vykazuje lepší výsledky, i když při tak malém kolísání zpoždění je tento rozdíl zanedbatelný.



Obr. 5.27 Srovnání MOS parametru pro službu VoIP při různé QoS

Poslední graf k VoIP komunikaci je zobrazen na Obr. 5.27. Tento graf zobrazuje průměrnou hodnotu parametru MOS (Mean Opinion Score). Jedná se o parametr, který souvisí s kvalitou VoIP hovoru a může nabývat hodnot od 1 až 5. Hodnota 5 značí nejlepší kvalitu a hodnota 1 nejhorší. Tento parametr je odvozen od poslechu hovoru velkým počtem uživatelů a na základě jejich subjektivních pocitů z kvality hovoru byla vytvořena tato stupnice.

Z grafu je vidět, že výsledky dosažené rozdílnou QoS vychází podle přepokládaných teoretických hodnot. Scénář Best_Effort vykazuje nejhorší parametry MOS, které se blíží při největším vytížení sítě až průměrné hodnotě 1,5. Hovor s takovou nízkou hodnotou sice je možné uskutečnit, ale uživatelé takové služby by si vůbec nerozuměli a pravděpodobně by komunikaci ukončili.

Druhý scénář s nastavením QoS pouze v páteřní síti vykazuje zlepšení oproti předchozímu scénáři, ale i tak parametr MOS dosahuje až hodnoty 2,3, což je taky velmi neuspokojivá kvalita hovoru.

Scénáře s plnou podporou DiffServ a IntServ i v přístupových sítích, vykazují nejlepší vlastnosti. Dokonce v případě služby IntServ má parametr MOS konstantní průběh, je to způsobeno vyhrazením virtuálního okruhu, ke kterému nemají přístup další datové služby. Hodnota MOS u IntServ se pohybuje kolem hodnoty 3,5, což je již považováno za kvalitní hovor. V případě scénáře DiffServ_Access je maximálně tato hodnota 3,3, která je také považovaná za dobrou kvalitu hovoru.

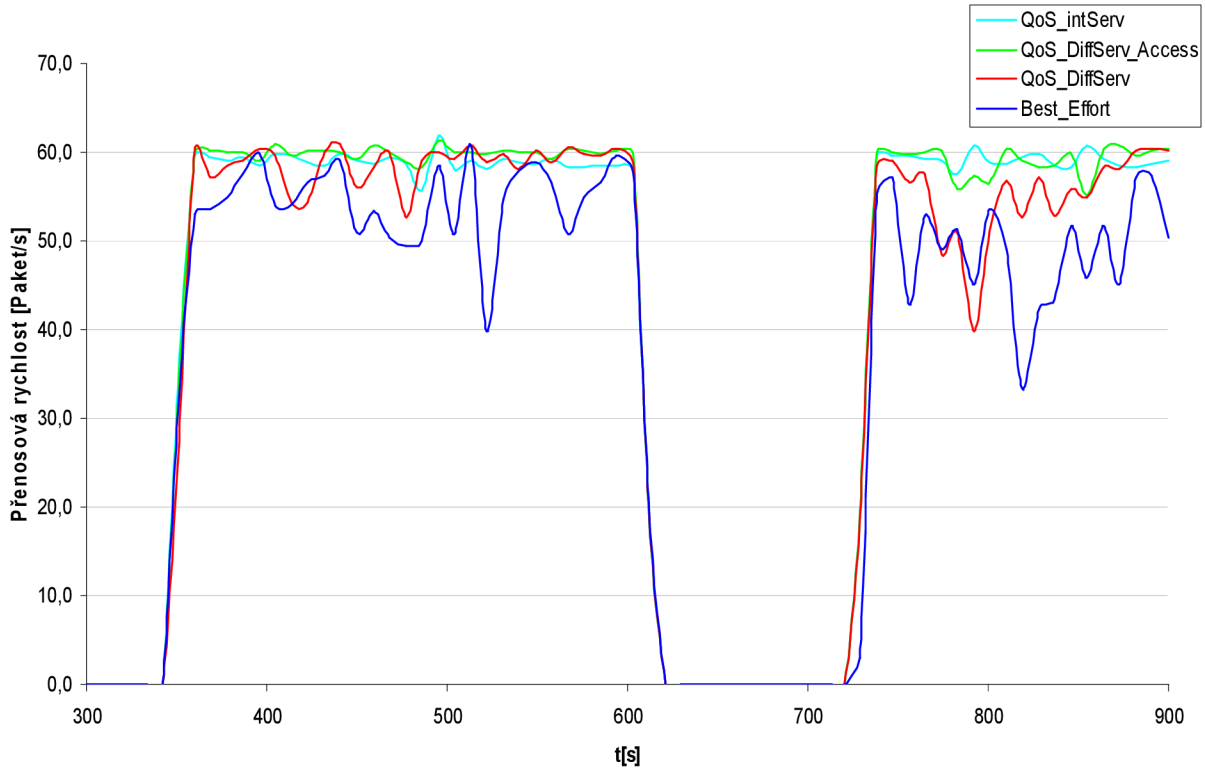
5.5.4 Aplikace videokonference

Tato služba má velmi podobné vlastnosti jako služba VoIP. Největší rozdíl mezi těmito službami je v přenosové šířce pásma. Videokonference potřebuje pro svůj provoz až několikanásobně větší šířku pásma než VoIP služba. Je tomu tak proto, že kromě hlasu se přenáší i obraz zakódovaný patřičným kodekem.

Na Obr. 5.28 je znázorněna komunikace mezi videoterminály v subsíti Wireless_Video_1 a Wireless_Video_2. Můžeme zde pozorovat, že v případě scénáře Best_Effort signál značně degraduje a v některých místech klesne přenosová rychlost až na poloviční hodnotu. Je to způsobeno tím, že o šířku pásma se tato služba dělí i s ostatními službami a není nikterak zajištěna prioritizace různých datových toků.

V případě druhého scénáře tedy QoS_DiffServ je komunikace o něco lepší, ale i zde dochází k poklesu přenosové rychlosti. Je to proto, že QoS je sice zajištěna v páteřní síti, ale od hraničních směrovačů, v našem případě se jedná např. o WiFi směrovače, již tato služba zajištěna není. Příchozí data na tento směrovač jsou dále řazena do fronty, která je stejná pro všechny datové toky, a to v pořadí, jak právě dorazily. Tím vznikne degradace signálu i když v páteřní síti byly jednotlivé datové toky rozděleny podle jejich kvalitativních tříd. Stejné je to v odchozím směru, kdy dochází k vysílání dat z jednotlivých stanic pomocí metody náhodného přístupu CSMA/CA. Tady není zajištěna také žádná priorita pro služby náchylné na včasné doručení.

U scénáře QoS_DiffServ_Access je již průběh přenosové rychlosti dobrý. Signál nikterak nekolísá a drží si poměrně konstantní hodnotu v celém průběhu hovoru. Je to způsobeno nastavením přístupové metody EDCA u koncových Wi-Fi stanic a u Wi-Fi směrovačů. Jakmile dorazí data na tento směrovač, dojde k přemapování DiffServ tříd na čtyři třídy používané v technologii EDCA a tím jsou data rozdělena do front podle jejich důležitosti a je s nimi podle této důležitosti zacházeno. Stejné je to i v odchozím směru, kdy koncová stanice, která má data s vyšší prioritou, může přednostně začít vysílat, jelikož má kratší čekací interval AIFS a délku okna CW. Ve směrovači jsou zpětně tyto parametry namapovány do DiffServ tříd.



Obr. 5.28 Průběh komunikace při videokonferenci s různou QoS

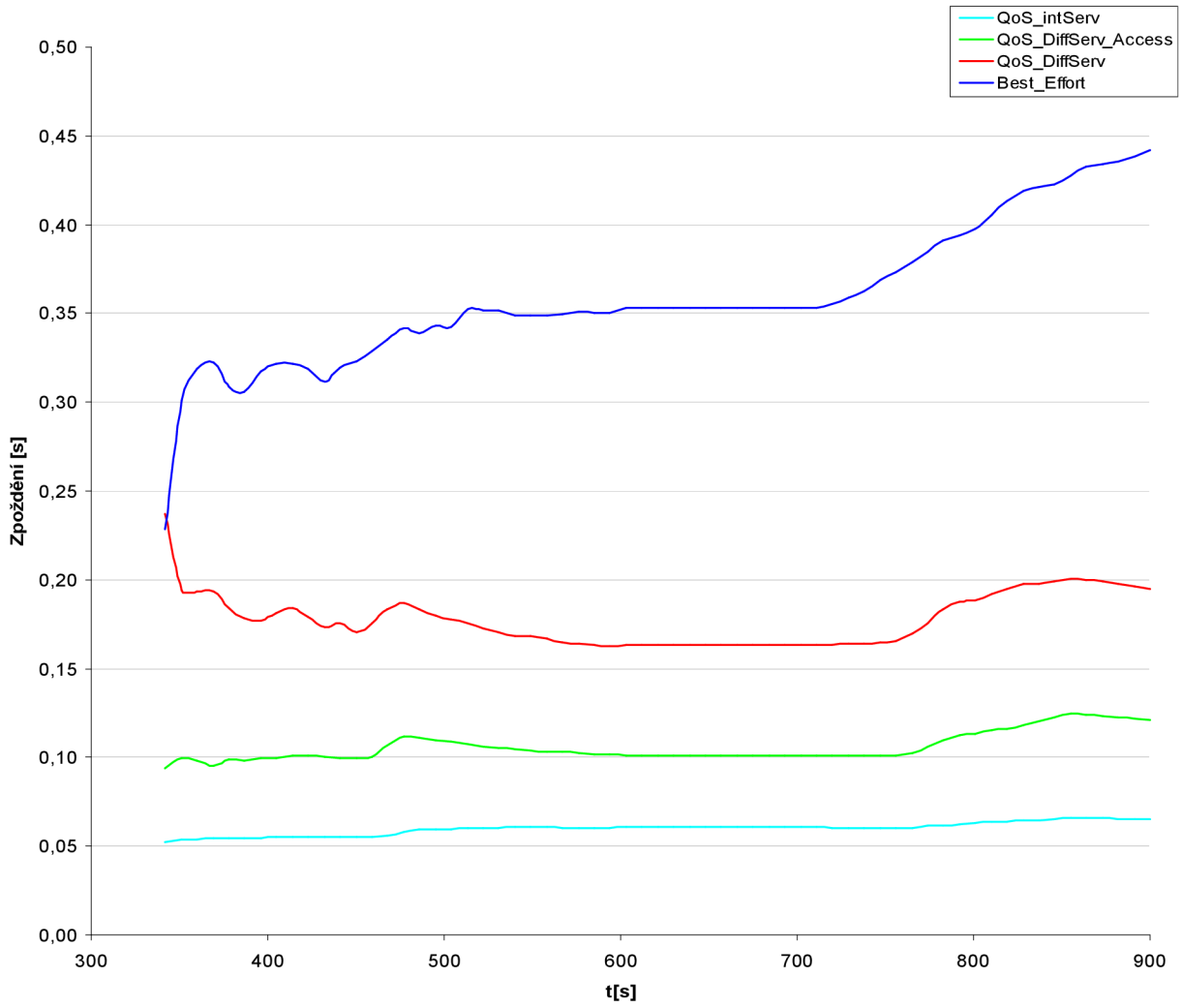
Scénář QoS_IntServ má shodné nastavení s předchozím scénářem, jelikož, jak bylo popsáno v kapitole o VoIP, nelze zde nastavit přístupovou technologii HCCA. Oproti předchozímu scénáři je zde ale nastaven rezervační protokol RSVP, který vybuduje spojení od zdroje vysílaní k cíli a vyhradí tak permanentní virtuální kanál pro danou komunikaci. Zprávy jsou stejně tak jak u aplikace VoIP opětovně zasílány každých 30 sekund.

V grafu Obr. 5.29 je znázorněno zpoždění aplikace videokonference. Můžeme pozorovat, že v případě scénáře Best_Effort je zpoždění nejhorší a pohybuje se v rozmezí průměrných hodnot 250 až 450ms. Dále můžeme pozorovat, že s rostoucím zatížením roste i zpoždění. Prakticky v celém rozsahu je zpoždění neakceptovatelné a video hovor by nemohl korektně fungovat. Docházelo by k značnému trhání obrazu i zvuku.

Ve scénáři QoS_DiffServ je již komunikace značně kvalitnější. Hodnota zpoždění se pohybuje v rozmezí 170 až 240ms. Toto zpoždění se dá kvalifikovat jako akceptovatelné. Za největší nárůst tohoto zpoždění jsou nejvíce zodpovědné přístupové sítě, které nepodporují mechanizmy QoS.

Scénář QoS_DiffServ_Access podává velmi dobré výsledky pro video hovor. Je vidět, jak správné nastavení QoS i v přístupových sítích značně snížilo zpoždění oproti předchozímu scénáři. Zpoždění se zde pohybuje kolem hodnoty 100ms, což je považováno za dobrou kvalitu hovoru.

Nejlepší výsledky vykazuje scénář s podporou IntServ. Zde je patrné bezkonkurenčně nejlepší zpoždění pohybující se kolem hodnoty 60ms. Jak bylo řečeno dříve, je to způsobeno díky vyhrazenému virtuálnímu spoji a přednostnímu zacházení s pakety označenými značkou, která udává, že daný datový tok patří do vyhrazeného virtuální spoje.



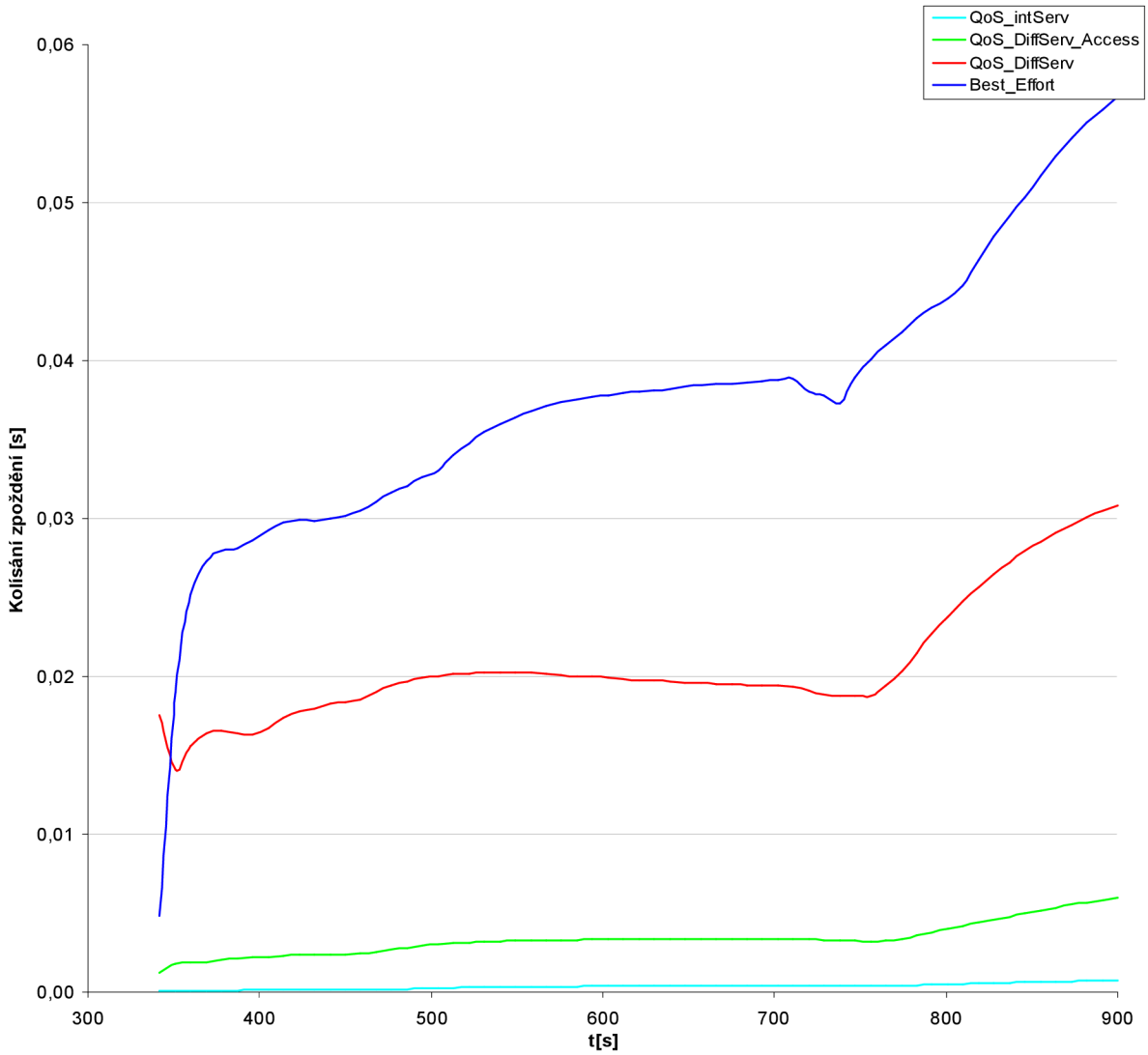
Obr. 5.29 Srovnání zpoždění pro službu videokonference při různé QoS

Poslední graf Obr. 5.30 zobrazuje kolísání zpoždění u aplikace videokonference. Opět jako tomu bylo u aplikace VoIP jsou zobrazeny průměrné hodnoty, které nejsou tak extrémní jako okamžité. U scénáře Best_Effort přesahuje toto zpoždění hodnotu 50ms, a to je pro video službu již neuspokojivé. Většinu času se však pohybuje toto zpoždění kolem hodnoty 35ms, která je klasifikována jako akceptovatelná.

U scénáře QoS_DiffServ se hodnota kolísání zpoždění pohybuje kolem hodnoty 20ms. Tato hodnota je na rozhraní klasifikace dobré až akceptovatelné, ovšem s rostoucí zátěží toto zpoždění rapidně roste.

Scénář QoS_DiffServ_Access vykazuje hodnotu kolísání zpoždění v rozmezí 1 až 6ms, což je velmi dobré, a růst tohoto zpoždění není tak strmý jako v případě dvou předchozích scénářů.

Poslední scénář QoS_IntServ vykazuje nejmenší hodnotu kolísání zpoždění, a to kolem 1ms. Tato hodnota je v podstatě konstantní v průběhu obou hovorů i při značně zatížené síti.



Obr. 5.30 Srovnání kolísání zpoždění pro službu videokonference při různé QoS

5.5.5 Subsystém IMS

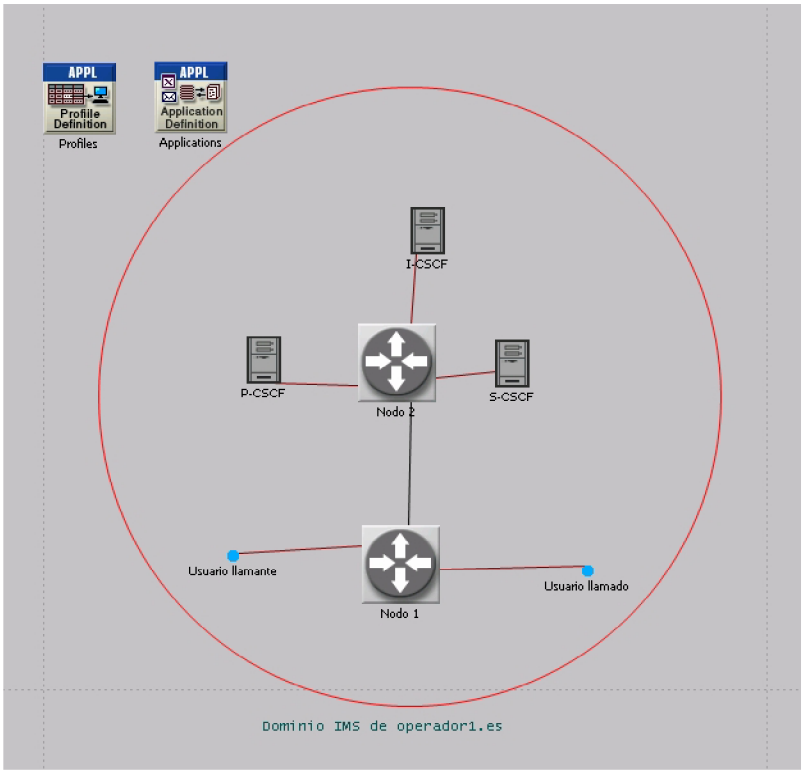
Na počátku této práce byl záměr do vytvořené sítě implementovat subsystém IMS, který by na základě uložených profilů uživatele vyjednal požadovanou kvalitu služeb. Simulační nástroj Opnet Modeler bohužel neobsahuje modul IMS. Uvádí však na svých internetových stránkách modul IMS, který byl vytvořen studenty na univerzitě ve Španělsku.

Tento model je rozšířením originálního SIP modelu, který byl již dříve v standardních knihovnách Opnet Modeleru zahrnut. Toto rozšíření umožňuje komunikaci koncových uživatelů přes více než jeden proxy server. Model obsahuje sadu tří serverů, a to S-CSCF, P-CSCF a I-CSCF, které jsou nezbytné pro fungování IMS sítě. Dále byly rozšířeny SIP zprávy o kompletní sestavení SIP spojení před samotným vysíláním uživatelských dat. Byla zde také vytvořena podpora roamingu mezi doménami patřícím jiným IMS operátorům. Dále je zde také vytvořeno umělé spojení mezi servery a databází HSS, které bylo reprezentováno nastavitelnou hodnotou zpoždění dané komunikace. Tento kompletní model

tedy dokázal simulovat sestavení IMS relace včetně zpoždění vznikajícího v rámci přenosu informace z databáze HSS a vyřízení požadavku na příslušných serverech.

Bohužel tento model neobsahuje zmiňovanou databázi HSS, a tak není možné provést registraci uživatelů a patřičné nastavení kvalitativních požadavků. Databáze HSS je nezbytnou součástí IMS sítě, bez které není možné rozhodovat o službách přiřazených jednotlivým uživatelům a vzájemné provázanosti uživatelů a služeb. V databázi HSS jsou uloženy profily uživatelů. Pokud chce některý z těchto uživatelů komunikovat, je vždy dotázáno HSS, jestli má daný uživatel oprávnění k požadované službě a jaké kvalitativní služby jsou mu povoleny. V případě oprávnění k zmiňované službě a patřičné QoS dojde k nastavení hraničních směrovačů tak, aby danému datovému toku přiřadili správný identifikátor provozu.

Díky faktu, že zde není databáze HSS implementována, ztrácí tento model význam z hlediska podstaty subsystému IMS. Jak bylo popsáno výše z pohledu kvality služeb není tento model použitelný, proto nebyl implementován do vytvořené sítě. Na Obr. 5.31 je znázorněn zmiňovaný model sítě IMS.



Obr. 5.31 Model IMS subsystému

6 ZÁVĚR

Práce byla zaměřena na problematiku kvality služeb QoS a síťového subsystému IMS. Počátek byl věnován teoretické části dané problematiky. Byl objasněn vrstvový model subsystému IMS, byla popsána architektura tohoto subsystému a dále byly podrobně popsány jednotlivé funkční bloky.

Další kapitola se zaobírala protokoly, které jsou nedílnou součástí IMS. Jedná se především o tyto protokoly: SIP, SDP, Diameter.

Velká část teoretického úvodu byla věnována QoS. Bylo podrobně rozebráno, proč je tato služba důležitá z hlediska služeb pracujících v reálném čase, a dále byly popsány a vysvětleny jednotlivé parametry, které souvisí s QoS. Stěžejním bodem této práce je vzájemné porovnání dvou typů zajištění kvality služeb. Jsou jimi služby DiffServ a IntServ. Každá tato služba vyjednává kvalitu služeb jiným způsobem, který je zde patřičným způsobem popsán.

V následující kapitole bylo stručně popsáno simulační prostředí Opnet Modeler a jeho základní části.

Praktická část se věnovala simulacemi sítí s různým nastavením QoS v simulačním prostředí Opnet Modeler. Tato práce nemá sloužit jako výukový text k vývojovému prostředí Opnet Modeler, proto zde není detailně popsán postup konfigurace. Nicméně nastavení jednotlivých bloků, které jsou důležité pro danou simulaci, je podrobně vysvětleno.

Po seznámení s konfigurací byla pozornost směřována na simulaci sítě, která se skládala ze čtyřech scénářů s různým nastavením QoS. Scénáře byly tvořeny páteřní sítí a subsítěmi Wi-Fi, UMTS a Ethernet. V takto vytvořené síti byly provozovány čtyři aplikace s rozdílnými požadavky na přenos. Jedná se o služby FTP, HTTP, VoIP a videokonferenci. První scénář byl bez jakékoliv podpory kvality služeb, tedy všechny aplikace byly v třídě best effort. Druhý scénář podporoval mechanismus DiffServ, ale pouze v páteřní síti, tedy po směrovače, které oddělovaly síť páteřní od přístupové. Třetí scénář obsahoval také technologii DiffServ, ale tentokrát již i jednotlivé přístupové sítě podporovaly kvalitu služeb. Bylo zde tedy nutné nakonfigurovat správné mapování jednotlivých nosných služeb v subsítích s různou technologií. Poslední scénář byl věnován technologii IntSev. Nastavení sítě zůstalo stejné jako v předchozím scénáři. Rozdíl byl v tom, že pro služby pracující v reálném čase byl nastaven rezervační protokol RSVP, který vybudoval virtuální spojení od zdroje k cíli a vyhradil tak pro danou aplikaci permanentní kanál. Jak bylo zmíněno, nastavení sítě zůstalo stejné jako ve scénáři číslo tři, jelikož bylo zjištěno, že Opnet Modeler nepodporuje přístupovou metodu HCCA, která by měla vykazovat lepší výsledky pro technologii IntServ než přístupová metoda EDCA.

Naměřené výsledky odpovídají teoretickým předpokladům. Scénář bez podpory QoS značně omezuje služby jako VoIP a video, jelikož tyto služby potřebují určitou prioritizaci před ostatními službami, protože jsou velmi náchylné na časové zpoždění a kolísaní zpoždění.

Naopak provoz FTP v tomto scénáři měl největší šířku pásma proto, že hustotou svého provozu naprosto obsadil fronty ve směrovačích, které jsou ve scénáři bez podpory QoS sdíleny všemi aplikacemi. Služba HTTP vykazovala také horší parametry než ve scénářích s podporou QoS.

Výsledky druhého scénáře vykazovaly lepší hodnoty než při scénáři bez podpory QoS. Zde vznikalo největší zpoždění v přístupových sítích, jelikož zde nebyly správně namapovány jednotlivé nosné služby.

Třetí scénář měl již velmi dobré výsledné hodnoty. Zpoždění i kolísání zpoždění vyhovovalo všem službám, pracujícím v reálném čase. Navíc tyto hodnoty byly téměř konstantní v celém simulovaném čase.

Poslední scénář, díky rezervačnímu protokolu RSVP vykazoval nejlepší výsledky ze všech simulovaných scénářů, jelikož každá služba s podporou RSVP dostala přidělený komunikační kanál po celou dobu komunikace. Funkce takového přenosu by se dala přirovnat ke klasické telefonii se spínáním okruhů. Nicméně ale i přes nejlepší výsledky technologie IntServ není tato technologie masivně využívána v páteřních sítích. Je vhodná v kombinaci s technologií DiffServ, která pracuje v páteřní síti, a technologie IntServ se dá tedy použít v sítích LAN. Je to hlavně z důvodu agresivity a neefektivnosti provozu vytvořeného pomocí RSVP protokolu. Jelikož takto vzniklá rezervace obsazuje kanál i v době, kdy nejsou žádná data přenášena, a dále, pokud bychom měli velké množství rezervací, došlo by ke znemožnění vzniku dalších rezervací díky vyčerpání přenosového pásma již sestavenými relacemi. Z těchto důvodů je více preferována technologie DiffServ.

Další částí diplomové práce bylo odsimulovat zmiňované scénáře s podporou IMS subsystému. Opnet Modeler bohužel nevydal oficiální model subsítě IMS. Tohoto úkolu se zhostila španělská univerzita, která vytvořila vlastní IMS modul. Přetvořila předdefinované síťové prvky, které již existovaly v dosavadních modelech. Jejich vytvořený model simuloval komunikaci s CSCF servery a větším množstvím proxy serverů. Bylo zde také možné směrovat datové služby přes cizí sítě IMS do jiné domény. Nicméně jelikož jejich model neobsahoval HSS databázi, není možné, aby takto vytvořený model podporoval plnou registraci, a již vůbec není schopen vyjednávat respektive určovat QoS jednotlivých uživatelů. V databázi HSS, jak bylo popsáno výše, jsou uloženy informace o registrovaných uživatelích, a to včetně jejich předplacených služeb a nastavení kvality služeb, které mají sjednané. Proto je nezbytná komunikace CSCF serverů s HSS. Z těchto důvodů nebyl tento model zařazen do simulovaných scénářů, jelikož z hlediska QoS neměl žádný význam pro provedené simulace.

POUŽITÁ LITERATURA

[1] CAMARILLO, G., GARCÍA-MARTÍN, M. A. *The 3G IP Multimedia Subsystem (IMS)*. England : WILEY, 2006. 427 s. Second edition. ISBN 0-470-01818-6.

[2] CHEN, R. LJ, SU, E. CY, SHEN, V. SC, WANG, Y. *The Introduction to IP Multimedia Subsystem (IMS)* [online]. Dostupné na WWW: <http://www.ibm.com/developerworks/webservices/library/ws-soa-ipmultisub1/>, [cit. 12-10-2009].

[3] POIKSELKA, M., MAYER, G., KHARTABIL, H., NIEMI, A. *The IMS: IP Multimedia Concepts and Services in the Mobile Domain*. England: WILEY, 2004. 448 s. ISBN 0-470-87113-X.

[4] MOLNÁR, K. *Zajištění kvality služeb v bezdrátových a mobilních sítích: skripta*. Brno: FEKT VUT Brno, 2008. 36 s.

[5] ČÍKA, P. *Multimediální služby: skripta.* Brno: FEKT VUT Brno, 2007. 106 s.

[6] KONEČNÝ, Z. *Posouzení vlivu parametrů přístupové sítě UMTS na výkonnost sítě prostřednictvím simulačního prostředí Opnet Modeler*: *Bakalářská práce*. Brno: FEKT VUT Brno, 2009. 79 s.

[7] MÁCHA, T. *Podpora kvalitativních požadavků služeb v prostředí IMS a její realizace na síťové úrovni: Pojednání.* Brno: FEKT VUT Brno, 2010. 30 s.

[8] MOLNÁR, K. *Řízení kvality služeb: skripta*. Brno: FEKT VUT Brno, 2008. 28 s.

[9] MOLNÁR, K. *Bezdrátové síťové technologie: skripta*. Brno: FEKT VUT Brno, 2008. 21 s.

[10] 3GPP. *All-IP Core Network Multimedia Domain*. IP Multimedia (IMS) session handling; IP Multimedia (IM) Call Model; Stage 2. TS 23.218. 3rd Generation Partnership Project 2. July 2005.

[11] 3GPP. *Technical Specification Group Services and System Aspects*. IP Multimedia Subsystem (IMS), Stage 2. TS 23.228. 3rd Generation Partnership Project. March 2010.

[12] 3GPP. *Technical Specification Group Services and System Aspects*. Quality of Service (QoS) Concept and architecture. TS 23.107. 3rd Generation Partnership Project. December 2009.

SEZNAM ZKRATEK

3GPP	3rd Generation Partnership Project
ACK	Acknowledge
ADSL	Asymmetric Digital Subscriber Line
AIFS	Arbitration Interframe Space
APN	Access Point Name
AS	Application Servers
AuC	Authentication Centre
BA	Behaviour Aggregate
BGCF	Breakout Gateway Control Functions
CDMA	Code Division Multiple Access
CN	Core Network
CS	Circuit Switched
CSCF	Call Session Control Function
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DiffServ	Differentiated Services
DCF	Distributed Coordination Function
DIFS	Distributed Coordination Function
DSCP	Interframe Space
EDCA	Ehanced Distributed Channel Access
EDCF	Enhanced DCF
DSCP	DiffServ Code Point
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
I-CSCF	Interrogating - Call Session Control Function
IntServ	Integrated Services
IM-SSF	IP Multimedia Service Switching Function
IMS	IP Multimedia Subsystem
LAN	Local Area Network
MF	Multi-Field Calssification
MGCF	Media Gateway Controller Function
MGW	Media Gateway
MOS	Mean Opinion Score
MRF	Media Resource Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Procesor
MSC	Mobile Switching Centre
OSA-SCS	Open Service Access - Service Capability Server
PCF	Point Coordiantion fiction
P-CSCF	Proxy - Call Session Control Function

PDF	Policy Decision Function
PDP	Packet Data Protocol
PEP	Policy Enforcement Point
PIFS	Point Coordination Function Interframe Space
PSTN	Public Switch Telephone Network
QoS	Quality of Service
RNC	Radio Network Controller
RSVP	Resource reSerVation Protocol
RTCP	Request to Send
RTP	Real-time Transport Control Protocol
RTS	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
S-CSCF	Serving - Call Session Control Function
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SGW	Signaling Gateway
SIFS	Short Interframe Space
SIP	Session Initiation protocol
SIP AS	Session Initiation Protocol Application Server
SLA	Service Level Agreement
SLF	Subscriber Location Function
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
TCA	Traffic Conditioning Agreement
TCP	Transmission Control Protocol
ToS	Type of Service
THIG	Topology Hiding Inter-network Gateway
TXOP	Transmission Oportunity
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol
WCDMA	Wideband Code Division Multiple Access
WFQ	Weighted Fair Queuing
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network