VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

HODNOCENÍ KVALITATIVNÍCH PARAMETRŮ SLUŽEB V DATOVÝCH SÍTÍCH
EVALUATION OF SERVICE QUALITY PARAMETERS IN DATA NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Lukáš Gregor**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Vít Novotný, Ph.D.**
SUPERVISOR

BRNO 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Lukáš Gregor ***ID:*** 160800
Ročník: 3 ***Akademický rok:*** 2015/16

NÁZEV TÉMATU:

Hodnocení kvalitativních parametrů služeb v datových sítích

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s požadavky různých typů datových služeb na vlastnosti síťové infrastruktury a prostudujte moderní techniky podpory kvalitativních požadavků služeb v současných datových sítích na různých úrovních (vrstvách) datové komunikace. S využitím vybavení ústavu navrhněte pro různé typy služeb měření jejich kvalitativních parametrů za různých podmínek provozu v mezilehlé síti. Na základě nabytých zkušeností navrhněte laboratorní úlohu pro předmět Architektura sítí a vypracujte k ní návod.

DOPORUČENÁ LITERATURA:

[1] MARCHESE, M., BARTELL, M. QoS over heterogeneous networks. Chichester: John Wiley, 307 s. Cisco Press networking technology series. ISBN 978-0-470-01752-4, 2007

[2] WANG,Z., BARTELL, M. Internet QoS: architectures and mechanisms for quality of service. San Francisco: Morgan Kaufmann, 2001, xv, 239 s. Cisco Press networking technology series. ISBN 15-586-0608-4

Termín zadání: 1.2.2016 ***Termín odevzdání:*** 1.6.2016

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.
Konzultant bakalářské práce:

doc. Ing. Jiří Mišurec, CSc., *předseda oborové rady*

ABSTRAKT

Bakalářská práce pojednává o problematice QoS v IP sítích. O technologiích pro zajištění kvality služeb, které je nezbytné implementovat v dnešních IP sítích díky velkému nárůstu datových toků. Bakalářská práce je orientována zejména na technologie IntServ, DiffServ, MPLS a požadavky různých typů služeb na kvalitativní parametry datových sítí. V praktické části je úkolem navrhnout laboratorní úlohu pro měření kvalitativních parametrů služeb za různých podmínek v mezilehlé síti. Emulace síťových parametrů probíhá pomocí emulačního nástroje WANem s jádrem GNU Linux.

KLÍČOVÁ SLOVA

QoS, DiffServ, IntServ, kvalita služeb, IP síť, diferencované služby, integrované služby, RSVP, WANem, VoIP, FTP, MOS

ABSTRACT

The bachelor thesis deals about the issues of IP networks. About technologies for ensuring the quality of services, that is necessary to implement in today's IP networks, due to the large increase of data flows. The bachelor thesis is oriented especially on technologies IntServ, DiffServ, MPLS and requirements of different types of services to the qualitative parameters of data networks. The aim of practical part is to devise a laboratory exercise for measuring qualitative parameters of different services under various condition in the intermediate network. Emulation of network parameters is carried out using emulation tool WANem with GNU Linux core.

KEYWORDS

QoS, DiffServ, IntServ, Quality of Services, IP network, diferentiated services, integrated services, RSVP, WANem, VoIP, FTP, MOS

GREGOR, Lukáš *Hodnocení kvalitativních parametrů služeb v datových sítích*: bakalářská práce. BRNO: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2016. 73 s. Vedoucí práce byl doc. Ing. Vít Novotný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Hodnocení kvalitativních parametrů služeb v datových sítích“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

BRNO ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Ing. Vítu Novotnému, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

BRNO ....

podpis autora

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

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

PODĚKOVÁNÍ

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

BRNO ....

podpis autora

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době je velmi důležité, aby se veškerá odesílaná data dostala ve správný čas na správné místo. Současné datové sítě jsou založené na přepínání datových jednotek, na rozdíl od původních sítí založených na přepojování fyzických okruhů. Pro sítě s přepojováním datových jednotek (paketů) je charakteristické sdílení síťových prostředků, čímž lze dosáhnout vysoké efektivity jejich využívání. Sdílení síťových prostředků umožňuje snížit náklady na vytvoření síťové infrastruktury, a tím snížit i cenu služeb. To vedlo k přesunu služeb ze sítí s přepojováním fyzických okruhů do paketových sítí, což způsobilo velký nárůst datových toků přenášených v datových sítích. Bylo tedy nutné ustavit jakýsi kompromis mezi cenou, rychlostí a potřebami jednotlivých služeb, a odeslat zaručeným způsobem data, která jsou klasifikovaná jako důležitější. [18]

Současný datagramový model, na kterém je internet založený, má jen omezené možnosti řízení zdrojů v rámci sítě. Nemůže tedy poskytnout žádné záruky rezervace zdrojů pro uživatele. K doručování paketů používá v základu metodu „best effort“, která nerozlišuje druh jednotlivých paketů, tedy jsou si všechny pakety rovnocenné, a tak obsluhované dle mechanismu FIFO. Internet směruje každý paket nezávisle sítí a jejím úkolem je doručit paket v co nejkratším čase. V praxi to může znamenat, že při pokusu uskutečnit telefonní hovor může být síť natolik zahlcená, že pakety nebudou doručeny včas, a mohou nastat problémy s plynulostí a celkovým zpožděním přenosu hovorových dat. [2]

To lze vyřešit aplikováním technologie zásad QoS (Quality of Services), což znamená rozdělit jednotlivé typy síťového provozu a následně jim přiřadit různé priority a způsob zpracování. O mechanizmech pro zajištění QoS v IP sítích a hodnocení kvalitativních parametrů budou pojednávat následující kapitoly. Závěrečné kapitoly obsahují návrh a realizaci laboratorní úlohy pro měření kvalitativních parametrů různých druhů provozu, za specifických podmínek v mezilehlé síti.

1 KVALITA SLUŽEB ELEKTRONICKÉ KOMUNIKACE – QOS

1.1 O kvalitě služeb elektronické komunikace

Po masivním přesunu služeb ze sítí s přepojováním okruhů do paketových sítí došlo k velkému nárůstu datového toku přenášeného v datových sítích, což bylo nutné řešit. Řešením je aplikace zásad kvality služeb QoS, jejímž úkolem je každé službě zajistit dostatek síťových zdrojů podél její trasy od zdroje k cíli tak, aby byl zaručen bezproblémový chod služby s ohledem na její kritické parametry, jimiž jsou ztrátovost a chybovost paketů, zpoždění, kolísání zpoždění a přenosová rychlost. [19] Jednotlivým paketům je přidělována priorita, podle níž je s nimi zacházeno. Pakety s vyšší prioritou mají přednost před pakety s nižší prioritou.

Interaktivní síťové aplikace jako např. VoIP (Voice over Internet Protocol) či videokonverzace jsou velmi citlivé na zpoždění a proměnlivost zpoždění, které jsou v tomto případě nežádoucí a musí být co nejnižší. Nežádoucí je i ztrátovost paketů, či opětovné odeslání paketu. Ztráta paketů je však do určité míry tolerovaná. Pokud však dojde k překročení míry tolerance, nastává degradace služby, která může vést ke zhoršení kvality hlasu a videa, či k úplné ztrátě spojení účastníků. Aplikace probíhající v reálném čase jsou proto řazeny do třídy s nejvyšší prioritou. [18]

Při implementaci pravidel QoS je nutné respektovat jisté zásady. Jinými zásadami se budeme řídit u firem provozující telefonní služby, kde bude prioritou bezproblémový přenos hlasu, na rozdíl od bankovní společnosti, kde bude prioritou přenos citlivých dat. [2]

1.2 Definice QoS

Z definice společnosti Cisco vyplývá, že QoS je schopnost sítě poskytovat lepší služby uživatelům a vybraným aplikacím na úkor jiných uživatelů a aplikací [3]. Zjednodušeně lze říct, že nástroje QoS uplatníme, budeme-li chtít upřednostnit jeden síťový typ provozu před druhým, nebo zajistit určité aplikaci jasné kvalitativní parametry přenosu. QoS nástroje tedy umožňují řízení jednotlivých datových toků v síti, rovnoměrné dělení zátěže s ohledem na druh přenášených dat a spravedlivé dělení konektivity mezi uživatele podle nastavených parametrů a priorit.

Kvalita služeb by měla být nastavena tak, aby služby nebyly pod hranicí použitelnosti a nedocházelo tedy k přílišné degradaci služby, a zároveň, aby nedocházelo k přílišnému zatížení sítě vlivem rezervace přílišného množství síťových prostředků.

Optimální je najít jakýsi kompromis mezi oběma krajními případy, neboť správné použití služeb QoS vede k vytvoření konzistentní a předvídatelné sítě.

1.3 Transportní protokoly

Pro přenos dat v datových sítích se využívají transportní protokoly TCP, UDP, SCTP v kombinaci s protokoly jiných vrstev, zejména IP protokolem, a pro přenos multimediálních dat protokolem RTP.

1.3.1 TCP protokol

TCP protokol je robustním protokolem transportní vrstvy popsaným v dokumentu RFC 793, pracujícím na bázi modelu klient-server. Jedná se o spolehlivý, spojově orientovaný protokol. Před samotným přenosem musí být navázáno spojení mezi komunikujícími stranami, čemuž se jinak říká „three-way-handshaking“. Spolehlivý proto, že po přijetí paketů přijímačem je potvrzována jejich správnost na základě porovnávání kontrolního součtu nastaveného TCP protokolem před odesláním s kontrolním součtem přijatého paketu. Pokud se nevrátí potvrzení ve stanoveném čase, nebo vůbec, dochází k opětovnému odeslání paketu. Protokol TCP je vhodný pro aplikace u kterých je vyžadováno doručení dat spolehlivě a ve správném pořadí. TCP protokol je využíván pro emailové služby, prohlížení internetu, nebo komunikaci s FTP serverem. [19]

1.3.2 UDP protokol

Protokol UDP je mnohem jednodušší než protokol TCP, který umožňuje řízení toku dat. Nedochází k žádném navazování spojení komunikujících stran, ani k potvrzování doručení. Neexistuje žádná záruka, že pakety dojdou k cíli, nebo že budou doručeny ve správném pořadí. V případě potřeby musí tyto problémy řešit vyšší vrstva. Protokol UDP je proto vhodný pro využití v případech, kdy je preferovaná rychlost doručení, před příjmem dat ve správném pořadí. Jedná se o real-time aplikace jako streamované video, online hry, nebo VoIP.

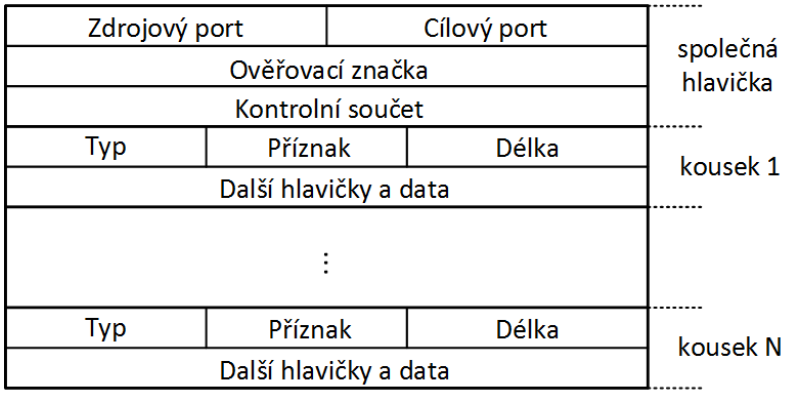
1.3.3 SCTP protokol

Protokol SCTP je stejně jako TCP spolehlivým transportním protokolem, původně navrženým pro přenos telefonních signalizačních zpráv SS7 v IP sítích. Na rozdíl od TCP protokolu umožňuje přenos více uživatelských zpráv v jednom paketu. Po navázání spojení, u SCTP protokolu asociace, tak lze paralelně přenášet řadu dílčích

datových proudů, tzv. streamů v rámci jedné asociace. SCTP garantuje doručení dat ve správném pořadí v rámci každého streamu, proto případný výpadek jednoho z nich nijak neovlivní ostatní proudy. Obdobně jako TCP řeší i SCTP protokol řízení datového toku a problémy se zahlcením sítě. [24]

Protokol SCTP dokáže ohlásit chybějící kusy dat. Pokud vysílač opakovaně dostane zprávy o chybějícím bloku dat, okamžitě chybějící část znovu odešle. SCTP mimo jiné vyniká mechanizmem obrany proti DoS útokům a multihomingem. Klient se musí před asociací prokázat tak zvaným cookie, které mu zaslal server. Při úspěšné autorizaci klienta odesílá server potvrzení a vytvoří asociaci. SCTP monitoruje všechny možné cesty a udržuje informace o jejich stavu. To znamená, že pokud má komunikující uzel více IP adres, je pro komunikaci vybrána jedna jako primární. Pro opakování přenosu je vybrána jiná adresa, pokud je dostupná [24].

SCTP paket je složen ze společné hlavičky, která mimo informací o zdrojovém a cílovém portu, či kontrolním součtu nese také údaje pro ověření totožnosti odesílatele. Následují jednotlivé kousky, zvané chunks, z nichž každý nese řídící informace, nebo data [24].



Obr. 1.1: Struktura SCTP paketu.

2 HODNOCENÍ KVALITATIVNÍCH PARAMETRŮ SÍTÍ

Rozlišujeme dva základní modely pro hodnocení kvality služeb. První QoS model je založený na hodnocení technických parametrů sítě jako takových. Nelze však nijak zjistit, jak moc uspokojila aplikace, pro kterou byly aplikovány zásady QoS, koncového uživatele. Problém hodnocení kvality ze strany uživatele proto řeší disciplína QoE (Quality of Experience).

2.1 Quality of Service

Kvalita přenosu dat je definována řadou parametrů popisujících datový přenos. Parametry jsou dané převážně stupněm vyspělosti síťových prvků. Při implementaci zásad QoS je tedy nutné identifikovat provoz na síti a jeho požadavky, tedy metriky, a rozhodnout, jak s ním bude zacházeno v síti dále. Metriky pro IP sítě jsou převážně spojené se službami běžícími v reálném čase („real-time“). Kvalita sítě je hodnocena podle základních metrik, které charakterizují stav dat přenášených v síti, tedy výkonem, který QoS poskytuje [27].
Mezi základní metriky QoS patří [20]:

- komunikační zpoždění – Delay [m/s],
- kolísání zpoždění – Jitter [ms],
- datová propustnost – Throughput (Bandwidth) [kb/s],
- ztrátovost paketů – Lossrate [%].

Komunikační zpoždění

Komunikační zpoždění vyjadřuje čas, který je potřebný k přenesení paketů od zdroje k cíli. Na cestě od zdroje k cíli mohou být data nejprve převedena z analogové oblasti do digitální oblasti, komprimována, a jednotlivé bity jsou vloženy do větších datových jednotek – paketů. Pakety cestou od zdroje k cíli putují přes několik síťových prvků, kde nějakou chvíli trvá jejich odbavení a odeslání dále se zpozdí ve frontách. Celkové zpoždění je tedy dáno součtem dílčích zpoždění např. serializační, rámcové, paketizační či zpoždění vlivem komprese, nebo kódování dat. [20]

Kolísání zpoždění

Jitter charakterizuje změnu zpoždění přijatých paketů na straně příjemce. Pakety jsou ze strany odesílatele nepřetržitě odesílány v rovnoměrném sledu po sobě. V ideálním případě by bylo kolísání zpoždění nulové. V reálné síti však vlivem zatížení

sítě, zdržením se paketu ve frontě směrovače, či špatné konfigurace může dojít k narušení rovnoměrnosti zpoždění mezi pakety. Výsledkem je, že jsou pakety doručovány v nerovnoměrných intervalech. Pro potlačení kolísání je použita vyrovnávací paměť, která má za úkol vyrovnat proměnlivost příchodu paketů, pozdržet pakety, které přišli dříve, nebo mimo pořadí. [26]

Datová propustnost

Pojem šířka pásma je spojena s analogovým signálem, kde je měřena v Hz. V telekomunikacích se spíše využívá pojem datová propustnost. Avšak v digitálním přenosu dat vyjadřuje objem bitů, které je možné za sekundu přenést přenosovým kanálem. Dnes se využívají její násobky kb/s, Mb/s a Gb/s.

Ztrátovost paketů a chybovost

Pokud je překročena kapacita prvků sítě, pakety došlé k síťovému prvku nemohou být zpracovány a odbaveny. Dochází tak k přetečení front a následnému zahazování paketů, nebo je paket jednoduše směrován jinam. Tomu lze částečně zabránit lepším návrhem sítě. [20]

Je nutné zmínit i bitovou chybovost (BER – Bit Error Rate), která je důležitá především pro digitální přenosy s nepřetržitým datovým tokem a paketovou chybovost (PER – Packet Error Rate). Bitová chybovost vyjadřuje poměr chybně přenesených bitů ku celkovému množství přenesených bitů. Obdobně jako BER vyjadřuje PER podíl chybných paketů ku celkovému počtu odeslaných paketů.
Za chybně přenesený paket je považován paket, který:

- byl zahozen,
- byl směrován jinam,
- obsahoval chyby,
- byl přijat několikanásobně,
- byl přijat jiný paket.

V tabulce 2.1 jsou shrnuty požadavky služeb na QoS dle doporučení. Po překročení stanovených hodnot dochází k degradaci služby.

2.1.1 Třídy provozu

Jak již bylo řečeno, různé aplikace vyžadují odlišné požadavky na zpoždění, ztrátovost paketů, nebo kolísání zpoždění, tak, aby se aplikaci dostalo požadované množství síťových prostředků a nedocházelo k degradaci služby, nebo k úplnému přerušení. Služby s podobnými požadavky jsou proto děleny do čtyřech charakteristických tříd dle 3GPP Release 99.

Tab. 2.1: Tabulka požadavků služeb na QoS. [6]

Typ služby	Přenosová rychlost [kb/s]	Zpoždění [ms]	Ztrátovost [%]
Audio	4 – 26	150 – 400	3
Video	32 – 384	150 – 400	1
FTP	161,599	177,6	0
VoIP	500	150 – 240	0,01
E-mail	301,55	400	0
Web	10	200	0

Přehled QoS tříd provozu [16]:

1. **Konverzační třída**
   Jelikož komunikace probíhá v reálném čase, je konverzační třída velice citlivá na zpoždění a kolísání zpoždění, které jsou nutné zajistit co nejnižší. Proto bývá konverzační třída opatřena nejvyšší prioritou a je typu klient-klient. Typickými aplikacemi je VoIP a videokonverzace.
2. **Třída proudového přenosu dat**
   Třída proudového přenosu dat slouží pro jednosměrnou komunikaci, například budeme-li se chtít připojit k nějakému streamovanému videu a audiu. Jedná se o komunikaci klient-server. Třída je citlivá na zpoždění, ovšem ne tak striktně jako třída konverzační, a kolísání zpoždění.
3. **Interaktivní třída**
   Interaktivní třída slouží pro aplikace, u kterých se upřednostňuje správnost a minimální chybovost doručených dat, před zpožděním. Typicky se jedná o prohlížení webových stránek a přístup k databázím a serverům.
4. **Třída služeb běžících na pozadí**
   Do této třídy se řadí služby s malými požadavky na šířku pásma, které nejsou náročné na zpoždění a kolísání zpoždění. Proto se tyto služby označují nejnižší prioritou a typicky se jedná o stahování e-mailů a databází.

2.2 Quality of Experience

V posledních letech se QoE stalo skutečně aktuálním tématem. Telekomunikační společnosti investují nemalé peníze do výzkumu QoE. Cílem telekomunikačních společností je poznat QoE uživatelů svých služeb a dosáhnout vyváženého poměru mezi kvalitou služby, uživatelskou spokojeností a cenou.

Vyjadřuje subjektivní pocit uživatele s poskytnutou službou. To, jak je uživatel

spokojen s poskytovanou službou z hlediska použitelnosti. QoE je ovlivněno nejen QoS, ale také sociálními faktory. To jak je uživatel spokojen s kvalitou poskytnuté služby závisí mimo QoS parametrů také na jeho předchozích zkušenostech s danou službou. Vliv na výsledné QoE má tedy řada faktorů. Tyto faktory lze rozdělit do tří skupin [11]:

1. Kvalita zvuku/videa na zdroji.
2. QoS, které ovlivňuje přenos obsahu sítí.
3. Lidské vnímání.

Kvalita zvuku/videa závisí například na použitém kodeku, nebo bitové rychlosti. QoS parametry ovlivňující výkon streamovaných služeb nejvíce jsou zpoždění a jeho kolísání, šířka pásma a ztrátovost paketů, které jsou blíže popsané v kapitole 2.1. První dvě kategorie lze snadno kvantifikovat, lidský faktor má však spíše kvalitativní charakter, tudíž je velmi těžké ho nějak standardizovat. Pro vyhodnocování lidského vnímání se užívá stupnice MOS (Mean Opinion Score) [11]. Hodnocení kvality přenosu multimediálních dat pomocí MOS faktoru se řídí doporučeními ITU-T P.800.1, které upřesňují podmínky pro měření kvality. Upřesňují požadavky na přehrávací a nahrávací zařízení, na úroveň šumu v prostředí, kde experiment probíhá, podmínky pro výběr respondentů, nebo parametry přenášených multimédií.

2.2.1 Parametr MOS

Parametr MOS lze rozdělit podle způsobu, jakou metodou je získán. Parametr MOS lze získat metodou: [11]

1. Subjektivní
2. Objektivní
    - Intrusivní
    - Neintrusivní
    - Odhadové

Subjektivní metody staví na hodnocení služby reprezentativním vzorkem uživatelů, kteří službu hodnotí. Jedná se o nejpřesnější, avšak velmi časově a finančně náročnou metodu, využívanou zejména při testování nových kodeků. [27]

Intrusivní objektivní metody jsou založené na odhadu výsledné kvality pomocí matematických algoritmů, bez přítomnosti lidského faktoru. V závislosti na porovnání originálních a přijatých dat, které jsou vlivem přenosu degradovány, se snaží odhadnout, jak by reagoval koncový uživatel. [27]

Neintrusivní metody neporovnávají odeslaný a přijatý datový tok jako metoda intrusivní. Výsledná kvalita je vypočítán na základě analýzy chyb v přijatých datech. [27]

Odhadové metody se snaží odhadovat hodnotu kvality z QoS parametrů, bez znalosti obsahu originálních a přenesených dat. Mnohdy bývají označovány za neintrusivní metody. [27]

2.3 QoS a QoE pro různé druhy provozu

2.3.1 Přenos dat

Pro přenos dat je velmi důležité, aby byla data stažena bez chyb s využitím zbývající šířky pásma. Obvykle se pro přenos dat užívá spolehlivý transportní protokol. Pokud tedy při přenosu dat dojde k chybě, nastává opakovaný přenos chybného segmentu. [19]

2.3.2 Audio streaming

Pro přenos zvuku (hudby, hlasu) jsou přísné požadavky na zpoždění, kolísání zpoždění a ztrátovost paketů, naopak malé požadavky na šířku pásma. S kolísáním zpoždění se vypořádává vyrovnávací paměť na straně příjemce, za cenu zvyšujícího se zpoždění. Při ztrátovosti paketů nad 25 % se služba stává takřka nepoužitelnou. Intenzivní šum bude snižovat srozumitelnost do té míry, že věty bude jen s těží možné pochopit. [19]

2.3.3 Video streaming

Video streaming není tak náročný na zpoždění, které se pohybuje v řádu 4–5 sekund. Příjemce proto může využít větší vyrovnávací paměť, která dokáže odstranit kolísání zpoždění, na kterém je videostreaming závislý. [19]

2.3.4 VoIP

VoIP využívá pro přenos dat transportní protokol UDP. Hlasová informace se přenáší pomocí protokolu RTP (Real-Time Protokol). Přenos signalizačních zpráv je realizovaný pomocí protokolů H.323, SIP, nebo MGCP. Signalizace obsahuje informace o navázání a ukončení spojení, nebo informace o změnách v navázané relaci.

Služba VoIP klade veliké nároky na zpoždění a jitter. Podle normy ITU-T G.114 lze klasifikovat kvalitu hovoru. Pokud je zpoždění nižší než 150 ms je hovor velmi kvalitní. Při zpoždění mezi 150 a 400 ms je kvalita hovoru přijatelná. Pokud přesáhne zpoždění hranici 400 ms, dochází ke špatné slyšitelnosti mezi komunikujícími účastníky, nebo ke ztrátě spojení. [19]

Nežádoucí pro VoIP je i ztrátovost paketů, stejně jako jejich opětovné odesílání. Ztrátovost paketů do 2 % však nijak neovlivní kvalitu hovoru. Důležitý je také použitý kodek a jeho odolnost vůči ztrátám. [19]

Pro hodnocení kvality hlasových služeb jsou standardizovány subjektivní i objektivní metody hodnocení kvality (převzato z [27]):

1. **Subjektivní**
   - Absolute Category Rating (ACR) – Metoda je založena na hodnocení kvality podle MOS stupnice 1–5, za stanovených testovacích podmínek. Hodnotitelem služby je skupina respondentů.
   - Treshold metod (TM) – Metoda je založena na pouhém rozhodnutí respondenta, zda je kvalita jednoho vzorku lepší než druhého.
2. **Objektivní**
   - Intrusivní
     - Perceptual Evaluation of Speech Quality (PESQ) – Metoda je standardizována pro úzkopásmové kodeky (300–3400 Hz) ve standardu ITU-T P.862. Výsledný faktor kvalitativní faktor je vypočítán z rozdílu referenčního a degradovaného signálu.
     - Perceptual Objective Listening Quality Analysis (POLQA) – Metoda standardizována v doporučení ITU-T P.863. Metodika vyhodnocování kvality je založena na principech metody PESQ. Umožňuje však testovat i širokopásmové kodeky.
   - Neintrusivní
     - Single Side Speech Quality Measure (3SQM) – Standardizována v doporučení ITU-T P.563.
     - Passive Voice Quality Analysis (PVQA) – Jedná se o nestandardizovanou metodu. MOS faktor je vyhodnocován z poměru SNR, chyb amplitudy, nebo ozvěn.
   - Odhadové
     - E-model

MOS

Jedná se o škálu hodnot od 1 do 5 vyjadřující lidské vnímání posuzované služby. Pro subjektivní vyhodnocení je potřebný relativně velký reprezentativní vzorek respondentů, kteří hodnotí například kvalitu VoIP hovoru, která se postupně snižuje dle normovaných předpisů pro testování. Respondent na základě spokojenosti ohodnotí službu stupni 5 = excellent; 4 = good; 3 = fair; 2 = poor; 1 = bad. Na stupnici MOS vyjadřuje nejnižší kvalitu stupeň číslo 1, kdy je služba tak znehodnocena, že ji nadále nelze užívat. Naopak nejvyšší kvalitu stupeň číslo 5. Například pro VoIP

hovory je doporučována MOS hodnota 4,4. [27]

Pro objektivní hodnocení kvality služby pomocí intrusivních a neintrusivních metod, je parametr MOS vypočítáván. Využívají se poznatky ze subjektivního hodnocení kvality. Analyzátory se z výpočtů snaží odhadnout, jak by na kvalitu přijatého signálu reagoval člověk. Parametr MOS se podle způsobu vyhodnocování a místa získání dále dělí na poslechový a konverzační. Konverzační MOS zohledňuje konverzaci oběma směry a vzájemnou synchronizaci. Poslechový MOS je vyhodnocován ze strany posluchače. [27]

Tab. 2.2: Druhy parametru MOS.

Metoda	**Poslechový**	**Konverzační**
Intrusivní	MOS_LQS	MOS_CQS
Neintrusivní	MOS_LQO	MOS_CQO
Odhadová	MOS_LQE	MOS_CQE

E-model

Vzhledem k ceně a náročnosti subjektivního testování byl pro potřeby návrhu sítí a posuzování kvality hovoru vytvořen odhadový E-model popsaný v dokumentu ITU-T G.107. Jedná se o odhadovou metodu. E-model poskytuje předpověď kvality hovoru tak, jak by ji vnímal typický uživatel, za stanovených konverzačních podmínek. Výstupem E-modelu je R-faktor. R-faktor se určuje pro celý přenosový systém. Zohledňuje tedy nejen vlastnosti přenosového kanálu, ale také vlastnosti samotných koncových zařízení. Faktor R nabývá hodnot od 0 po 100, přijatelné jsou však pouze hodnoty v intervalu 50–100 [8]. E-model bere v potaz vzájemné působení jednotlivých rušivých vlivů popsaných v rovnici 2.1, jejíž výstupem je R-faktor [22].

$$R = R_0 - I_S - I_D - I_E + A \tag{2.1}$$

kde R_0 vyjadřuje hodnotu odvozenou z vysílaného SNR. I_s je lineární zkreslení, které může nastat přenosem hlasu. Faktor A zohledňuje výhody jednotlivých terminálů (pevný terminál A=0, pohyblivý DECT A=5 a mobilní GSM A=10). I_D vyjadřuje zkreslení vzniklé zpožděním a I_E vliv použitého kodeku [22].

Parametr R-faktor lze přepočítat na parametr MOS dle následujícího vztahu [22]:

$$MOS = \begin{cases} R \leq 6,5 & 1, \\ 6,5 \leq R \leq 100 & 1 - \frac{7}{1000} * R + \frac{7}{6250} * R^2 - \frac{7}{1000000} * R^3, \\ R \geq 100 & 4,5. \end{cases} \tag{2.2}$$

Tab. 2.3: Hodnocení uživatelské spokojenosti se službou [8].

R-faktor	Uživatelská spokojenost	MOS
90–100	Velmi spokojeni	4,34–5
80–89	Spokojeni	4,03–4,33
70–79	Někteří uživatelé nespokojeni	3,60–4,02
60–69	Mnoho uživatelů nespokojeno	3,10–3,59
50-59	Téměř všichni uživatelé nespokojeni	2,58–3,09

2.3.5 Online gaming

Hraní online her vyžaduje nízké a konstantní zpoždění a nízkou úroveň ztrát paketů. Hlavním faktorem je end-to-end zpoždění. Vysoké zpoždění způsobuje špatný požitek ze hry samotnému hráči i ostatním hráčům a na mnohých hracích serverech není vysoké zpoždění tolerováno. Způsobuje takzvané „lagy“. Ideální hodnota zpoždění je do 50 ms.

2.3.6 IPTV

IPTV umožňuje sledování televizního vysílání přes IP protokol s poskytovanou úrovní QoS a QoE. Tato služby bývá operátory často poskytována s dalšími službami v rámci Triplay služeb (data, VoIP a IPTV), kdy se řeší podpora QoS prioritami pro každou službu zvlášť. Nutností je přihlášení se do multicastových skupin, pomocí kterých se IPTV šíří. Pro přihlášení se k multicastové skupině slouží set-top-boxy. Požadavky na QoS jsou mimo jiné závislé na použitých audio a video kodecích, využívajících různou šířku pásma pro přenos. Je tedy nutné vyhradit dostatečnou šířku pásma. Důležitým parametrem je ztrátovost a chybovost paketů, která silně ovlivňuje QoE. K částečnému odstranění chybovosti, vzniklé např. vlivem interferencí na přenosovém médiu, slouží FEC dekodér na Set-top-boxu. Pro dobrý požitek ze služby se doporučuje zpoždění do 200 ms a jitter do 50 ms. [1]

Subjektivní hodnocení

MOS faktor nesouvisí pouze s VoIP, ale používá se také při hodnocení kvality streamovaných videí, nebo IPTV. V souvislosti s IPTV se používá MOS_C vyjadřující dojem z interakce IPTV služeb, MOS_A hodnotící kvalitu zvuku, MOS_V hodnotící kvalitu videa, nebo kombinovaný faktor MOS_AV, který zahrnuje také synchronizaci mezi zařízeními. Využívá se stejná stupnice jako v případě MOS u VoIP technologie. Výsledná hodnota MOS faktoru je dána aritmetickým průměrem. Kvalitu sledovaného obrazu může narušit výpadek snímků, špatná synchronizace obrazu

a zvuku, chyby ve snímcích, nebo šum. [1][12]. Pro snížení přenosové rychlosti se používají kompresní kodeky. Perspektivním kodekem je H.264/MPEG-4 part 10 AVC, který dokáže snížit přenosovou rychlost až o 50 % oproti kodeku MPEG-2 při zachování stejné vizuální kvality. Kodek MPEG-4 AVC bude v průběhu následujících let nahrazován úspornějším kodekem H.265 HEVC.

Stupnice DSCSQ (Double Stimulus Continuous Quality Scale) slouží pro subjektivní hodnocení referenční a testované sekvence, které jsou zobrazovány v krátkých intervalech a pozorovatel neví, která ze sekvencí je testovací a která je referenční. Hodnotí se pomocí stupnice 0–100 se slovním hodnocením kvality (výborná, velmi dobrá, ještě dobrá, špatná a velmi špatná).[12]

Objektivní hodnocení

Pro objektivní hodnocení kvality jsou známe především parametry MSE (Mean Square Error) a PSNR (Paek signal-to-nois ratio), dalšími parametry jsou MDI, MPQM, SSIM a další. Tyto metody se zakládají zejména na matematických výpočtech, které porovnávají surové a komprimované snímky.[12] Pro hodnocení videosekvencí zatím nebyly standardizovány žádné odhadové metody. Objektivní hodnocení je založeno pouze na intrusivních a neintrusivních metodách. [27]

MSE vyjadřuje střední kvadratickou odchylku přijatého video signálu od původního videosignálu.

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{n-1} (x_{ij} - y_{ij})^2 \qquad [-] \quad , \tag{2.3}$$

kde M je počet pixelů na výšku, N počet pixelů na šířku, x je originální obrazec, y je přijatý obrazec a i a j jsou prvky obrazové matice.[12]

PSNR vyjadřuje poměr nejvyšší hodnoty signálu ku MSE.

$$PSNR = 10 \log \frac{m^2}{MSE} \qquad [\mathrm{dB}] \quad , \tag{2.4}$$

kde m je maximální hodnota, které může pixel nabýt. [12]

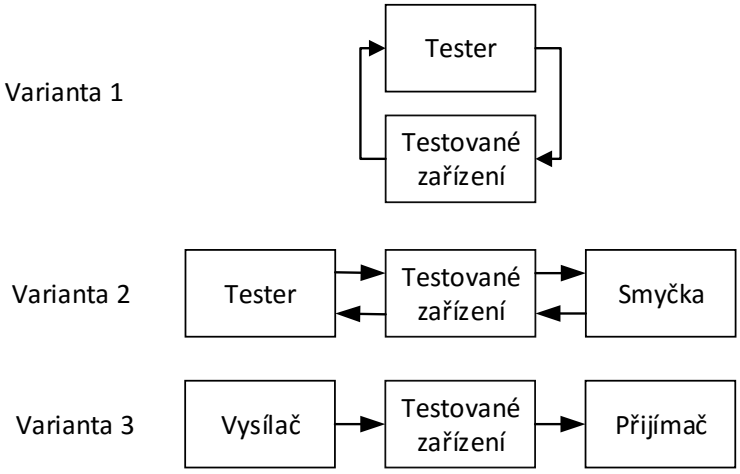
2.4 Testování kvality služeb v datových sítích

Pro testování QoS a QoE parametrů v datových sítích je definována řada testů, z nichž nejznámějšími jsou testy podle standardu RFC 2544 a ITU-T Y.1564.

2.4.1 RFC 2544

RFC 2544 je doporučení vydané společností IETF. Kompletní název dokumentu je „Benchmarking Methodology for Network Interconnect Devices“. Obsahuje soubor testů pro ověření přenosových parametrů síťových prvků, nebo datových okruhů a také způsob reprezentace výsledků testů. Původním záměrem bylo využití RFC 2544 v laboratorních podmínkách. RFC 2544 neobsahuje testy parametrů sledovaných v moderních datových sítích, proto dnes bývá často nahrazen moderními doporučeními, jako Y.1564. Test se provádí pro různé délky rámců. Podle výběru testů a zvolených velikostí testovacích rámců může test RFC 2544 trvat od několika minut až po hodiny. [7] [9]

Test je složen z několika dílčích testů. Těmi jsou test propustnosti, měření zpoždění, měření ztrátovosti rámců, měření zatížitelnosti a test kolísání zpoždění. Test je možné provádět v několika možnostech zapojení, které jsou zobrazeny na obrázku 2.1 níže. [7] [9]



Obr. 2.1: Schémata zapojení pro testy RFC 2544. [9]

Při použití jednoho analyzátoru lze využít dvě možnosti zapojení. Lze použít pouze jeden analyzátor s vysílacím a přijímacím portem (*Varianta 1*) , nebo využít druhý port v režimu smyčky. V režimu smyčky *(Varianta 2*) je datový tok obracen zpět do směru k původnímu zdroji dat. Vysílací port tak zároveň slouží jako přijímací. Jako smyčkovací zařízení lze také použít jiný tester schopný obracet síťový provoz zpět ke zdroji. Poslední možností je využití jednoho zařízení jako vysílače a druhého jako přijímač (*Varianta 3*). Toto zapojení je vhodné pro měření datových okruhů s asymetrickými přenosovými parametry. [9]

Test propustnosti

Ověřuje se maximální rychlost přenosu rámců, při které nedochází ke ztrátě rámců. Test se provádí rámci o velikosti 64 B, 128 B, 256 B, 512 B, 1024 B, 1280 B, 1518 B. Test je zahájen s nejvyšší možnou přenosovou rychlostí. Kontroluje se počet přijatých a odeslaných rámců. Pokud je zjištěna ztráta rámců, nebo chyba, dochází ke snížení rychlosti obvykle o polovinu. Pokud není zjištěna ztráta ani chyba, dochází ke zvýšení rychlosti obvykle o polovinu. Pomocí této iterace se postupně určí propustnost sítě pro různé velikosti rámců zvlášť. [7] [9]

Výsledkem je tabulka a graf znázorňující závislost maximální propustnosti rámců za sekundu (FPS) na velikosti rámců. Je nutné specifikovat formát datového toku a protokol. [7] [9]

Test zpoždění

Při testu zpoždění je nutné rozlišit jednosměrné zpoždění, které je definováno časem, který uplyne od odeslání dat ze zdroje, po přijetí dat v cíli a zpožděním obousměrným nazývaným také RTT (Round-Trip Time). Pro měření se využívá obousměrného zpoždění, které zahrnuje také čas potřebný pro zpracování a znovu odeslání dat zařízením v loop-back módu, které smyčkuje datový provoz. [7] [9]

Test vychází z výsledků měření propustnosti. Je vytvářen datový tok s maximální propustností, při které nedochází k chybám, ani ztrátám rámců. Měření by se mělo provádět po dobu alespoň dvou minut, přičemž po 60 s by měl být do datového toku vložen rámec s časovou značkou svého vysílání, který by měl být detekován na přijímací straně. Rozdílem mezi časem přijetí a časem vyslání je hodnota zpoždění. Pro každou velikost rámce by mělo být měření provedeno 20 krát a výsledné zpoždění by mělo být dáno aritmetickým průměrem těchto dvaceti hodnot. [7] [9]

Test ztrátovosti rámců

Měří se počet ztracených rámců při přenosu v konkrétních podmínkách. Výsledky jsou důležité zejména pro real-time služby, neboť využívají protokolu UDP, který neumožňuje opakování přenosu dat. Test začíná při propustnosti 100 % a porovnává se počet přijatých a odeslaných rámců. Pokud je zjištěna ztráta, sníží se FPS nejčastěji o 10 %, nebo méně, a test je opakován. Tato iterace pokračuje až do doby, kdy je ztráta rámců rovna 0. Výsledkem je graf závislosti ztrátovosti rámců v procentech na přenosové rychlosti v procentech. [7] [9]

Test zatížitelnosti

Cílem měření zatížitelnosti síťových prvků je určit schopnost síťových prvků zpracovávat rámce odesílané kontinuálně s minimální mezirámcovou mezerou. Ověřují se možnosti vyrovnávacích pamětí prvků.

Test začíná vysláním skupiny rámců s minimální mezirámcovou mezerou. Pokud je počet odeslaných a přijatých rámců shodný, dojde ke zvýšení počtu rámců v sekvenci. Pokud se počet vyslaných a přijatých rámců nerovná, dojde ke snížení počtu rámců v sekvenci. Výsledkem je maximální počet rámců v sekvenci, při kterém nedochází ke ztrátám rámců. Nejkratší povolená sekvence rámců by měla být alespoň 2 s. Pro různé velikosti rámců by mělo být měření opakováno alespoň 50 krát. Výstupem testu je tabulka s průměrným počtem rámců pro všechny velikosti rámců. [7] [9]

Test zotavení po přetížení

Test slouží pro zjištění doby mezi tím, kdy zařízení nepřeposílá rámce v případě přetížení a následnou obnovou normálního stavu. Je vysílán datový tok s vyšší propustností, než je změřena maximální propustnost v testu propustnosti, a následně je rychlost snížena na polovinu. Od této doby nastává měření času od snížení rychlosti o 50 % po dobu , kdy je ztrátovost rámců nulová. Test je několikrát opakován pro všechny velikosti rámců a výsledný čas je dán aritmetickým průměrem. [7] [9]

Test zotavení po restartu

Test je prováděn pouze pro rámce s velikostí 64 B. Cílem je stanovit dobu mezi posledním a prvním přeneseným rámcem po restartu zařízení. [7] [9]

2.4.2 ITU-T Y.1564

Název dokumentu je „Ethernet service activation test methodology“. Řeší nedostatky testu RFC 2544, které vznikly s příchodem nových služeb a technologií. Zatímco test RFC 2544 se zabýval zejména testem síťových prvků, Y.1564 se zabývá obecným ověřením parametrů datových toků různých služeb a možnost testu paralelních datových toků. Definuje způsob posuzování parametrů přenosu služeb využívající technologii ethernet. Doporučení upravuje vztah mezi poskytovatelem připojení a zákazníkem, tzv. smlouvu o garantované úrovni služeb SLA a podmínky přenosu. Zejména kvalitativní parametry přenosu, které jsou posuzovány pomocí QoS parametrů. Test se skládá ze dvou fází. [9]

Kontrola nastavení síťové konfigurace

Kontrolují se parametry SLA a jejich správnost. Po stupních je zvyšována přenosová rychlost, kdy každý krok trvá 1–10 s. V jednotlivých krocích jsou kontrolovány parametry SLA. Jsou definovány hodnoty CIR a EIR, které určují 3 pásma. V **garantovaném pásmu** jsou data vždy přenášena v souladu s SLA, v **Best Effort pásmu** nemusí být dodrženy parametry SLA. Data jsou přenášeny pouze tehdy, když je volná kapacita. V **Dropped pásmu** nejsou data přenášena nikdy. [9]

Kontrola QoS parametrů

V druhé fázi jsou různé služby generovány paralelně a nahlíží se na ně jako na jeden datový tok, pro přiblížení běžnému provozu. Kontrola má za úkol ověřit prioritizaci vybraných datových toků přenášených paralelně, což v testu RFC 2544 zcela chybělo. Tento test je důležitý zejména pro Triple play služby, které jsou dnes hojně poskytovány různými společnostmi na celém světě.[9]

2.4.3 Test bitové chybovosti

Test bitové chybovosti je poskytován na linkové, fyzické a síťové vrstvě. Bitová chybovost vyjadřuje poměr chybně přijatých bitů ku celkovému počtu přijatých bitů. V případě technologie ethernet by BER měla být v intervalu od 10^{-15} do 10^{-12}. Rámec lze vyplnit pseudonáhodnou bitovou sekvencí, nebo standardizovanými sekvencemi. [9]

3 MECHANIZMY PRO ZAJIŠTĚNÍ QOS V IP SÍTÍCH

V současných IP sítích rozlišujeme různé úrovně QoS, tudíž existují i jejich modely a nástroje, pomocí nichž je dosaženo daných úrovní. Dále budou definovány a popsány modely pracující na síťově vrstvě IP sítí, kterými jsou:

- Best Effort,
- Integrované služby – IntServ,
- Diferencované služby – DiffServ,
- Multiprotokolové přepínání podle návěští – MPLS.

3.1 Best Effort

V sítích s využitím mechanizmu Best-Effort jsou data aplikací odesílána bez politiky. Síťové prvky se snaží doručit data co nejrychleji k cíli, ale bez jakýchkoli garancí. Jak tedy z názvu vyplývá, snaží se data doručit s největším úsilím. Všechna data jsou si rovná a nelze zvýhodnit jednu službu před druhou, protože nedochází k jejich rozlišování.

Na principu Best Effort byl původně vybudován internet a dodnes na něm funguje jeho velká část. V praxi se od ní čím dál tím více upouští, protože díky tomu, že není schopna garance, může některý „agresivní“ datový tok zcela vyčerpat veškerou kapacitu sítě, nebo síťových prvků a sám zahltit síť. Na jiné aplikace tedy nezbydou prostředky a nejsou vykonány. Proto je nutné přistoupit k sofistikovanějším mechanizmům QoS.

3.2 Integrované služby – IntServ

Architektura integrovaných služeb je prvním modelem, který měl zajistit v IP sítích požadavky na QoS. Tento model byl definován již v roce 1994 v dokumentu RFC1633 a pracuje převážně na 3. vrstvě referenčního modelu ISO/OSI. Principem architektury Intserv je rezervace zdrojů podél celé cesty od zdroje k cíli, tzv. „per-flow“. Aplikaci je zajištěna potřebná kvalita přenosového kanálu, ještě před samotným přenosem paketů. Tento proces je poněkud zdlouhavý, protože se směrovače a přepínače musí shodnout na úrovni poskytnutí služby. O rezervaci zdrojů se starají rezervační protokoly jako RSVP, COPS, nebo YESSIR. Mechanizmus integrovaných služeb rozlišuje kategorie aplikací na [14]:

- **Pružné aplikace** – bez požadavků na doručení. Aplikace nekladou požadavky na kapacitu spojení nebo zpoždění. Jedná se o aplikace využívající ke komunikaci TCP protokol, jako např. HTTP, elektronická pošta, atd.
- **Real Time Tolerant (RTT) aplikace** – citlivé na maximální zpoždění v síti. Aplikace je schopna vypořádat se s občasnými ztrátami paketů. Typickým příkladem je video aplikace využívající vyrovnávací paměti, která vyrovnává ztrátu paketů. Jedná se o aplikace pracující nad protokolem UDP.
- **Real Time Intolerant (RTI) aplikace** – přísně vyžaduje minimální zpoždění, jitter a ztrátovost paketů. Opět se jedná o aplikace pracující nad UDP protokolem, např. videokonference.

K zajištění obsluhy těchto aplikací používá IntServ třídy služeb nazývané jako CoS – Class of Services [14]:

- **Služba s řízenou zátěží** – Je určena pro RTT aplikace. Služba zaručuje průměrné zpoždění. Zpoždění jednoho paketu mezi koncovými uzly není deterministické.
- **Garantovaná služba** – Určena pro RTI aplikace, jako jsou interaktivní aplikace a aplikace v reálném čase. Garantovaná služba zaručuje deterministickou horní hranici zpoždění a šířku pásma. Aplikace tedy mohou snížit zpoždění zvýšením požadavku na šířku pásma.
- **Best Effort**

3.2.1 Referenční model IntServ

Referenční model IntServ architektury zahrnuje 4 základní části [26]:

- rezervační protokol,
- řízení přístupu (Admission Control),
- klasifikátor paketů (Flow Identification),
- plánovač paketů (Packet Scheduling).

Rezervační protokol

Pro nastavení rezervace prostředků potřebujeme rezervační protokol, který krok po kroku postupuje komunikačním kanálem a nastavuje rezervační stav na směrovačích. Rezervační protokol nese také informace o charakteru provozu a požadavcích na zdroje, takže v každém uzlu podél cesty může být rozhodnuto, zda bude nový požadavek na rezervaci přijat. Cesta musí být definovaná ještě před zahájením rezervace. Rezervační protokol musí být schopen vypořádat se se změnami v topologii sítě. Například pokud v nějakém místě podél komunikační cesty dojde k přerušení

linky, rezervační protokol musí zařídit novou rezervaci a zrušit starou rezervaci. Nejznámějším rezervačním protokolem je RSVP [26].

Řízení přístupu

Aby bylo možné garantování prostředků pro vyhrazený datový tok, musí síť neustále monitorovat využívání zdrojů. Síť může zamítnout žádost o rezervaci, pokud nemá k dispozici dostatečné množství prostředků. Pokud je žádost zamítnuta, aplikace rozhodne, zda požádá o rezervaci s nižšími nároky na prostředky sítě. Řízení přístupu má dvě funkce. První funkcí je rozhodnout, zda bude nastavena rezervace na základě pravidel pro řízení zátěže. Druhou funkcí je sledování a měření dostupných prostředků [26].

Klasifikátor paketů

Při zpracovávání paketů musí směrovač prozkoumat každý příchozí paket a následně rozhoduje, zda paket patří k nějakému z rezervovaných RSVP toků. Pakety jsou identifikovány na základě pěti polí v hlavičce paketu: zdrojová IP adresa, cílová IP adresa a protokol ID, zdrojový port a cílový port. Tato pětice je následně porovnávána s hodnotami ve stejných polích všech toků v rezervační tabulce. Pokud je zjištěna shoda, je vyvolán korespondující rezervační stav z rezervační tabulky a paket je poslán spolu s rezervačním stavem spojeným s hledaným tokem do plánovače paketů [26].

Plánovač odesílání paketů

Plánovač paketů je implementován ve směrovačích, kde jsou pakety řazeny do front. Řídí odesílání paketů podle tříd, do kterých klasifikátor zařadil jednotlivé pakety a je posledním krokem rezervace zdrojů. Jeho hlavním úkolem je vybrat pakety k odeslání z výstupních portů, pokud je odchozí spojení připraveno.

3.2.2 RSVP (Resource reSerVation Protocol

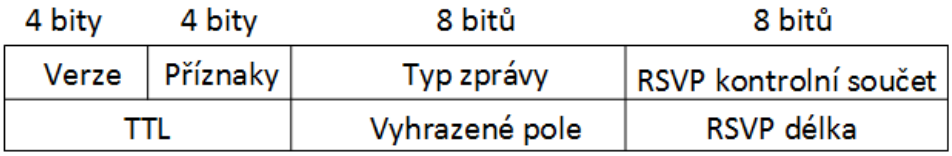
Mechanizmus integrovaných služeb vyžaduje rezervaci síťových zdrojů ještě před začátkem přenosu dat. To vedlo organizaci IETF k vytvoření protokolu RSVP, který tyto požadavky splňuje. RSVP využívají koncové stanice pro zasílání požadavků na služby do sítě a směrovače pro zřízení rezervace podél cesty mezi odesílatelem a příjemcem výhradně v jednom směru.

RSVP je protokol orientovaný na příjemce. Příjemce tedy rozhoduje, jaké prostředky budou vyhrazeny, a je zodpovědný za inicializaci. Žádost putuje od příjemce k odesílateli a vytváří rezervační strom [26].

Protokol RSVP definuje základní typy zpráv, jako jsou PATH, RESV, PATHErr, RESVErr, PATHTear, RESVTear a RESVConf. Nejvýznamnějšími však jsou PATH a RESV.

Formát RSVP zprávy

Každá RSVP zpráva začíná hlavičkou, po které následují data složená z různě dlouhých RSVP objektů. Formát hlavičky je uveden na obrázku 3.1 [26].



Obr. 3.1: Formát RSVP zprávy.

RSVP kontrolní součet je podobný jako kontrolní součet v IP, UDP a TCP. Vyhrazené pole a pole příznaků nejsou definovány. Pole TTL zaznamenává hodnotu time-to-live využívanou odesílatelem IP hlavičky. RSVP délka je celková délka zprávy zahrnující proměnnou délku objektů, které následují. [26]

RSVP objekty

Pro ustanovení QoS parametrů slouží v rámci RSVP spojení RSVP objekty. RSVP protokole definuje celou řadu těchto objektů. Pomocí objektů v RSVP zprávách, které si mezi sebou zasílají odesílatel a příjemce, se odesílatel a příjemce dohodnou na typu požadované rezervace, nebo kvalitě [23]. Základními RSVP objekty jsou [26]:

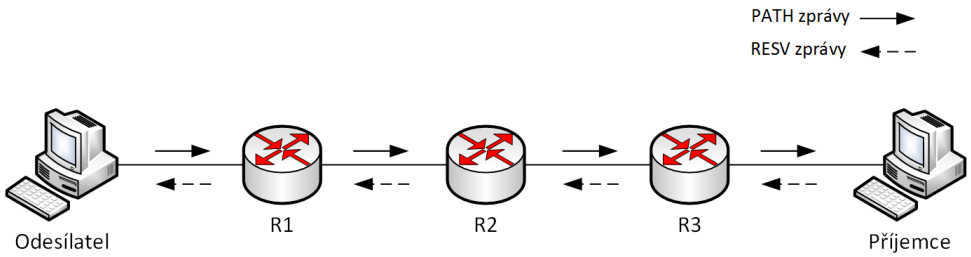
TSPEC – specifikace charakteristiky datového toku.
SENDER_TSPEC – specifikace datového toku generované příjemcem. (PATH)[1]
RECIEVER_TSPEC – popis toku, pro který má být provedena rezervace. (RESV)
FLOWSPEC – definuje specifikaci provozu a rezervační žádost. (RESV)
FILTER_SPEC – filtr paketů QoS. (RESV)
TIME_VALUE – doba po které se obnoví RESV a PATH zprávy. (PATH, RESV)
RESV_CONF – zápis adresy na kterou se budou zasílat rezervační potvrzení. (RESV)
RSVP_HOP – data o síťových uzlech v cestě. (PATH, RESV)
SCOPE – předcházení smyčkám. (RESV)
SESSION – informace o cestě spojení a cílové adrese. (PATH, RESV)

[1] V závorkách je uvedeno, zda mohou daný objekt využít RESV zprávy, nebo PATH zprávy.

SENDER_TEMPLATE – identifikuje odesílatele. (PATH)
HOP – nese IP adresu síťového uzlu v cestě (PATH, RESV)

Činnost RSVP protokolu

Odesílatel pošle PATH zprávu k příjemci, které nese rezervační informace. Zprávy PATH distribuují informace o zdroji provozu a nastavují potřebný stav pro RESV zprávy. Do PATH zprávy je tedy zapisována cesta mezi zdrojem a příjemcem dat. Po obdržení PATH zprávy vygeneruje přijímač RESV zprávu a pošle ji k odesílateli. Zprávou RESV přijímač žádá přidělení síťových prostředků.



Obr. 3.2: Činnost RSVP protokolu.

3.3 Diferencované služby – DiffServ

Modely best effort a integrovaných služby představují dva extrémní případy napříč spektrem rezervace prostředků. Zatímco best effort se vypořádává nezávisle s každým paketem, mechanizmus IntServ se zabývá jednotlivými datovými toky. Mechanizmus DiffServ lze zařadit někde mezi tyto dva extrémy. Byl vyvinut jako reakce na potřebu vzniku modelu, který by poskytl různé úrovně služeb internetovému provozu, podporoval různé typy aplikací a vyhověl specifickým požadavkům aplikací [26].

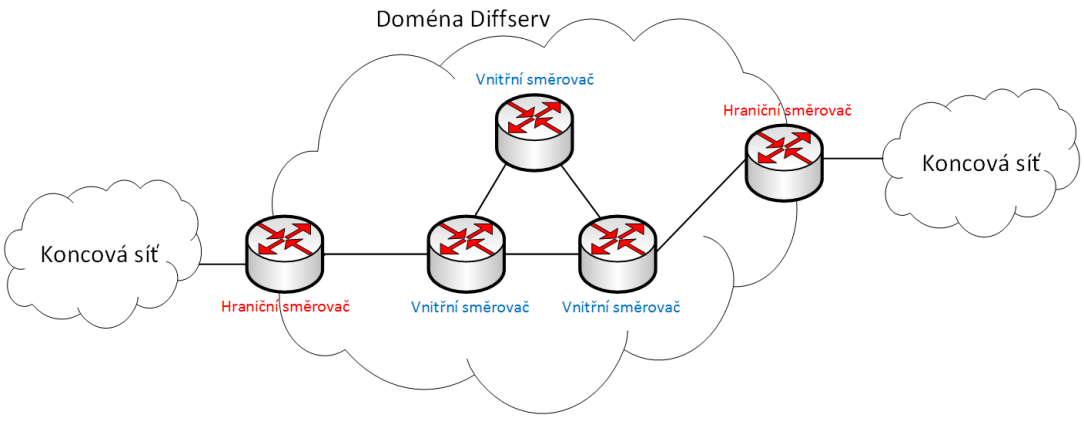
Na okrajových směrovačích probíhá klasifikace datového toku a přidělování síťových prostředků na základě příslušnosti datového toku k třídě, která je definována v poli DSCP. Na rozdíl od mechanizmu integrovaných služeb mechanizmus DiffServ nevyžaduje žádnou rezervaci prostředků podél celé cesty, paket je označen v okrajovém směrovači a dále už je v síti identifikován a směrován podle třídy datového toku v DSCP poli v hlavičce paketu. Směrovače tedy nemusí udržovat informace o tocích a rezervovaných prostředcích. Díky tomu nedochází k vysokému zatěžování sítě. Způsob přidělování síťových prostředků závisí na každém směrovači v cestě.

3.3.1 DiffServ doména

V rámci mechanizmu Diffserv je síť dělena do menších oblastí s vlastními pravidly, takzvaných DiffServ domén, které jsou složeny z více síťových prvků. Směrovače v rámci jedné Diffserv domény dělíme na vnitřní směrovače, které pouze směrují pakety na základě značky, kterou jim přidělí hraniční směrovače, a směrovače hraniční. Hraniční směrovače se nachází na vstupech do DiffServ domény. [2]

V praxi může dojít ke dvou případům. Za prvé mohou k hraničnímu směrovači přijít ještě neoznačené pakety, které jsou následně v hraničním směrovači klasifikovány a označeny. V druhém případě mohou k hraničnímu směrovači přijít již označkované pakety z jiné DiffServ domény. Pak záleží na pravidlech jednotlivých DiffServ domén. Pokud jsou pravidla podobná a mají stejný identifikátor, není třeba nic měnit. V případě stejných pravidel, ale odlišných identifikátorech stačí pouze aktualizovat identifikátor. Může však nastat případ, že v obou doménách budou zcela odlišná pravidla. Potom je tedy nutné kompletní znovuzpracování a přidělení identifikátoru, dle pravidel DiffServ domény, do které paket vstupuje. [2]

Na obrázku 3.3 je zobrazena jednoduchá architektura DiffServ domény s hraničními směrovači pro značkování paketů a s vnitřínimi směrovači sloužícími pro předávání si paketů od zdroje k cíli.



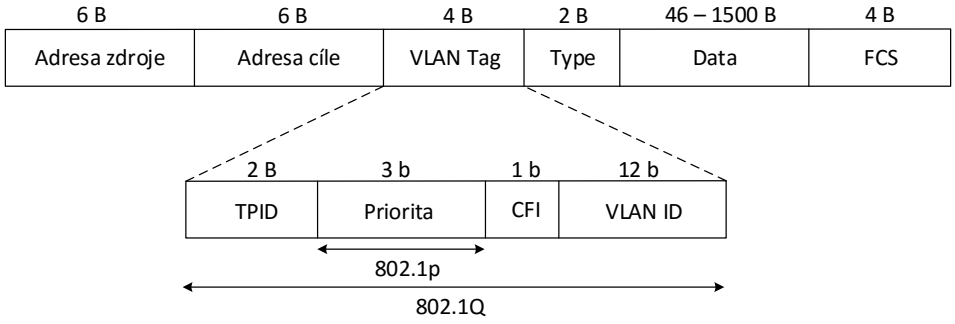
Obr. 3.3: Doména DiffServ.

3.3.2 Klasifikace rámců na linkové vrstvě

Klasifikace datového provozu je možná už na linkové vrstvě, kde je možné klasifikovat rámce. Nutnou podmínkou je existence mapování mezi síťovou a linkovou vrstvou.

Pro přenos rámců mezi přepínači se využívá *trunk*. Standartd IEEE 802.1Q definuje, rozšíření hlavičky původního rámce o tzv. *frame tagging*, kdy je originální

rámec rozšířen o 4bajtový VLAN tag. Tag definuje příslušnost jednotlivých rámců k VLAN a obsahuje mimo jiné i informace o prioritě přenášených dat dle standardu 802.1p viz obrázek 3.4 [15].



Obr. 3.4: Struktura pole VLAN Tag ethernetového rámce.

Pole **TPID** (Tag Protocol Identifier) nese identifikátor značky, pro IEEE 802.1Q má hodnotu 0x8100. **CFI** (Cannonical Format Indicator) obsahuje informaci, zda jsou adresy v rámci v kanonické formě. V poli **VLAN ID** je jednoznačně zapsané, do které VLAN rámec patří. Maximální počet VLAN je teoreticky 4096 (2^{12}), prakticky je to však 4094 VLAN, neboť 0 a 4095 jsou rezervovány [15]. Pole **Priorita** indikuje hodnotu CoS rámce. Pomocí 3 bitů lze zakódovat až 8 prioritních úrovní viz tabulka 3.1.

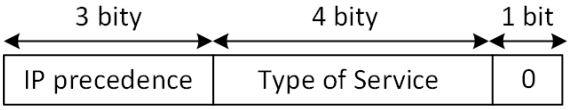
Tab. 3.1: Priority dat na linkové vrstvě dle IEEE 802.1p.

Priorita	Klasifikace služeb
0	služba typu Best Effort (BE)
1	rezervovaná, horší služba než typu BE
2–3	rezervovaná
4	data citlivá na zpoždění, bez záruky
5	data citlivá na zpoždění, do 100 ms
6	data citlivá na zpoždění, do 10 ms
7	řízení sítě

3.3.3 Klasifikace paketů na síťové vrstvě

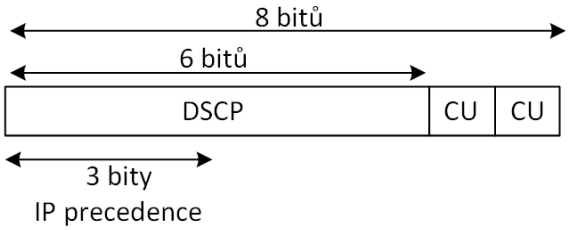
DSCP (Diferentiated Services Code Point)

Pojmem DSCP je nazýváno prvních 6 nejvýznamnějších bitů z DiffServ pole v hlavičce IP datagramu. Pole DiffServ se nachází v jednobajtovém ToS poli v hlavičce IPv4 paketu. Pro IPv6 paket je pole ToS nazýváno CoS (Class of service). Poslední dva bity CU (Currently Unused) v DiffServ mohou být využity koncovými uzly pro oznámení o přetížení sítě ECN (Explicit Congestion Notification), jinak jsou nevyužity. V DiffServ sítích klasifikují a značkují pakety hraniční směrovače buď podle hodnoty IP precedence, nebo podle hodnoty DSCP [10]. Dříve se využívaly převážně 3 bity IP precedence, dnes se však využívá 6bitové pole DSCP, jehož první 3 bity jsou plně kompatibilní s IP precedence [4]. Další tři bity jsou nazvané Class Selector (CS) [16]. Soudě dle typu aplikace může pole DSCP nabývat hodnot 0–63.



Obr. 3.5: Pole ToS IPv4 paketu.

V prvních třech bitech je aplikací či směrovačem zapsaná hodnota IP precedence, která slouží k určení priority jednotlivých dat. Hodnota v následujících 3 bitech nazývaných jako ToS (Type of Service) určuje zpoždění, propustnost a spolehlivost. Poslední bit je vždy 0.



Obr. 3.6: DiffServ pole.

Výchozí hodnotou DSCP pole je 000 000. DSCP využívá pro nastavení priority první tři bity stejně tak jako IP precendence viz obrázek 3.6. Mimo těchto třech bitů využívá DSCP ještě následující tři bity, což umožňuje rozdělit služby až do 64 tříd [4].

Tab. 3.2: Tabulka DSCP hodnot v porovnání s hodnotami IP Precedence. [16]

Třída	DSCP	Hodnota DSCP	IP Precedence
BE	000000	0	0
CS1	001000	8	1
AF11	001010	10	1
AF12	001100	12	1
AF13	001110	14	1
CS2	010000	16	2
AF21	010010	18	2
AF22	010100	20	2
AF23	010110	22	2
CS3	011000	24	3
AF31	011010	26	3
AF32	011100	28	3
AF33	011110	30	3
CS4	100000	32	4
AF41	100010	34	4
AF42	100100	36	4
AF43	100110	38	4
EF	101110	46	5

AF – Zaručené předávání (Assured Forwarding

AF zaručuje svým 4 podtřídám určitou šířku pásma, popřípadě možnost přístupu k větší šířce pásma, pokud je k dispozici. Mimo to jsou pro každou podtřídu definované 3 úrovně pravděpodobnosti zahození paketů [16].

EF – Urychlené předávání (Expedited Forwarding

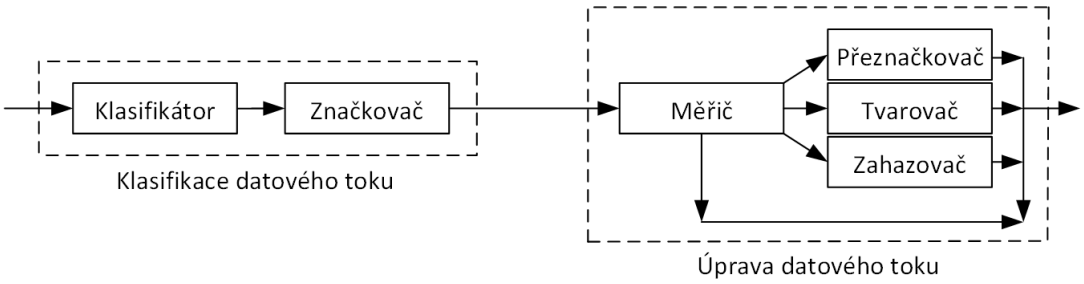
EF umožňuje přeposílání paketů bez bufferů, což zaručuje nejnižší zpoždění, ztrátu a jiter. Pakety této třídy jsou zahazovány s nejnižší pravděpodobností. EF bývá také nazývána jako prémiová služba. [16]

BE – Best Effort

Jedná se o službu bez záruky, která nedefinuje žádnou úroveň kvality služeb.

3.3.4 Referenční model DiffServ

Referenční model model DiffServ se skládá z několika funkčních bloků a pracuje ve dvou fázích viz Obr. 2.6. V první fázi dochází ke klasifikaci datového toku, v druhé fázi pak k samotné úpravě datového toku [26].



Obr. 3.7: Blokové schéma referenčního modelu DiffServ.

Klasifikátor (Classifier)

Klasifikátor rozděluje příchozí pakety podle předdefinovaných pravidel do různých tříd. Rozlišujeme dva způsoby klasifikace. Prvním způsobem je rozdělování paketů na základě hodnoty zapsané v DSCP poli hlavičky paketu, nazývané jako BA (Behavior Aggregate). Tento způsob se používá v případě, že byla hodnota v DSCP poli nastavena ještě před tím, než pakety přišly ke klasifikátoru. Druhým způsobem je MF (MultiField), který třídí pakety na základě jednoho, nebo více polí z hlavičky paketu, kterými jsou například zdrojová adresa, cílová adresa, zdrojový nebo cílový port, či ID protokolu [26].

Značkovač paketů (Marker)

Značkovač přiřadí paket k příslušné třídě (BE, AF, EF, CS), tak, že nastaví v DiffServ poli příslušnou hodnotu DSCP. Značkování může probíhat v okrajových směrovačích pracujících na síťové vrstvě, nebo mohou být pakety již označkovány aplikací. Další funkcí značkovače je přeznačkování již označkovaných paketů, které přišly například z jiné DiffServ domény, pokud je to vyžadováno odlišnou politikou obou domén. [26]

Měřič (Meter)

Úkolem datového toku je měření vlastností paketů vybraných klasifikátorem a následné porovnání s uloženým datovým profilem. Při shodě s profilem je datový tok vpuštěn do sítě. V opačném případě jsou data zahozena, přeznačena, nebo upravena v tvarovači síťového provozu. [26]

Zahazovač (Dropper)

Pokud se pakety neshodují se síťovým profilem, mohou být zahozeny. Důvodem může být vyčerpání kapacity fronty, nebo překročení objemu přicházejících dat. [26]

Tvarovač (Shapper)

Úkolem tvarovače je zpožďování paketů, tak aby šířka přenosového pásma korespondovala s požadovaným síťovým profilem provozu. Jinak řečeno upřednostňuje pakety, které splňují parametry síťového profilu před nevyhovujícími pakety, které zpozdí. Pro tvarování síťového provozu využívá metody „token bucket“. [26]

3.3.5 Ochrana před zahlcením front – CA (Congestion Avoidance)

Účelem ochrany před zahlcením front je včasné zabránění úplnému zahlcení front síťových prvků. Tím lze předejít kolapsu prvku, v krajním případě celé sítě [17]. Rozlišujeme několik způsobů ochrany před zahlcením:

A) PASIVNÍ SPRÁVA FRONT
- Tail Dropping.

B) AKTIVNÍ SPRÁVA FRONT
- Random Early Detection – RED.
- Weighted Random Early Detection – WRED.
- Explicit Congestion Notification – ECN.

Tail Dropping

Jedná se o jednoduchou, starší, pasivní správu front se špatným vlivem na TCP provoz. Metoda spočívá v zahazování paketů, pro které již není místo ve frontách kvůli jejich úplnému zaplnění, což znamená dočasné zastavení zpracovávání paketů do té doby, než se fronty uvolní. Pro pakety nesoucí TCP segmenty je zde riziko TCP synchronizace a s ní spojeným snížením využití přenosové kapacity [17].

RED

Předčasná detekce s náhodnou reakcí spočívá v monitorování stavu front. V případě, že je vyhodnoceno, že by mohla být fronta brzy zaplněna, dojde k náhodnému zahazování paketů ve frontě, které postupně sníží intenzitu některého z navázaných TCP spojení. Metoda RED je plně kompatibilní s metodou potvrzování doručení TCP segmentů. Případné zahození paketu je tedy směrovačem signalizováno vysílači [17].

Pro UDP datagramy pozbývá metoda včasného varování zcela smysl, protože nijak neovlivní rychlost odesílání paketů.

WRED

Předčasná detekce s váženou náhodnou reakcí je pouhou modifikací metody RED. Doplňuje ji o možnost přiřazení profilů k jednotlivým frontám. V rámci jedné fronty může být přiděleno více profilů, čemuž se říká barvení paketů. V praxi to znamená možnost zahození méně důležitých paketů při určité úrovni zaplnění fronty. [2]

ECN

Pro explicitní signalizaci zahlcení mohou být využity poslední dva bity CU pole DS, které jsou jinak nevyužity. Nedochází tak k zahazování paketů, ale k jejich označení a odeslání k cíli, který upozorní zdroj, aby snížil rychlost vysílání paketů, což vede k předcházení zahlcení. [10]

3.3.6 Řízení odesílání paketů

Úkolem řízení odesílání paketů je monitorování dostupných síťových prostředků, zejména šířky pásma, tak aby nedošlo k zahlcení sítě. Pakety jsou ve směrovačích rozděleny do front podle hodnoty zapsané v hlavičce paketu, kterou jim přiřadil klasifikátor, což umožňuje různé zacházení s pakety v dané frontě při odesílání dále do sítě. Jak konkrétně budou fronty obsluhovány definují různé metody řízení odesílání paketů, které se liší metodou obsluhy svých front. Mezi základní metody řízení odesílání paketů patří: [17]

- fronta s obsluhou FIFO (First In First Out),
- fronta s prioritní obsluou – PQ (Priority Queuing),
- fronta se spravedlivou obsluhou – FQ (Fair Queuing),
- fronta s váženou cyklickou obsluhou – WRR (Weighted Round Robin),
- fronta s váženou spravedlivou obsluhou – WFQ (Weighted Fair Queuing),
- fronta s váženou spravedlivou obsluhou řízenou dle tříd – CBWFQ (Class Based Weighted Fair Queuing).

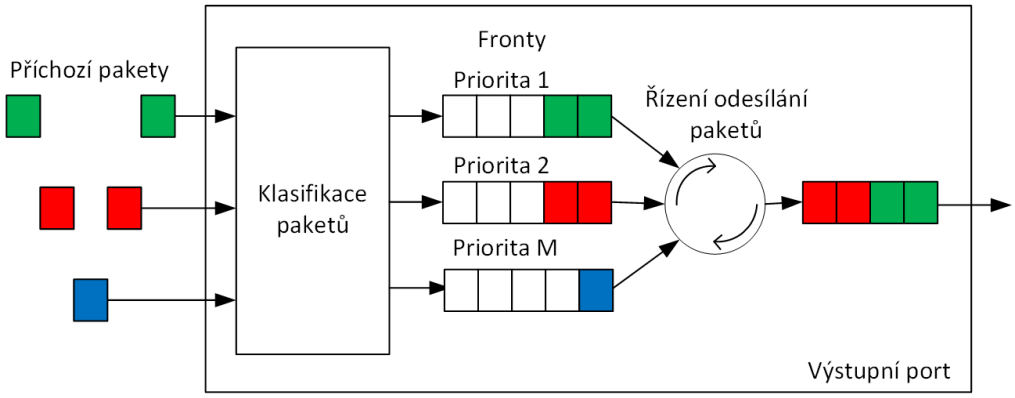
FIFO

FIFO je nejjednodušší a zároveň nejstarším algoritmem pro řízení odesílání. Příchozí pakety jsou jednoduše řazeny do jediné fronty podle pořadí, v jakém přišly. V tomto pořadí jsou i odesílány. Výhodou metody FIFO je její snadná implementace [13]. Všem paketům je zajištěno stejné zacházení a tak FIFO nejvíce vyhovuje technologii best effort. Problém však nastává při zahlcení sítě. Jelikož FIFO nerozlišuje žádné

třídy služeb, tak zahlcení sítě ovlivní všechny pakety stejně, bez ohledu na to, jaká data nesou.

Priority Queuing – PQ

PQ je velmi jednoduchým algoritmem, s jednoduchou implementací. Princip spočívá v tom, že každé frontě je přidělena priorita. Fronta s nejvyšší prioritou má absolutní přednost před ostatními frontami. Z fronty s nižší prioritou lze odeslat paket až poté, co je fronta s vyšší prioritou zcela prázdná. Nevýhodou PQ je nebezpečí nadměrného zdržení paketů ve frontě s nízkou prioritou při vysokém datovém provozu. Pakty ve frontě z nižší prioritou mohou být v případě TCP provozu považovány za ztracené a dojde k jejich znovu odeslání. Výhodné je využití PQ v případě, že data s vysokou prioritou tvoří pouze nepatrnou část celkového síťového provozu [17].



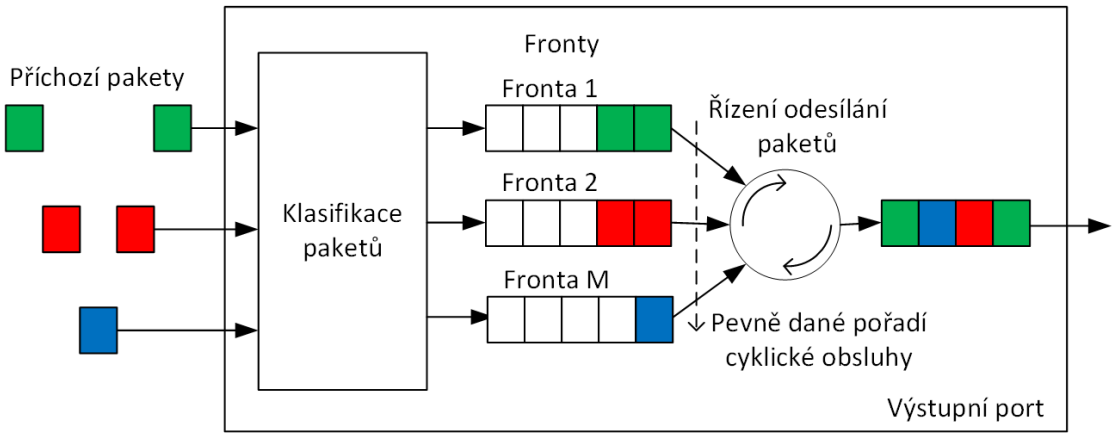
Obr. 3.8: Prioritní fronta PQ.

Fair Queuing – FQ

Dalším, poměrně jednoduchým, algoritmem je FQ. Příchozí pakety jsou rozděleny do front, které jsou cyklicky obsluhované. Při každém cyklu je z každé fronty odeslán maximálně jeden paket. Přesto, že se může zdát, že je FQ spravedlivé, skutečnost je jiná. FQ není schopen rozlišit velikost paketů, nebo požadavek na šířku pásma. Nelze tedy rozdělit šířku pásma ve vyžadovaném poměru, pakety s větší velikostí obsadí větší šířku pásma, než pakety s menší velikostí [17].

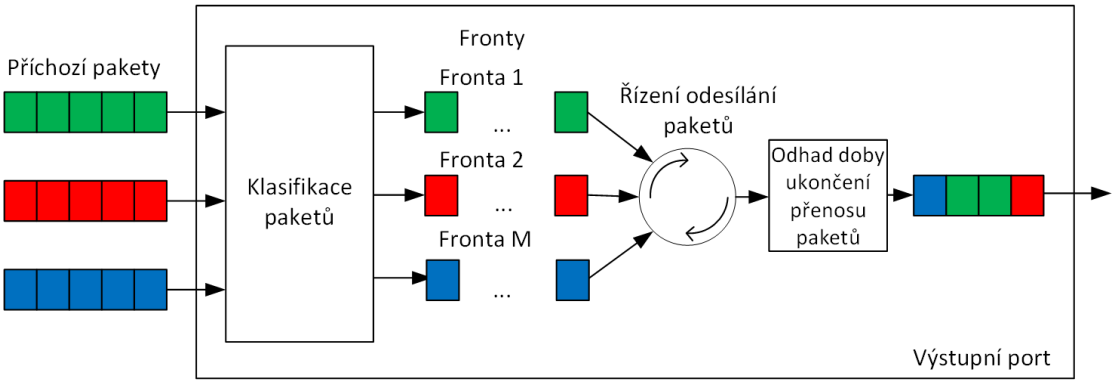
Weighted Fair Queuing – WFQ

Systém front s váženou spravedlivou obsluhou je další modifikací systému FQ. Na rozdíl od FQ , kde je odesílán celý paket nezávisle na jeho velikosti, eliminuje WFQ vliv délky paketu na šířku pásma. Příchozímu datovému toku je přidělena váha



Obr. 3.9: Fronta se spravedlivou obsluhou FQ.

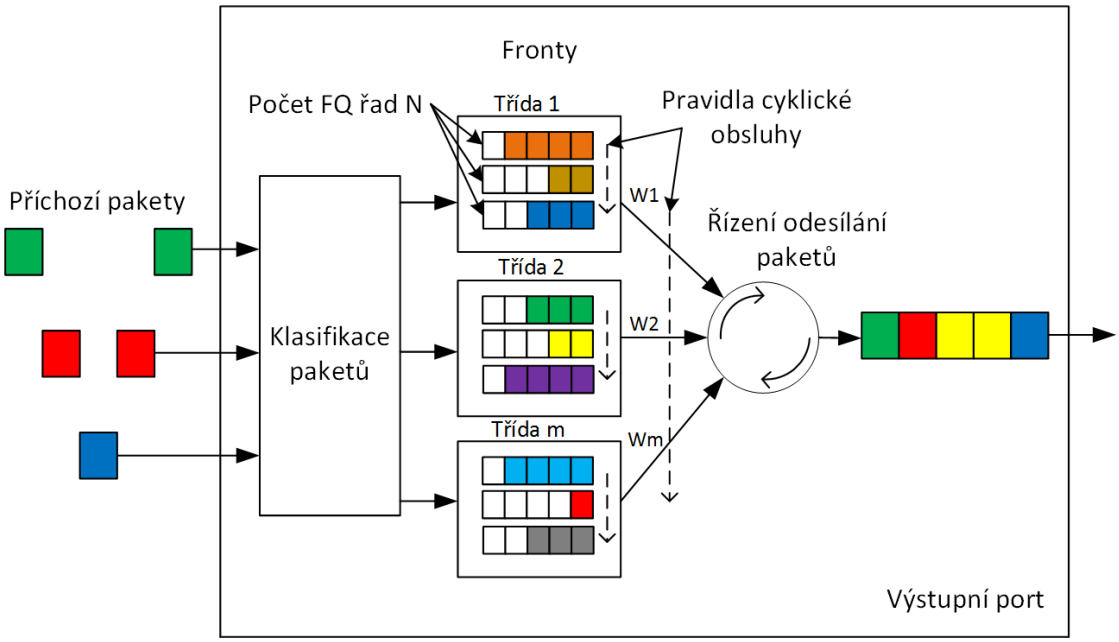
vyjadřující, jaká část celkové kapacity systému bude danému toku k dispozici. Součet všech váhových hodnot musí být roven 100 %. Odesílání paketů se řídí vypočítanou dobou konce odesílání [17].



Obr. 3.10: Fronta s váženou spravedlivou obsluhou WFQ.

Weighted Round Robin – WRR

Jedním z problémů FQ přidělování stejné šířky pásma každému datovému toku. Proto byl vyvinut systém front s váženou cyklickou obsluhou, který je schopný tento problém napravit. Vstupní datový tok je rozdělen do m tříd se specifickou váhovou hodnotou. Na základě váhy je jednotlivým třídám přidělena šířka pásma. Součet všech váhových hodnot je roven 100 %. WRR využívá dvou úrovní cyklické obsluhy Round Robin, kdy jedna úroveň vybírá frontu z třídy a druhá vybírá samotnou třídu. Systém váženou cyklickou obsluhou je nevhodný pro služby s vysokými nároky na zpoždění [13] [17].



Obr. 3.11: Fronta s váženou cyklickou obsluhou WRR.

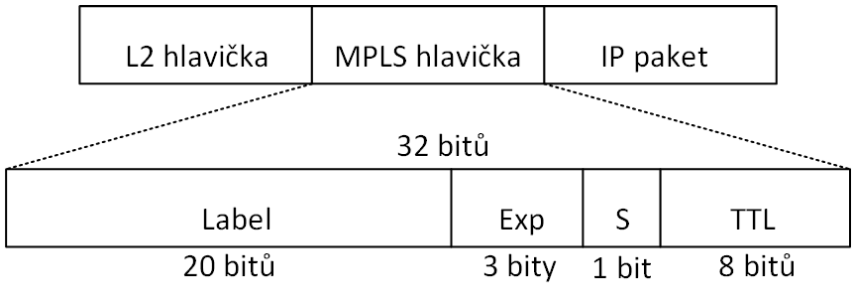
Class-Based Weighted Fair Queuing – CBWFQ

Systém front s váženou spravedlivou obsluhou podle tříd je, jak už z názvu vyplývá, kombinací systému WRR a WFQ. Přicházející datový tok je rozdělen do tříd. Blokové schéma je téměř shodné se systémem WRR s tím, že pro obsluhu datových toků uvnitř tříd je využit systém WFQ, na rozdíl od WRR, který využívá pro obsluhu datových toků uvnitř třídy systému FQ. Na rozdíl od samotného systému WFQ umožňuje spravedlivě rozdělit zbytek pásma mezi ostatní třídy.

3.4 MPLS

Multi protocol label switching vzniklo kombinací výhod klasických IP sítí s výhodami sítí ATM. Z klasických IP sítí je převzata jednoduchost a snadnost implementace protokolů, ze sítí ATM potom techniky řízení provozu [16]. Z hlediska referenčního modelu ISO/OSI pracuje MPLS mezi síťovou a linkovou vrstvou. Proto bývá MPLS někdy označováno jako vrstva 2,5. [21]

MPLS je protokolově nezávislou technologií, jejímž cílem je zjednodušení přepojování paketů a optimalizace rozdělení zátěže v síti, tzv. traffic engineering. Přepojování paketů probíhá výhradně na základě návěští (labels), které jsou paketům přiřazena. Není potřeba kontrolovat celý paket. Díky přepojování paketů podle návěští odpadá nutnost kontroly směrovacích tabulek, tak jak je tomu u klasických IP sítí, kde jsou pakety směrovány podle IP adres. [21]



Obr. 3.12: Struktura hlavičky MPLS.

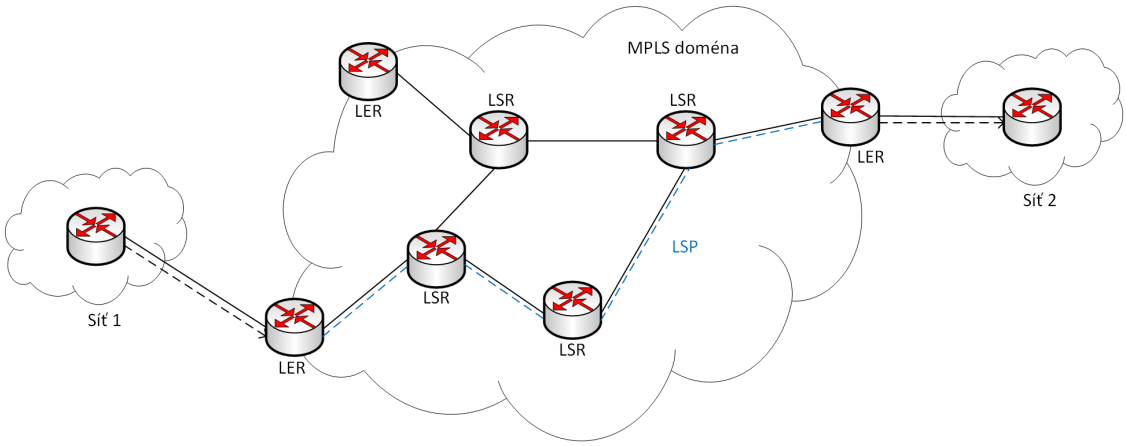
- **Label** – pole nesoucí aktuální hodnotu návěští.
- **EXP** – *Experimental* slouží pro experimentální využití, nebo pro nastavení priority zahazování paketů, podobně jako u DiffServ.
- **S** – *Bottom of Stack* je nastavený na 1, pokud se jedná o poslední položku v zásobníku návěstí, jinak je 0.
- **TTL** – *Time To Live* je 8bitové pole využité pro zakódování doby životnosti MPLS paketu.

3.4.1 MPLS architektura

V rámci MPLS architektury rozlišujeme dva druhy síťových zařízení. Na vstupu do MPLS domény, a výstupu z ní, se nacházejí hranové směrovače Label Edge Routers (LERs). Funkcí LER je generovat a přidávat MPLS návěstí k příchozím paketům na vstupu do MPLS domény a odebírání návěstí paketům opouštějícím doménu. Druhým typem zařízení jsou směrovače uvnitř domény Label Switching Routers (LSRs). Jak již bylo řečeno, směrování probíhá výhradně podle hodnoty návěstí. Po přijetí paketu porovnává LSR hodnotu návěstí s hodnou ve své tabulce pro nalezení nového návěstí a dalšího hopu. Jednoduché MPLS tabulky na směrovači podle vstupní hodnoty návěstí určují, kam má být dále paket směrován. Staré návěstí je nahrazeno novým. Všechny pakety se stejným návěstím, tedy všechny pakety v rámci třídy Forwarding Equivalence Class (FEC), se posílají stejnou cestou Label Switched Path (LSP) k cíli přes příslušné LSR. Virtuální okruh LSP pak vzniká tak, že si všechny LSR mezi hranovými LER vytvoří vazby mezi příchozí a odchozí hodnotou návěstí pro daný datový tok v rámci FEC. [21]

3.4.2 LDP protokol

Label distribution protokol (LDP) byl vytvořen pracovní skupinou MPLS. Jeho funkcí je distribuce návěstí mezi LER a LSR a mapování datového toku. LDP pro-



Obr. 3.13: Architektura MPLS.

tokol byl postupně rozšířen pro signalizace cesty s omezením, jako CR-LDP (LDP for Constraint Route signaling) a pro explicitní směrování pro řízení provozu protokolem RSVP-TE (RSVP for Traffic Engineering) na základě protokolu RSVP [21].

4 NÁVRH LABORATORNÍ ÚLOHY

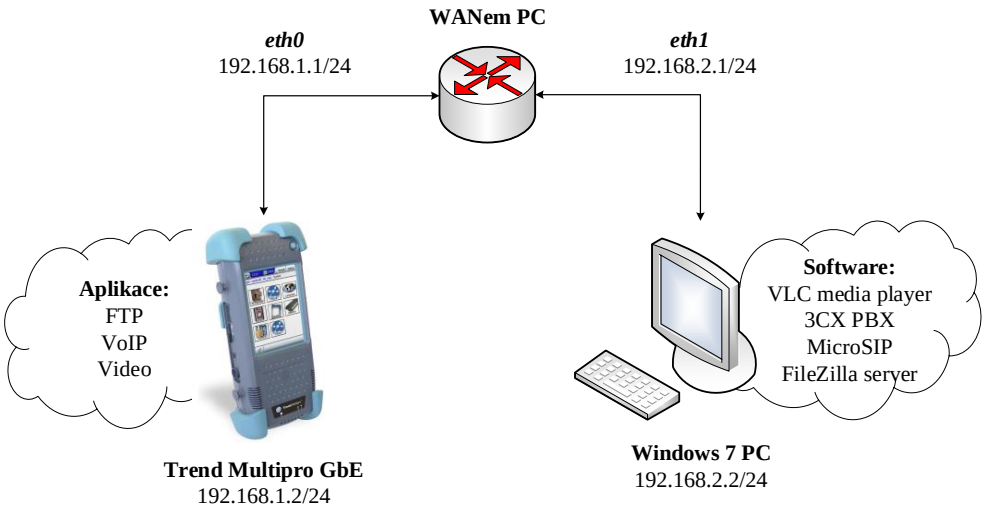
4.1 Výchozí podmínky

Cílem práce je návrh laboratorní úlohy pro měření kvalitativních parametrů v datových sítích za různých podmínek v mezilehlé síti. Laboratorní úloha je vytvořena pro předmět Architektura sítí. Při návrhu se vycházelo z následujících podmínek.

- Čas pro vypracování laboratorní úlohy je maximálně 90 minut.
- Pro realizaci využít tester Trend Multipro.
- Základní znalost podpory kvality služeb QoS ze strany studentů.

4.2 Topologie laboratorní úlohy

Testovací síť se skládá z testeru Trend Multipro zapojeného v režimu koncového zařízení, ve kterém se chová jako klientské koncové zařízení s možností testování serverových služeb, nebo VoIP, jednoho hostitelského počítače se dvěma virtualizovanými stanicemi WANem PC a Windows 7 PC. Bližší popis zapojení a konfigurace zařízení pro sestavení laboratorní úlohy jsou uvedeny v kapitole 4.3.



Obr. 4.1: Topologie testovací sítě.

4.3 Zařízení pro realizaci laboratorní úlohy

4.3.1 Trend Multipro GbE

Trend Multipro je moderní přenosný síťový tester se širokou škálou výkonnostních testů a možností ukládání jejich výsledků. Tester lze doplnit o celou řadu rozšiřujících modulů. Tester pro laboratorní úlohu je rozšířen gigabitovým modulem GbE, díky kterému lze provádět měření v různých bodech sítě. [25]

Obr. 4.2: Tester Trend Multipro GbE [25].

Tester umožňuje výběr ze třech odlišných módů. V každém módu si lze vybrat některý z nabízených testů, v CPE módu ještě navíc aplikaci. Základními nabízenými módy jsou:

1. **Monitoring mode**
   Tester monitoruje síťový provoz bez jakéhokoliv zásahu do dat. Tento mód umožňuje výběr ze dvou testů (APS, In-service) vhodných například pro detekci zahlcení sítě. [25]
2. **Through mode**
   V tomto módu je tester zapojen mezi LAN a WAN rozhraním. Tester je použit jako náhrada síťového prvku. Jedná se o mód velmi podobný Monitoring módu, dochází však k zásahu mezi data. Tester přeruší komunikační linku, analyzuje příchozí data a odesílá je dále do sítě. Výběr testů je stejný jako u Monitoring módu. [25]
3. **Customer Premises mode (CPE mode)** [25]
   Při využití CPE módu je Trend Multipro použit jako koncové zařízení, které

nahrazuje CPE, vhodné pro testy Triple play služeb. Zkratkou CPE (Customer-Premises Equipment) se v oblasti telekomunikací označují koncová zařízení zákazníka, připojené k telekomunikační síti, typicky telefony, modemy, nebo set-top-boxy. Po výběru módu a rozhraní si lze vybrat ze čtyřech aplikací (data, VoIP, video, GbE). Pro každou aplikaci jsou dále k dispozici specifické testy. [25]

- **VoIP aplikace**
  Tato aplikace umožňuje provádět jednoduché QoS testy a emulovat funkci VoIP telefonu na základě použití SIP protokolu. V laboratorní úloze se bude jednat o aplikaci `voip`, umožňující sestavit hovor mezi účastníky, a aplikaci `qoe` umožňující analyzovat QoS parametry spojení a faktory subjektivního hodnocení hovoru QoE. [25]
- **Data aplikace**
  Aplikace umožňuje testovat funkčnost, spolehlivost a kvalitu služeb xDSL sítí a jejich prvků. K dispozici je například test dostupnosti hosta (Ping), test synchronizace mezi routerem a DSLAM-em, nebo měření rychlosti přenosu souboru za pomoci FTP, nebo HTTP protokolu. [25]
- **Video aplikace**
  Tester umožňuje emulovat funkci set-top-boxu, analyzovat IPTV video tok dat poskytovaných providerem a určit chyby přenosu mezi providerem a zákazníkem. [25]
- **GbE aplikace**
  Pro aplikaci GbE jsou k dispozici testy dle standardu RFC 2544, SLA, nebo PING test.

Konfigurace zařízení:

V laboratorní úloze bude tester použit v CPE módu. Tester se chová jako koncové zařízení, je tedy nutné mu po výběru aplikace a zvolení testu přidělit statickou IP adresu. To lze provést nastavením IP vrstvy v kartě **Layers**. Po zvolení volby **IP** a **Conf.** se dostaneme přímo k nastavení síťové adresy a výchozí brány. Toto nastavení je nutné provést pro každou aplikaci. Konkrétní nastavení jednotlivých testů se liší.

Bližší konfigurace jednotlivých testů jsou uvedeny v návodu laboratorní úlohy v kapitole 5.5 a jsou součást učitelského manuálu. Předkonfigurované soubory `voip-lab-bars`, `ftp-lab-bars`, `video-lab-bars` a `rfc-lab-bars` sloužící k inicializaci nastavení testeru jsou součástí přiloženého DVD.

4.3.2 PC

Pro laboratorní úlohu je potřeba dvou PC stanic jež budou virtualizovány v jednom hostitelském PC pomocí programu `VirtualBox`. První WANem PC využívající systému Linux a druhý počítač OS Windows 7. V hostitelském operačním systému je nutné vypnout bránu firewall, která blokuje některé služby.

a) Windows 7 PC

Tato stanice je využita jako FTP server, VoIP ústředna, VoIP client a video server. Pro stream videa byl zvolen program `VLC media player`, jako FTP server byl zvolen program `FileZilla`, a jako softwareová pobočková ústředna byla vybrána `3CX PBX` s jednoduchým grafickým ovládáním. Jako VoIP client byl zvolen program `MicroSIP` podporující ve své free verzi širokou škálu audio kodeků, včetně kodeku ITU-T G.729.

Nastavení síťových karet ve Virtualbox-u:

Propojení WANem PC a Windows 7 PC je realizováno využitím vnitřní sítě v konfiguraci síťových rozhraní virtuálního Windows 7 PC po povolení síťové karty viz tabulka 4.1.

Tab. 4.1: Nastavení síťové karty pro stanici Windows 7.

Připojena k	Vnitřní síť
Název	intnet
Typ síťové karty	PCnet-FAST III
Promiskuitní režim	Povoleno vše

Konfigurace Windows 7 PC po spuštění OS:

Na PC s OS Windows 7 je též nutné úplně vypnout bránu firewall blokující některé služby. Dále je nutné na počítači staticky nastavit IPv4 adresu rozhraní podle tabulky 4.2.

Tab. 4.2: Nastavení síťového rozhraní Ethernet.

IP adresa	192.168.2.2
Maska podsítě	255.255.255.0
Výchozí brána	192.168.2.1

b) WANem PC

Emulátor WAN sítě WANem 3.0 je volně šiřitelný systém založený na linuxové distribuci Knoppix 3.7.1. Emulátor umožňuje nastavení širokého spektra parametrů pro emulaci síťového provozu. Mezi nejdůležitější parametry patří zpoždění, jitter, ztrátovost či duplicita paketů a nastavení šířky přenosového pásma. Pro účely laboratorní úlohy je emulátor WANem bootován z bootovacího `iso` souboru jako virtuální stanice v prostředí VirtualBox. Emulátor tak umožňuje nastavování parametrů na každém síťovém rozhraní zvlášť. Síťové karty jsou nastavené v režimu mostu, pouze spojení mezi virtuálním počítačem s WIN7 a virtuálním počítačem WANem jsou síťové karty v režimu `Vnitřní síť`, neboť obě stanice jsou spuštěny na jedné fyzické stanici. Stanici s emulátorem se po spuštění a konfiguraci rozhraní bude ovládat z webového rozhraní virtuálního Windows 7 PC nacházejícího se ve stejné doméně, zadáním adresy `http://<192.168.2.1>/WANem/`.

Nastavení síťových rozhraní ve VirtualBox-u:

Tab. 4.3: Nastavení síťové karty *Karta 1.*

Připojena k	Síťový most
Název	Adaptér Intel(R) Gigabit CT desktop 2
Typ síťové karty	PCnet-FAST III
Promiskuitní režim	Povoleno vše

Tab. 4.4: Nastavení síťové karty *Karta 2.*

Připojena k	Vnitřní síť
Název	intnet
Typ síťové karty	PCnet-FAST III
Promiskuitní režim	Povoleno vše

Nastavení síťových rozhraní ve WANem:

Jelikož WANem PC pracuje jako router, je po každém jeho spuštění nutné v okně `Network Connections` nastavit jednotlivým síťovým rozhraním IPv4 adresy, tak aby byly bránami pro ostatní zařízení. Nastavení síťových rozhraní se provádí v programu **Network Connection Editor→Wired**. Síťová rozhraní se nastavují vybráním rozhraní a zvolením **Edit** a **IPv4 Settings**. Statická IP adresa se nastavuje

editací pole `Method` na **Manual** a tlačítkem **Add** se přidá IP adresa a masku podsítě. Nastavení se potvrdí tlačítkem **Save**. Nastavení pro všechna rozhraní je uvedeno v tabulce 4.5.

Tab. 4.5: Nastavení síťových rozhaní ve WANem.

eth0	192.168.1.1	255.255.255.0
eth1	192.168.2.1	255.255.255.0

Stanici s emulátorem se po spuštění a konfiguraci rozhraní bude ovládat z webového rozhraní virtuálního Windows 7 PC nacházejícího se ve stejné doméně, zadáním adresy `http://<192.168.2.1>/WANem/`.

4.4 Testovací video sekvence

Testovací transportní streamy byli vytvořeny programem `ffmpeg` ovládaným z příkazového řádku z originálního videa **`video.mkv`**.

`video.mkv`

video kodek: MPEG-4 part 10 AVC
bitová rychlost video: 3163 Kbps
FPS: 25
Rozlišení: 1280x720
audio kodek: AC-3
bitová rychlost video: 384 Kbps

`video_TS1.ts`

video kodek: MPEG-2
bitová rychlost video: 1536 Kbps
FPS: 25
Rozlišení: 720x576
audio kodek: MPEG-1 Audio
bitová rychlost video: 128 Kbps

Překódování ve ffmpeg:

```
ffmpeg -i video.mkv -c:v mpeg2video -b:v 1568k -s 720x576 -r 25 -c:a
libmp3lame -b:a 128k video_TS1.ts
```

`video_TS2.ts`

video kodek: MPEG-4 part 10 AVC
bitová rychlost video: 768 Kbps
FPS: 25
Rozlišení: 720x576
audio kodek: AAC
bitová rychlost video: 128 Kbps

Překódování ve ffmpeg:
`ffmpeg -i video.mkv -c:v libx264 -b:v 768k -s 720x576 -r 25 -c:a aac -b:a 128k video_TS2.ts`

4.5 Popis navržených úloh

4.5.1 Nastavení síťových rozhraní WANem

Cílem je po nabootování stanice WANem nastavit jednotlivá síťová rozhraní tak, aby byly pakety přeposílány z jednoho síťového rozhraní na druhé. Seznámit se s ovládáním programu a zprovoznit vzdálené ovládání ze stanice Windows 7 PC.

4.5.2 Měření FTP přenosu dat

Cílem úkolu je zjistit, jak ztrátovost paketů ovlivňuje rychlost přenosu dat. Úkolem je změřit přenosovou rychlost při uploadu a downloadu dat z (na) FTP server při různé ztrátovosti paketů v mezilehlé síti. Dále zachytit programem Wireshark komunikaci mezi klientem a FTP serverem. Jako FTP server slouží program FileZilla nainstalovaný ve virtuální stanici Windows 7 PC.

4.5.3 Měření VoIP provozu

Cílem je změřit závislost kvalitativních faktorů MOS a R na ztrátovosti paketů a jitteru pro kodeky G.711 aLaw a G.729 využívající rozlišné způsoby kódování. Subjektivně porovnat kvalitu hovoru při různých hodnotách zpoždění, jitteru a ztrátovosti paketů v mezilehlé síti. Dále zachytit a analyzovat registraci VoIP klienta k 3CX PBX ústředně, zachytit a analyzovat uskutečněný hovor mezi klienty, obojí pomocí programu Wireshark.

4.5.4 Měření video streamu

Cílem úlohy je analyzovat složení transportního streamu a signalizované chyby v něm. Porovnat subjektivní kvalitu dvou video sekvencí využívající jiné audio a video kodeky. Jednotlivé TS analyzovat a zjistit bitové rychlosti využívané pro tabulky a ES a získané hodnoty porovnat.

5 LABORATORNÍ ÚLOHA – MĚŘENÍ KVALITATIVNÍCH PARAMETRŮ RŮZNÝCH TYPŮ PROVOZU ZA RŮZNÝCH PODMÍNEK V MEZILEHLÉ SÍTI

5.1 Cíl

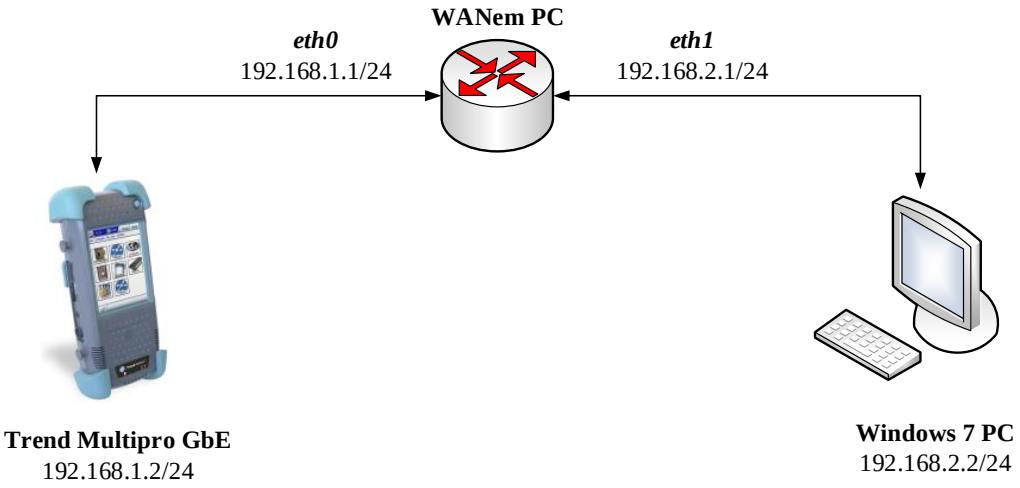
Cílem laboratorní úlohy je seznámit se s ovládáním a konfigurací testeru. Pomocí něj proměřit, jak ovlivňují zpoždění, kolísání zpoždění a ztrátovost v mezilehlé síti různé typy služeb. Sledovanými provozy budou VoIP hovor, přenos dat a streamované video. Degradace síťového provozu bude probíhat pomocí emulátoru WAN sítě WANem. Absolvováním laboratorní úlohy se student naučí ovládat a využívat moderní měřící přístroje, a zjistí, jak různé podmínky v mezilehlé sítí ovlivňují kvalitu vybraných síťových služeb.

5.2 Úkoly

1. Seznámit se s ovládáním testeru Trend Multipro. Nasavit rozhraní WANem PC.
2. Provést měření vlivu specifických podmínek v mezilehlé síti na přenos dat z(na) FTP server.
3. Porovnat odolnost hlasových kodeků vůči ztrátám paketů v datových sítích. Zjistit vliv jitteru na kvalitu VoIP hovoru pro vybrané kodeky.
4. 4. Změřit vliv různých parametrů na kvalitu transportního streamu simulujícího IPTV vysílání. Analyzovat TS a porovnat použité kodeky.
5. 5. Z naměřených hodnot sestavit přehlednou zprávu o měření s vynesenými grafickými závislostmi v tabulkovém editoru excel.
6. Zodpovědět kontrolní otázky.

5.3 Vybavení pracoviště

Počítač se dvěma síťovými kartami, s předinstalovaným operačním systémem Windows 7 a virtuálními stanicemi WANem PC a Windows 7 PC, tester TREND MULTIPRO.



Obr. 5.1: Topologie testovací sítě pro laboratorní úlohu.

5.4 Teoretický úvod

5.4.1 Podpora QoS

Zajištění podpory kvality služeb – QoS je důležité, aby nedošlo k zahlcení přenosové cesty. Jedná se o soubor pravidel, které umožňují klasifikaci paketů a přidělení priorit jednotlivých datových toků, podle čehož je pak daným tokům přidělováno požadované množství síťových prostředků ke správné funkci, tak aby nedocházelo k jejich „vyhladovění“. Dle druhu provozu a priority je s pakety následně zacházeno ve frontách síťových prvků. Implementací pravidel QoS se snažíme vybudovat kvalitní a předvídatelnou síť. [19]

QoS – Quality of Services

Výslednou kvalitu služby ovlivňují QoS metriky. Každý datový tok má odlišné požadavky na síťové prostředky. Síťové prostředky jsou vyjádřeny pomocí těchto metrik: komunikační zpoždění, kolísání zpoždění, datová propustnost a ztrátovost paketů.

Komunikační zpoždění vyjadřuje čas potřebný pro doručení paketů od zdroje k cíli. Zahrnuje zpoždění vlivem zpracování dat (komprimace, paketizace), zpoždění ve frontách mezilehlých síťových prvků a také vliv zvoleného přenosového média.

Jitter vyjadřuje změnu zpoždění přijatých paketů, vzniklou zatížením sítě, špatnou konfigurací, či zdržením se paketů ve frontách síťových prvků. Do určité úrovně si s kolísáním zpoždění poradí vyrovnávací paměť, záleží však na její velikosti.

Datová propustnost vyjadřuje, kolik dat je teoreticky možné přenést přenosovým kanálem za jednotku času.

Ztráta paketů vzniká, pokud dojde k zahlcení front síťových prvků, dojde k zahazování paketů podle zvolených mechanizmů, kdy jsou pakety zahazovány například podle priority.

Každý datový provoz klade jiné požadavky na množství síťových prostředků. Prioritou je zajistit dostatečné množství síťových prostředků službám s vyšší prioritou. Služby s podobnými požadavky se rozdělují do tříd. Nejvyšší prioritou se zpravidla označují služby pracující v reálném čase, tzv. real-time služby. Důležitým faktorem je také to, zda je využíváno TCP, nebo UDP spojení. TCP spojení je vhodné při požadavku bezchybného přenosu dat, neboť dochází k potvrzování segmentů a při chybě, nebo nepřijetí segmentu v daném čase je požadován opakovaný přenos. Naopak pro real-time služby je vhodné využít nespolehlivý UDP přenos, kdy nedochází k žádnému potvrzování dat, které by bylo nežádoucí a způsobovalo by nárůst zpoždění.

Přenos dat – Pro přenos dat je velmi důležité, aby byla data stažena bez chyb s využitím zbývající šířky pásma. Pro přenos dat je tedy kritická ztrátovost paketů. Obvykle využívá spolehlivý protokol TCP. [19]

VoIP – VoIP využívá protokol UDP. Hlasová informace se přenáší pomocí protokolu RTP (Real-Time Protokol). Přenos signalizačních zpráv je realizovaný nejčastěji pomocí protokolů H.323, nebo SIP. Signalizace obsahuje informace o navázání a ukončení spojení, nebo informace o změnách v navázané relaci. Služba VoIP klade veliké nároky na zpoždění a jitter. [19]

Audio streaming – Pro přenos zvuku (hudby, hlasu) jsou přísně požadavky na zpoždění, kolísání zpoždění a ztrátovost paketů, naopak malé požadavky na šířku pásma. S kolísáním zpoždění se vypořádává vyrovnávací paměť na straně příjemce za cenu zvyšujícího se zpoždění. Při ztrátovosti paketů nad 25 % se služba stává takřka nepoužitelnou. [19]

Video streaming – Video streaming není tak náročný na zpoždění, které se pohybuje v řádu 4–5 sekund. Příjemce proto může využít větší vyrovnávací paměť, která dokáže odstranit kolísání zpoždění, na kterém je videostreaming závislý. Důležitá je také ztrátovost paketů. [19]

IPTV – Požadavky na QoS jsou mimo jiné závislé na použitých audio a video

kodecích, využívajících různou šířku pásma pro přenos. Je tedy nutné vyhradit dostatečnou šířku pásma. Důležitým parametrem je ztrátovost a chybovost paketů, která silně ovlivňuje QoE. K částečnému odstranění chybovosti, vzniklé např. vlivem interferencí na přenosovém médiu, slouží FEC dekodér na Set-top-boxu. Pro dobrý požitek ze služby se doporučuje zpoždění do 200 ms a jitter do 50 ms. [1]

Tab. 5.1: Tabulka požadavků služeb na QoS [6].

Typ služby	Jitter [kb/s]	Zpoždění [ms]	Ztrátovost [%]
Audio	ovlivněno bufferem	0 – 400	3
Video	ovlivněno bufferem	150 – 400	1
FTP	–	–	různé
VoIP	0 – 20	150 – 240	2

QoE – Quality of Experience

Vyjadřuje hodnocení kvality poskytnuté služby ze strany příjemce. To, jak je uživatel spokojen s poskytovanou službou z hlediska použitelnosti. Jedná se o statistickou metodu, ke které je potřebný reprezentativní vzorek respondentů. QoE je ovlivněno nejen QoS, ale také sociálními faktory. To jak je uživatel spokojen s kvalitou poskytnuté služby závisí mimo QoS parametrů také na jeho předchozích zkušenostech s danou službou. Důležitý je také zvolený kodek, a jeho odolnost.

Pro hodnocení kvality služby se využívá zejména MOS stupnice a také R-faktor. Parametr MOS lze rozdělit podle způsobu, jakou metodou je získán. Parametr MOS lze rozdělit na: [11]

1. Subjektivní
2. Objektivní
    - Intrusivní
    - Neintrusivní
    - Odhadové

Subjektivní metody staví na hodnocení služby reprezentativním vzorkem uživatelů, kteří službu hodnotí. Jedná se o nejpřesnější, avšak velmi časově a finančně náročnou metodu, využívanou zejména při aplikaci nových kodeků. [27]

Intrusivní objektivní metody jsou založené na odhadu výsledné kvality pomocí matematických algoritmů, bez přítomnosti lidského faktoru. V závislosti na porovnání originálních a přijatých dat, které jsou vlivem přenosu degradovány, se snaží odhadnout, jak by reagoval koncový uživatel. [27]

Neintrusivní metody neporovnávají odeslaný a přijatý datový tok jako metoda intrusivní. Výsledná kvalita je vypočítán na základě analýzy chyb pouze v přijatých datech. [27]

Odhadové metody se snaží odhadovat hodnotu kvality z QoS parametrů bez znalosti obsahu originálních a přijatých dat. Mnohdy bývají označovány za neintrusivní metody. [27]

5.4.2 Analýza VoIP hovoru

Pro subjektivní vyhodnocování kvality hovoru byla stanovena stupnice MOS se škálou od 1 do 5. MOS stupnice souvisí zejména s VoIP a IPTV. Pro účely plánování sítí byl vytvořen E-model jehož výstupem je R faktor. MOS faktor lze na R faktor jednoduše přepočítat. R faktor může nabývat hodnot 0–100, přičemž se využívají pouze hodnoty 50–100. E-model poskytuje předpověď kvality hovoru, tak jak ji vnímá typický uživatel, za stanovených konverzačních podmínek daných v doporučení ITU-T G.107.

Pro objektivní hodnocení kvality služby pomocí intrusivních a neintrusivních metod je parametr MOS vypočítáván. Využívají se poznatky ze subjektivního hodnocení. Analyzátory se z výpočtů snaží odhadnout, jak by na kvalitu přijatého signálu reagoval člověk. Parametr MOS a R se podle způsobu vyhodnocování a místa získání dále dělí na poslechový a konverzační. Konverzační MOS zohledňuje konverzaci oběma směry, a také vzájemnou synchronizaci. Poslechový MOS a R faktor je vyhodnocován ze strany posluchače. [27]

- **MOS_CQ** – MOS konverzační,
- **MOS_LQ** – MOS poslechový,
- **R_CQ** – R konverzační,
- **R_LQ** – R poslechový.

Tab. 5.2: Hodnocení uživatelské spokojenosti se službou [8].

R-faktor	Uživatelská spokojenost	MOS
90–100	Velmi spokojeni	4,34–5
80–89	Spokojeni	4,03–4,33
70–79	Někteří uživatelé nespokojeni	3,60–4,02
60–69	Mnoho uživatelů nespokojeno	3,10–3,59
50-59	Téměř všichni uživatelé nespokojeni	2,58–3,09

5.4.3 Analýza transportního toku IPTV

IPTV umožňuje sledování televizního vysílání přes IP protokol s poskytovanou úrovní QoS a QoE. Tato služby bývá operátory často poskytována s dalšími službami v rámci Triplay služeb (data, VoIP a IPTV), kdy se řeší podpora QoS prioritami pro každou službu zvlášť. Nutností je přihlášení se do multicastových skupin, pomocí kterých se IPTV šíří. Požadavky na QoS jsou mimo jiné závislé na použitých audio a video kodecích, využívajících různou šířku pásma pro přenos. Je tedy nutné vyhradit dostatečnou šířku pásma. [1] Moderní analyzátory umožňují zjistit, jakou šířku pásma využívají jednotlivé elementární streamy.

Jelikož není ve skutečném přenosovém prostředí možné zajistit bezchybný přenos, je nutné data na vysílací straně zabezpečit některým z FEC kódů. Transportní tok je vytvářen postupně. Nejprve jsou jednotlivé elementární audio či video toky rozděleny do paketů, které ve své hlavičce obsahují časové značky umožňující správné dekódování snímků na straně příjemce. Elementární audio a video toky příslušící jednomu programu vytváří programový tok. Několik programových toků je multiplexováno do jednoho transportního toku. Pakety transportního toku jsou identifikovány pomocí identifikátoru PID. PID=0 odkazuje na PAT tabulku s PID obsažených programů. PAT odkazuje na PMT, která obsahuje jednotlivé elementární streamy (audio, video, titulky) pro daný program.

Subjektivní hodnocení kvality

Stupnice MOS nesouvisí pouze s VoIP, ale používá se také při hodnocení kvality streamovaných videí, nebo IPTV. V souvislosti s IPTV se používá MOS_C, vyjadřující dojem z interakce IPTV služeb, MOS_A hodnotící kvalitu zvuku, MOS_V hodnotící kvalitu videa, nebo kombinovaný faktor MOS_AV, který zahrnuje také synchronizaci mezi zařízeními. Využívá se stejná stupnice jako v případě MOS u VoIP technologie. Výsledná hodnota MOS faktoru je dána aritmetickým průměrem. Kvalitu sledovaného obrazu může narušit výpadek snímků, špatná synchronizace obrazu a zvuku, chyby ve snímcích, nebo šum. [1][12]. Pro snížení přenosové rychlosti se používají kompresní kodeky. Perspektivním kodekem je MPEG-4 (H.264), který dokáže snížit přenosovou rychlost až o 50 % oproti kodeku MPEG-2, při zachování stejné vizuální kvality.

Objektivní hodnocení kvality

Pro objektivní hodnocení kvality jsou známe především parametry MSE (Mean Square Error) a PSNR (Paek signal-to-nois ratio), dalšími parametry jsou MDI,

MPQM, SSIM a další. Tyto metody se zakládají zejména na matematických výpočtech, které porovnávají surové a komprimované snímky.[12]

MSE vyjadřuje střední kvadratickou odchylku přijatého video signálu od původního videosignálu.

PSNR vyjadřuje poměr nejvyšší hodnoty signálu ku MSE.

Chyby v transportním toku [5]

Vybranými chybami, které dokáže analyzátor Trend Multipro analyzovat jsou:
TS_sync_loss nastává pokud tři po sobě jdoucí pakety neobsahují hodnotu 0x47.
Continuity_count_error nastává, pokud pakety nejsou doručeny ve správném pořadí, nebo nastane ztráta 2 a více paketů.
PAT_error nastává, pokud není PAT tabulka přijata každých 0,5 s, nebo paket neobsahuje hodnotu 0x00 identifikující PAT tabulku. Dekodér nedekóduje žádný program.
PTS_error nastává, pokud perioda příchodu časových razítek je větší než 700 ms.
PMT_error nastává, pokud není dekódována PMT tabulka.
Transport_error informuje, že v paketu jsou chyby. Chyba je ohlášena nastavením pole transport_error_indicator v hlavičce paketu na hodnotu 1.

5.5 Pokyny k vypracování

5.5.1 Úkol č. 1 – Nastavení síťových rozhraní ve WANem

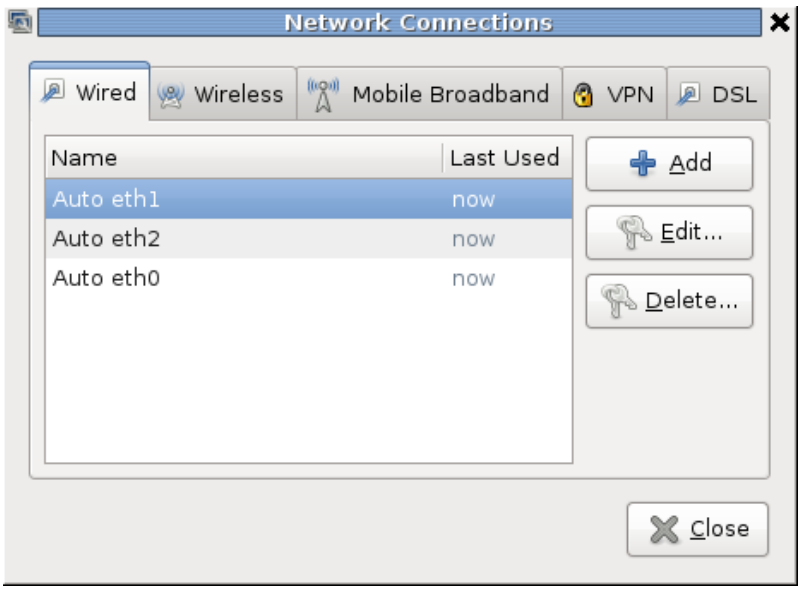
Po spuštění virtuálního PC s WANem emulátorem je nutné nastavit síťová rozhraní tak, aby se emulátor WANem choval jako router a přepínal pakety z jednoho síťového rozhraní na druhé. V okně `Network Connections` nastavte jednotlivá rozhraní. Okno vyskočí automaticky, nebo jej otevřete pomocí nabídky v hlavní liště a zvolte **System Tools→Network Connection Editor→Wired**. Síťová rozhraní nastavte dle topologie testovací sítě. Vyberte rozhraní a zvolte **Edit** a **IPv4 Settings**. Položku `Method` nastavte na **Manual** a tlačítkem **Add** přidejte IP adresu a masku podsítě. Potvrďte tlačítkem **Save** a obdobně nastavte i ostatní rozhraní.

Adresy rozhraní zkontrolujte ve WANem terminálu, který se spouští ikonou monitoru v hlavní liště emulátoru. Ve WANem terminálu lze využívat příkazy z tabulky 5.3.

Tab. 5.3: Příkazy terminálu WANem.

Příkaz	Význam
`status`	výpis síťových rozhraní
`reset`	reset síťových rozhraní
`wanemreset`	reset síťových rozhraní do výchozího nastavení
`exit2shell`	přepnutí do klasického Linux terminálu (z WANem terminálu)
`wanem`	přepnutí do WANem terminálu (z Linux terminálu)
`shutdown`	vypnutí WANem

Dostupnost všech koncových zařízení ověřte příkazem **`ping`** z druhé virtuální stanice s OS Windows 7. Emulátor můžete minimalizovat a dále se k němu vzdáleně připojovat zadáním adresy `http://<IP adresa WANem>/WANem/`.



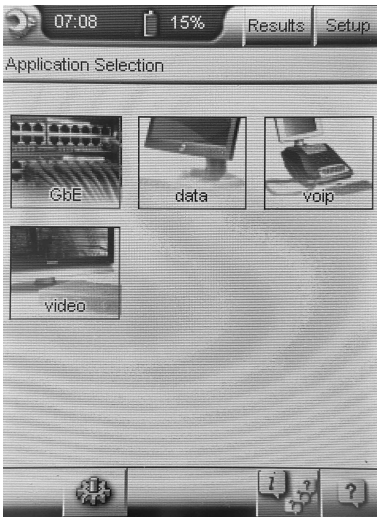
Obr. 5.2: Okno pro nastavení síťových rozhraní ve WANem.

Nastavování parametrů se provádí ve webovém rozhraní, v sekci **Advance mode** po vybrání příslušného síťového rozhraní.

5.5.2 Úkol č. 2 – Měření FTP přenosu dat

Spusťte program `FileZilla Server Interface` na lokální smyčce 127.0.0.1, port ponechejte defaultně. V nabídce klikněte na **Edit→Users**, přidejte uživatele v poli `Users` pomocí tlačítka **Add** a nastavte mu heslo. Uživatele nepřidělujte do žádné skupiny. V záložce `Shared folders` pomocí tlačítka **Add** přidělte vytvořenému uživateli přístup s veškerými právy k adresáři `FTP`, který se nachází na ploše. Nastavení

uživatele potvrďte pomocí **OK**. V adresáři FTP se nachází soubory `*.bin`, které se budou ze serveru stahovat.



Obr. 5.3: Výběr aplikace na testeru Trend Multipro.

Zapněte tester Trend Multipro a vyberte aplikaci `data` a test `ftp`. V pravém horním rohu zvolte **Setup**, nahrajte předkonfigurovaný soubor `ftp-lab-bars` a vraťte se zpět k testu. V kartě `Status` vidíte aktuální nastavení, stav a průběh testu. V kartě `Layers` zvolte **IP→Config**, ověřte nastavení statické IP adresy, masky a výchozí brány podle topologie testovací sítě 5.3. Vraťte se do hlavní nabídky a v kartě `Setup` nastavte IP adresu FTP serveru, uživatelské jméno a heslo, které jste zvolili. K FTP serveru se připojte pomocí **Log On**. Navázání spojení mezi klientem a serverem zachyťte v programu Wireshark a analyzujte.

Pro stahování dat z FTP serveru vyberte možnost **GET** a vyberte některý ze souborů připravených pro stažení. Pro měření uploadu zvolte **PUT** a z testeru zvolte soubor, který chcete na server nahrát.

Přes webový prohlížeč se vzdáleně připojte ke stanici WANem PC zadáním adresy `http://<adresa rozhraní>/WANem/` a zvolte **Advanced mode** a rozhraní, které chcete emulovat. Zde nastavte propustnost v poli **Bandwidth**, a dále měňte ztrátovost paketů v poli **Loss**.

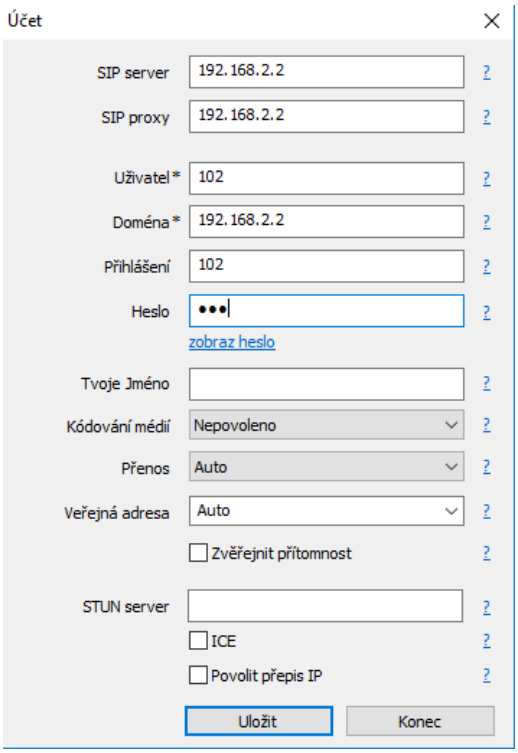
Otevřete připravený tabulkový soubor a proměřte pro upload i download závislost přenosové rychlosti na ztrátovosti paketů.

5.5.3 Úkol č. 3 – Měření VoIP provozu

Na ploše spusťte `3CX Management Console` a přihlaste se (User name: `admin`, password: `admin`). V záložce **Settings→Network→Public IP** zkontrolujte zda

jsou obě adresy nastavené na adresu virtuálního Windows 7 PC. Pokud ne, adresy přenastavte. Na ústředně jsou předkonfigurovány dva účty (ID:101 a heslo:101 pro tester, ID:102 a heslo:102 pro microSIP). Správa jednotlivých účtů se provádí v záložce **Extension**.

Nyní spusťte program `MicroSIP`, klient by se měl automaticky připojit k účtu 102 na ústředně. Pokud se tak nestane otevřete záložku **Nabídka→Upravit nastavení účtu** a zkontrolujte, zda nastavené ID a heslo, koresponduje s účtem vytvořeným pro MicroSIP v ústředně. V poli `Domain` ověřte IP adresu rozhraní, na kterém je spuštěna PBX ústředna, SIP proxy, SIP server a uložte.



Obr. 5.4: Nastavení účtu MicroSIP.

Na testeru spusťte aplikaci `voip→ip-phone` a nahrajte konfigurační soubor `voip-lab-ftp` obdobně jako u FTP nastavení. Registraci testeru k ústředně zaznamenejte pomocí Wireshark-u. Pokud nedošlo k modifikaci konfiguračního souboru, tester se během cca 30 s automaticky přihlásí k účtu 101 vytvořenému v ústředně. Při úspěšné registraci by v kartě `Status` měla zeleně svítit kontrolka **Registered**. Pokud se tak nestane, zkontrolujte nastavení IP adresy na IP vrstvě v kartě `Layers→IP` a vraťte se zpět. Dále v kartě `Setup` zkontrolujte nastavení účtu *Voip Number, User a Password* podle toho, jak je nastaven účet pro Trend Multipro v ústředně. Zkontrolujte, zda jsou zatrženy položky `SIP Registration Server` a `SIP Proxy Server` s IP adresou ústředny. Port ponechte defaultně na **5060**. Pokud jste postupovali

správně, v přehledu účtů PBX ústředny (**View→Extension View**) byste měli vidět zelený čtvereček u obou z vytvořených účtů, který značí registraci VoIP klientů k ústředně.

Stiskněte symbol ciferníku (**<To>**) a zvolte číslo MicroSIP klienta, na kterého budete volat. Na testeru si prohlédněte hodnoty **RTP QoS**. Opět sestavte hovor a sledujte, jak zpoždění, jitter a ztrátovost, nastavené emulátorem WANem, ovlivňují kvalitu hovoru. Zejména se zaměřte na kolísání zpoždění, které je silně závislé na vyrovnávací paměti koncového zařízení a na ztrátovost paketů.

Vraťte se zpět k výběru testů a zvolte `voip-qos` test. Nastavení neměňte, zůstalo zachováno nastavení z předchozího testu. Sestavte hovor mezi účastníky s audio kodekem G.711 A law a v kartě `Status` nalistujte **QoS Summary**, kde jsou znázorněny QoS statistiky odesílaných a přijímaných dat. Klikněte na **Quality** a zvolte statistiku přijímaných dat `Quality Metrics - Rx`. Do záznamového excel souboru zaznamenejte základní QoS parametry hovoru. Dále změřte závislost MOS a R faktoru na kolísání zpoždění, a závislost MOS a R faktoru na ztrátovosti paketů. Stejné měření zopakujte i pro kodek G.729, který změňte v kartě **Setup→Codec Setup**. Po každé změně parametrů v emulátoru WANem je nutné sestavit nový hovor!

Z naměřených hodnot a vynesených závislostí porovnejte odolnost audio kodeků vůči ztrátám. Dále stanovte vliv kolísání zpoždění na VoIP provoz.

Pozn.: Kodek **G.711** využívá PCM. Vzorkovací frekvence je 8 kHz a rozlišení 8 bitů, což po vynásobení dává přenosovou rychlost 64 kbit/s. Nejvyšší dosažitelnou hodnotou MOS faktoru v reálné síti je 4,4. Výhodou kodeku je vysoká kvalita přenášeného zvuku, nevýhodou je poměrně velká bitová rychlost.

Kodek **G.729** využívá hybridní kódování a algoritmus CS-CELP. Přenosová rychlost dat je 8 kbit/s a udávanou nejvyšší hodnotou MOS faktoru je 3,9. Výhodou kodeku je jeho velmi nízká přenosová rychlost, nevýhodou je, že kódovaný hlas má syntetický charakter.

5.5.4 Úkol č. 4 – Měření video streamu

Pro hodnocení kvality transportního streamu jsou na ploše v adresáři `Video` připraveny dvě videosekvence se stejnou video i audio stopou, ovšem kodované pomocí jiných kodeků. Nejprve si obě videa otevřete pomocí VLC media playeru vedle sebe a pokuste se je časově synchronizovat. Subjektivně porovnejte kvalitu obou videí. Následně spusťte stream videa na testr, kde jej budete analyzovat.

Stream spustíte pomocí `VLC media player`-u. V záložce **Media→Stream** vyberte tlačítkem **Add** z plochy video, které chcete streamovat, a zvolte **Stream** a **Next**. V následujícím okně vyberte `RTP / MPEG Transport Stream` a zvolte **Add**.

Déle nastavte IP adresu analyzátoru a port ponechejte defaultně na 5004. Deaktivujte překódování a spusťte streamování videa.

Na testeru Trend zvolte aplikaci `video` a test `player`. Nahrajte předkonfigurovaný soubor `video-lab-bars` a ověřte nastavení síťové vrstvy obdobně jako v předchozích aplikacích. V záložce **Setup** klikněte na ikonu ovladače a zvolte stream nazvaný **BARS** na adrese **192.168.1.2** a portu **5004**. Stream otevřete tlačítkem play. Analyzujte transportní stream pro obě videa. Zjistěte z jakých částí se skládá a které složky jsou dominantní z hlediska přenosové rychlosti. Zjistěte použité kodeky pro jednotlivá videa a jaký je vztah mezi kvalitou videí kódovaných odlišnými kodeky a přenosovou rychlostí dat.

5.6 Kontrolní otázky

1. Jaký je rozdíl mezi subjektivním a objektivním hodnocením kvality?
2. Jaké druhy faktoru MOS rozlišujeme?
3. Jaké QoS metriky zásadně ovlivňují VoIP hovory, FTP přenos dat a video stream?
4. Která strana zahajuje spojení při přenosu dat z/na FTP server v pasivním režimu?
5. Jaké zprávy si zasílají UAC a UAS pro inicializaci a ukončení VoIP spojení?
6. Jaký protokol je využíván pro dohodnutí kodeků využívaných pro kódování dat mezi terminály?
7. Jak ovlivňují použité kodeky šířku pásma transportního streamu?
8. Jaké transportní protokoly jsou využívány pro FTP přenos dat, VoIP hovory, nebo přenos videa pomocí transportního streamu?
9. Jaký aplikační protokol se využívá pro přenos multimediálních dat po internetu?

6 ZÁVĚR

Bakalářská práce se zabývala problematikou zajištění kvality služeb v IP sítích a hodnocením kvality služeb. Vzhledem k nárůstu datových toků přenášených datovými sítěmi je podpora QoS na vrstvách L2 a převážně L3 nepostradatelná. Důvodem implementace mechanizmů pro zajištění kvality služeb je budování kvalitní a předvídatelné sítě.

Hodnocení kvality služeb lze provádět na základě technických parametrů sítě v případě QoS, kdy má každý síťový provoz odlišné požadavky na parametry sítě, zvané metriky. Hodnotit kvalitu služby lze i subjektivně, za příspěvku koncových uživatelů pomocí stupnice MOS, nebo s využitím počítačových simulací a faktoru R. QoE je značně využíváno poskytovateli služeb, pro zajištění dostatečné kvality služby za přijatelnou cenu.

Prvním technologií, která měla zajistit podporu QoS v IP sítích byl model Integrovaných služeb. Do té doby byla využívána pouze služba bez záruky – best effort. Hlavní výhodou technologie IntServ je rezervace síťových zdrojů podél celé přenosové cesty za pomoci rezervačního protokolu a jeho zpráv. Hlavními nevýhodami IntServ jsou velké nároky na směrovače, vyšší režie a doba pro sestavení spojení. Architektura IntServ je vhodná pro využití v podnikových sítích.

Podstatně novější a v současnosti nejvyužívanější technologií je DiffServ s výhodným nasazením v páteřních sítích. Výhodou této technologie je možnost rozdělení datových toků do tříd podle hodnoty DSCP pole. Pakety jsou značkovány pouze v hraničních směrovačích DiffServ domény, nedochází tedy k takovému zatížení sítě.

Nejnovější technologií je, protokolově nezávislá, MPLS s využitím Traffic engineering pro optimalizaci výkonu sítě. Směrování paketů probíhá na základě návěští. Technologie MPLS vyniká také svým zabezpečením proti DoS útokům.

Závěrečná část práce se zabývá návrhem laboratorní úlohy pro měření závislosti požadavků různých typů provozu na kvalitativních parametrech sítě, které budou emulovány. V úvodu této části jsou popsány použitá zařízení. Trend Multipro pro měření a generování testovacího signálu. Pro zhoršování parametrů linky je využitý nástroj WANem běžící na linuxovém jádru, umožňující měnit zpoždění, kolísání zpoždění a ztrátovost paketů.

Poslední kapitolu bakalářské práce tvoří podrobný návod pro vypracování laboratorní úlohy. Po absolvování laboratorní úlohy bude student schopen určit metriky ovliňující jednotlivé datové služby a vliv těchto metrik na výslednou kvalitu služby. Vzorové vypracování, jednotlivé návody a konfigurační soubory pro tester Trend Multipro jsou součástí přiloženého DVD.

LITERATURA

[1] BALEJ J. *Simulace QoS v nástroji Network Simulator.* Brno: Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací, 2008. 58 s., Bakalářská práce. Vedoucí práce byl Ing. Milan Šimek.

[2] BUMBÁL, M. *QoS v IP síti.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 69 s. Vedoucí diplomové práce Ing. Lukáš Růčka.

[3] CISCO, Inc.. *Implementing Cisco Quality of Service.* Student Guide, Volume 1-2, Version 2.2, 2014.

[4] CISCO, Inc.. *Implementing Quality of Service Policies with DSCP* [online]. 2008-02-15 [cit. 2015-11-10]. Dostupné z URL: <http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html>.

[5] ETSI. Digital Video Broadcasting (DVB): Measurement guidelines for DVB systems, ETR 290 [online]. In: . [cit. 2016-05-14]. Dostupné z: <http://www.etsi.org/deliver/etsi_etr/200_299/290/01_60/etr_290e01p.pdf>.

[6] HASSAN, S. A., YE, L. *Medical Quality-of-Service Optimization in Wireless Telemedicine System Using Optimal Smoothing Algorithm* [online]. Shenzhen Institutes of the Advanced Technologies, Chinese Academy of Sciences, Shenzhen, China, 2012. Dostupné z URL: <http://file.scirp.org/Html/1-2370017_29573.htm>.

[7] IETF. Benchmarking Methodology for Network Interconnect Devices: RFC 2544. Network Working Group, 1999. Dostupné z: <http://www.ietf.org/rfc/rfc2544.txt>.

[8] ITU-T . G.107: The E-model: a computational model for use in transmission planning [online]. 2011a [cit. 2015-12-5]. Dostupné z URL: <http://www.itu.int/rec/T-REC-G.107>.

[9] JAREŠ, Petr. *Diagnostika přenosových systémů a sítí využívajících technologii Ethernet* [online]. In: . České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2016-04-25]. Dostupné z: <http://data.cedupoint.cz/oppa_e-learning/2_KME/152.pdf>.

[10] Krasňan, L. *Testovanie mechanizmov QoS Cisco IOS pre zabezpečenie kvality hlasových služieb a bezpečnosti.* Brno: Masarykova univerzita: Fakulta informatiky, 2013. Diplomová práce. Vedoucí práce: doc. Ing. Jaroslav Do˘ckal, CSc..

[11] Kuipers, F. a kol. 2010. *Techniques for Measuring Quality of Experience.* In: Proceedings of the 8th international conference on Wired/Wireless Internet Communications , s. 216–227. ISBN 978-3-642-13314-5.

[12] KREJČÍ, J. a T. ZEMAN. *Hodnocení kvality IPTV* [online]. In: . Praha: České vysoké učení technické v Praze, FEL, 2010 [cit. 2016-05-13]. Dostupné z: <http://access.feld.cvut.cz/view.php?cisloclanku=2010050004>.

[13] LEE, Byeong Gi a Woojune KIM. *Integrated broadband networks: TCP/IP, ATM, SDH/SONET, and WDM/Optics.* Boston: Artech House, c2002, xviii, 605 p. ISBN 1580531636.

[14] LEDVINA, Jiří. *QoS v datových sítích, IntServ a DiffServ* [online]. 2007. [cit.2008-11-22], Dostupné z URL: <http://www.kiv.zcu.cz/~ledvina/Prednasky-PSI-2007/qos-text.pdf>.

[15] LUHOVÝ, Karel. *VLAN (4) – standard 802.1Q* [online]. 2003-04-22 [cit. 2015-12-12]. Dostupné z URL: <http://www.svetsiti.cz/clanek.asp?cid=VLAN-4--standard-8021Q-2242003>.

[16] MARCHESE, Mario. *QoS over heterogeneous networks.* Hoboken, N.J.: John Wiley & Sons, c2007, xix, 307 p. ISBN 047001752x.

[17] MOLNÁR K. *Mechanizmus diferencovaných služeb.* [online], 2008, [cit. 2015-04-12], Dostupné z URL: <http://www.utko.feec.vutbr.cz/~molnar/mmos/QoS.pdf>.

[18] NOVOTNÝ, V. *Pevné a bezdrátové síťové technologie pro integrovanou výuku VUT a VŠB-TUO.* Elektronické skriptum. Brno: FEKT VUT v Brně, 2014.

[19] NOVOTNÝ, Vít. *Požadavky různých druhů provozu na kvalitu služby.* Laboratorní úloha. Brno: FEKT VUT v Brně.

[20] PARK, K. I. *QoS in packet network.* New York: Springer Science+Business Media, Inc., 2005. ISBN 0-387-23389-8.

[21] PUŽMANOVÁ, R. *Vývoj paketových sítí a postavení MPLS* [online]. 2006. [cit.2008-12-13]. Dostupné z: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=302>.

[22] Vozňák, M., Zukal, D. *Vyhodnocení kvality hovoru pomocí R-faktoru v sítích VoIP*, CESNET, 2004, Dostupné z URL:<https://http://homel.vsb.cz/~voz29/files/voz49.pdf>.

[23] [RFC 2210] Wroclawski, J. *The Use of RSVP with IETF Integrated Services.* RFC 2210. September 1997. Dostupné z URL: <https://tools.ietf.org/html/rfc2210>.

[24] SATRAPA, Pavel. *Transportní protokol SCTP* [online]. 2001-05-17 [cit. 2015-12-12]. Dostupné z URL:<http://www.lupa.cz/clanky/transportni-protokol-sctp/>.

[25] TREND COMUNICATIONS. *Trend Multipro: Multipro help.* 10. vydání. Maidenhead, Berkshire: IDEAL INDUSTRIES Ltd., 2009.

[26] WANG, Zheng. *Internet QoS: architectures and mechanisms for quality of service.* San Francisco: Morgan Kaufmann, c2001, xv, 239 p. Morgan Kaufmann series in networking. ISBN 1558606084.

[27] ZACH, Petr. *Metodika sledování a hodnocení počítačové sítě podniku.* Brno, 2015. Disertační práce. Mendelova univerzita v Brně. Vedoucí práce Doc. Ing. Arnošt Motyčka, CSc.

SEZNAM ZKRATEK

AF	Asured Forwarding
ATM	Asynchronous Transfer Mode
CBWFQ	Class Based Weighted Fair Queuing
COPS	Common Open Policy Service
CoS	Class of Service
CPE	Customer-Premises Equipment
CR-LDP	LDP for Constraint Route signaling
DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
FEC	Forwarding Equivalence Class
FIFO	First In First Out
FQ	Fair Queuing
FTP	File Transport Protocol
IntServ	Integrated Services
IP	Internet Protocol
ITU-T	ITU Telecommunication Standardization Sector
LER	Label Edge Routers
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSR	Label Switching Router
MGCP	Media Gateway Control Protocol
MPLS	Multi Protocol Label Switching

MOS	Mean Opinion Score
OSI	Open Systems Interconnection
PQ	Priority Queuing
QoE	Quality of Experience
QoS	Quality of Service
RED	Random Early Detection
RFC	Request For Commentsn
RESV	Reserve
RTI	Real Time Intolerant
RTP	Real-Time Protokol
RTT	Real Time Ttolerant
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol for Traffic Engineering
RSVP	Resource Reservation Protocol
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
ToS	Type of Service
TTL	Time to Live
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VWQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
WRED	Weighted Random Early Detection

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO DVD

- **Config** – konfigurační soubory pro tester Trend Multipro
  - data
    - `ftp-lab-bars.xml` – konfigurační soubor FTP aplikace.
  - video
    - `video-lab-bars.xml` – konfigurační soubor video aplikace.
  - voip
    - `voip-lab-bars.xml` – konfigurační soubor VoIP aplikace.
- **Video**
  - `video_TS1.ts` – video kódované kodekem MPEG-2.
  - `video_TS2.ts` – video kódované kodekem MPEG-4 AVC.
- **WANem**
  - `WANem PC.ova` – virtuální stanice WANem.
  - `WANem_3.0_Beta.iso` – bootovací disk s WANem emulátorem.

- `BP_Gregor.pdf` – elektronická verze bakalářské práce.
- `Lab_studentsky_manual.pdf` – návod k vypracování laboratorní úlohy pro studenty.
- `Lab_ucitelsky_manual.pdf` – návod k sestavení a konfiguraci laboratorní úlohy pro vyučující.
- `Lab_vzorovy_protokol.pdf` – vzorově vypracovaný protokol.
- `Lab_zaznamovy_arch.xlsx` – tabulkový soubor pro záznam naměřených hodnot.
- `Lab_zaznamovy_arch_vzorovy.xlsx` – vzorový tabulkový soubor pro záznam naměřených hodnot.
- `Multipro_manual.pdf` – návod k testeru Trend Multipro.