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

OVĚŘOVÁNÍ STABILNÍHO PROVOZU SÍTĚ NOVÉ GENERACE MĚŘENÍM PŘENOSOVÝCH PARAMETRŮ

VERIFICATION OF STABLE NEXT GENERATION NETWORKS VIA TRANSMISSION PARAMETERS MEASUREMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Lukáš Gregor**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. David Grenar**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Lukáš Gregor ***ID:*** 160800
Ročník: 2 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Ověřování stabilního provozu sítě nové generace měřením přenosových parametrů

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s měřením parametrů provozu na přístupových sítí nové generace. Popište jednotlivá doporučení a standardy pro konkrétní typ sítí nových generací. Definujte metodiku pro datové přenosy, služby v reálném čase a přenosy s požadavky na vysokou prioritu. Dále proveďte testování dle EtherSAM, RFC 2544, ExacTCP a ověření Traffic Engineeringu. Na základě experimentálního měření navrhněte pro daný typ nejvhodnější metodiku měření.

DOPORUČENÁ LITERATURA:

[1] FILKA, Miloslav. Optoelektronika pro telekomunikace a informatiku. Brno: M. Filka, 2009. ISBN 978-808-67-5-141.

[2] SPORTACK, Mark A. Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]. Brno: Computer Press, 2004. Cisco systems. ISBN 80-25--0127-4.

[3] LAFATA, Pavel a Jiří VODRÁŽKA. Optické přístupové sítě a přípojky FTTx. Praha: České vysoké učení technické v Praze, 2014. ISBN 978-800-1054-635.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 21.5.2018

Vedoucí práce: Ing. David Grenar
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Tato diplomová práce se zabývá měřením přenosových parametrů v přístupových sítích nové generace NGA. Cílem práce je sestavení a konfigurace testovací sítě a scénářů pro měření kvalitativních parametrů služeb a následné ověření stability přenosu. V teoretické části práce je popsáno obecné fungování sítí NGN, požadavky různých telekomunikačních služeb na kvalitativní parametry, metodika a doporučení pro měření přenosových parametrů v paketových sítích. Praktická část se zabývá konfigurací scénářů využívajících různé technologie a metodikou jejich testování. Měření bylo provedeno dle standardů IETF RFC 2544, IETF RFC 6349 testem ExacTCP a ITU-T Y.1564 testem EtherSAM. Pro měření byly využity měřící přístroje značky EXFO. Závěrem byly zhodnoceny výsledky měření scénářů dle uvedených doporučení a diskutována výhodnost využití těchto doporučení pro testování přístupových sítích NGA.

KLÍČOVÁ SLOVA

IP, NGN, NGA, IETF RFC 2544, IETF RFC 6349, ITU-T Y.1564, MEF 23.1, kvalita služeb, QoS, triple play, latence, kolísání zpoždění, ztrátovost paketů, datová propustnost

ABSTRACT

This thesis deals with the measurement of transmission parameters in the new generation access networks NGA. The aim of the thesis is to build and configure a test network and scenarios for the measurement of service quality parameters and then verify the transmission stability. The theoretical part describes general functioning of NGN networks, the requirements of different telecommunications services on quality parameters, methodology and recommendations for measuring transmission parameters in packet networks. The practical part deals with the configuration of scenarios using mainly MPLS technology and methodology of their testing. Measurements were performed according to recommendations IETF RFC 2544, IETF RFC 6349 with the ExacTCP test and ITU-T Y.1564 with the EtherSAM test. For measurements were used measuring instruments of EXFO brand. In conclusion, the measurement results according to the mentioned standards were evaluated and also the advantages of using the measurement according to the given standard in NGA access networks were discussed.

KEYWORDS

IP, NGN, NGA, IETF RFC 2544, IETF RFC 6349, ITU-T Y.1564, MEF 23.1, quality of services, QoS, triple play, latency, jitter, packet loss, throughput

GREGOR, Lukáš. *Ověřování stabilního provozu sítě nové generace měřením přenosových parametrů*. Brno, 2018, 87 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. David Grenar

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Ověřování stabilního provozu sítě nové generace měřením přenosových parametrů“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících 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 ....

Bc. Lukáš Gregor

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Davidu Grenarovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

Bc. Lukáš Gregor

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

Brno ....

Bc. Lukáš Gregor

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V důsledku rychlého technologického vývoje a rostoucích požadavků koncových uživatelů se očekává, že současné informační a komunikační služby budou přesunuty do sítí nové generace – NGN (Next Generation Network), v nichž bude komunikace probíhat nezávisle kdykoliv a odkudkoliv. Síť NGN využívá hlavních výhod datových sítí založených na IP (Internet Protocol) protokolu a PSTN (Public Switched Telephone Network) sítí založených na přepojování fyzických okruhů. Snahou je tedy vytvořit širokopásmovou síť nezávislou na přenosové technologii, umožňující konvergenci a paketový přenos rozmanitých aplikačních služeb datovou sítí pomocí IP protokolu. Hlavním cílem nasazení NGN sítí je tedy zvýšení rychlosti a dostupnosti datových přenosů, snížení provozních nákladů a jednoduchá správa sítě a datových toků. [5]

Původní jednoduchý model internetu založený na principu doručování paketů s největším úsilím, tzv. best–effort, disponující pouze omezenými možnostmi řízení datových toků se ukázal jako nedostačující. S nárůstem datových toků bylo nutné zavést jisté zásady pro zajištění kvality poskytovaných telekomunikačních služeb – QoS (Quality of Services). Tyto zásady umožňují v síti klasifikaci datových toků a stabilní provoz rozmanitých aplikačních služeb. Cílem je poskytnout koncovému uživateli různé datové služby v určité kvalitě a za přijatelnou cenu s ohledem na kritické parametry a kapacitu sítě. Mechanizmy QoS jsou v NGN sítích mimo jiné doplněny také protokoly nové generace, IPv6 protokoly a protokoly zajišťující bezpečnost a mobilitu účastníků. [21]

Výše zmíněné protokoly, mechanizmy a modely jsou vyvíjeny telekomunikačními standardizačními organizacemi jako např. ITU–T, IETF, ETSI, 3GPP a dalšími, a bude o nich pojednáno v následujících kapitolách práce. Dále budou popsány známá doporučení pro měření parametrů provozu v přístupových sítí nové generace a vliv různých metrik na kvalitu služeb. Závěrečná kapitola obsahuje návrh testovacích scénářů využívajících různé síťové technologie, jejich testování dle známých doporučení, vyhodnocení naměřených dat a porovnání využitých telekomunikačních standardů.

1 DEFINICE SÍTÍ NOVÉ GENERACE

Sítě nové generace vznikly spojením a kombinací výhod klasických telefonních PSTN sítí s přepojováním fyzických okruhů a datových sítí založených na protokolu IP. Výsledkem tohoto spojení je širokopásmová síť NGN umožňující vysokorychlostní paketový přenos informací a poskytování širokého spektra telekomunikačních služeb. Přístupové sítě nové generace jsou v terminologii NGN sítí nazývány jako NGA – Next Generation Access. [5]

Oficiální definice sítí NGN, publikovaná standardizační organizací ITU–T uvádí, že se jedná o vysokorychlostní paketově orientovanou síť umožňující poskytnout koncovým uživatelům telekomunikační služby v určité kvalitě, s podporou QoS mechanizmů. Paketový přenos dat je charakteristický pro přístupové i transportní sítě. Síť nové generace též umožňuje sloučení několika nezávislých sítí pro přenos různých hlasových, obrazových či datových služeb do jednotné širokopásmové sítě, která je nezávislá na přenosové technologii. Uživatelům je umožněn neomezený přístup ke službám dle svého výběru. Samozřejmostí je také podpora mobility, která umožní konzistentní využívání služeb odkudkoliv a kdykoliv. Dle organizace ITU-T je tedy síť NGN charakterizována následujícími aspekty: [12]

- paketový přenos dat,
- oddělení řídících funkcí,
- podpora široké škály služeb, aplikací a mechanizmů, včetně služeb v reálném čase, streamingu, multimediálních a ostatních služeb neprobíhajících v reálném čase,
- širokopásmové připojení s podporou end–to–end QoS,
- podpora spolupráce se staršími sítěmi prostřednictvím otevřených rozhraní,
- mobilita a neomezený přístup uživatelů ke službám různých poskytovatelů,
- konvergované služby mezi pevnými a mobilními sítěmi,
- nezávislost služeb na přenosové technologii,
- podpora více technologií přístupových sítí.

Z výše uvedených bodů vyplývá, že hlavním cílem sítí NGN je konvergence služeb. Při procesu konvergence se využívají klasické technologie a technologie založené na otevřených standardech a rozhraních. Využití otevřených standardů dává možnost připojení různých druhů komunikačních systémů a funkcí s nimi spojených. To vše umožňuje operátorům snížení provozních nákladů a možnosti nabídnout koncovým zákazníkům širokou nabídku poskytovaných služeb bez ohledu na to, zda využívají přenos služeb přes mobilní nebo pevnou síť. [5]

1.1 Konvergence

Konvergence IP technologií je v dnešní době již široce rozšířená a využívaná. Typickým příkladem je konvergence hlasových a datových služeb viz podkapitola 1.1.1 níže. Konvergence umožňuje integraci stávajících hlasových a datových sítí do jedné komunikační sítě založené na protokolu IP. Hlavní výhodou konvergence těchto technologií je jednoduché rozšíření stávající sítě, a také jednoduchá a transparentní správa této konvergované sítě. Tyto sítě jsou potom nazývané NGN/NGA. [5]

Praktická realizace je poté založena na realizaci spojení mezi několika různými vrstvami síťové infrastruktury. Nezbytná je také konvergence přístupových sítí a účastnických terminálů, aby bylo možné přistupovat k různým typům služeb a sítí bez negativních dopadů na kvalitu služby QoS. [5]

Výsledkem konvergence by tedy měla být jednotná síť umožňující integraci veškerých současně dostupných telekomunikačních sítí jako PSTN, ISDN, IP, ATM, Frame Relay včetně technologie MPLS. [5]

Součástí konvergence je také konvergence telekomunikačních služeb. Konvergence služeb umožňuje využití telefonních, datových, textových a jiných telekomunikačních služeb z jediného účastnického terminálu, což je velká výzva pro operátory, poskytovatele služeb a vývojáře.

1.1.1 Konvergence telefonních a datových sítí

Porovnáním telefonních a datových sítí lze rozlišit několik základních odlišností. Klasické telefonních sítě pracují na principu časového dělení TDM – Time Division Multiplex, kde dochází k periodickému střídání jednotlivých účastnických kanálů v přesně definovaných krátkých časových periodách. Dochází tedy k vytvoření pevného fyzického spojení (okruhu) mezi komunikujícími účastníky, které je udržováno po celý čas relace. Nevýhodou je, že spojení zůstává aktivní i v okamžicích, kdy není přenášen užitečný obsah (např. uživatel mlčí), čímž dochází k blokování kapacity kanálu pro ostatní účastníky služby. Tyto sítě, obecně nazývané jako PSTN, se vyvinuly z původních analogových sítí na digitální sítě ISDN (Integrated Services Digital Network) [20]. Problém trvalého blokování přenosové kapacity po celou dobu relace je v datových sítích založených na protokolu IP ošetřen paketovým přenosem dat. Užitečné informace jsou tedy zabaleny do paketů a přenášeny sítí. Díky přenosu pouze užitečných informací je tak datový tok výrazně menší než u sítí PSTN a zbývající přenosová kapacita trasy tak může být využita pro stejného, nebo jiného poskytovatele služeb [5]. Další odlišností plynoucí z charakteru jednotlivých sítí je spolehlivost přenosu informací, hrající ve prospěch telefonních sítí. Díky rezervaci celého přenosového okruhu pro dané spojení mezi dvěma účastníky je zaručena prů-

chodnost, zpoždění a konstantní šířka přenosového pásma. To v datových sítích pracujících na principu snahy doručení s nejlepší možnou kvalitou není možné bez aplikace mechanizmů QoS [20]. Následkem konvergence hlasových sítí a datových sítí tak mohou vznikat nové aplikace jako například použití systémů PBX pro IP telefony nebo řešení pro call centra a rozsáhlé podnikové sítě.

1.2 Architektura NGN založená na IMS

Základem této varianty architektury jsou IP subsystémy multimédií – IMS (IP Multimedia Subsystems) tvořené aplikačními servery. IMS tedy zahrnuje veškeré elementy pro poskytování IP multimediálních služeb (audio, video, text, chat, apod.). Tyto subsystémy jsou založené na architektuře IP. Subsystémy jsou umístěny jako nosné prvky sítě, které mají poskytovat standardizované služby pro mobilní uživatele. Hlavními výhodami IMS jsou snadná rozšiřitelnost, možnost přizpůsobení těchto sítí konkrétním podmínkám podle potřeby a nižší počet řídících prvků [5]. Díky těmto výhodám se IMS stala referenčním bodem, ze kterého se dále vyvíjely architektury založená na jejím principu, jako např. 3GPP IMS nebo nejnovější ETSI TISPAN. [19]

Hlavním počinem 3GPP bylo převzetí a úprava původního protokolu SIP (Session Initiation Protocol) standardizovaného v IETF, který nesplňoval veškeré požadavky potřebné pro nasazení v síti IMS. Bylo tedy nutné provést několik přepracování, ze kterých vznikl komplexní protokol IMS SIP. V protokolu IMS SIP dochází zejména k rozšíření funkcí pro správu hovoru, virtuální přítomnost a okamžité zprávy. Výhodou protokolu SIP je jeho modifikovatelnost. Protože není navržen pro specifickou aplikaci a síť, lze pro něj definovat uživatelské profily, což je velkým přínosem pro telekomunikační průmysl. [19]

2 KVALITA SLUŽEB V DATOVÝCH SÍTÍCH

V IP sítích rozlišujeme dva základní modely pro hodnocení kvality služeb. První QoS model založený na metrikách je určen pro vyhodnocení technických parametrů sítí. V případě QoS modelu však nelze zjistit, jak kvalita dané služby uspokojila koncového zákazníka. Tímto problémem se zabývá disciplína QoE (Quality of Experience). Oba modely spolu úzce souvisí. Pokud vhodně aplikujeme na daný typ provozu zásady QoS, bude pozitivně ovlivněna kvalita služby vnímaná koncovým uživatelem.

2.1 Quality of Services – QoS

Kvalita přenosu dat komunikační sítí je definována řadou parametrů popisujících datový přenos, které reflektují zejména technickou vyspělost síťových prvků. Tyto parametry se nazývají metriky. Vhodnou aplikací mechanizmů QoS (DiffServ, IntServ, MPLS) lze dosáhnout lepších hodnot daných metrik a s tím spojeným zlepšením vnímané kvality služby. Při aplikaci těchto zásad je nutné nejprve identifikovat a klasifikovat provoz v síti a jeho požadavky na QoS, a následně stanovit, jak s tímto typem služby zacházet v síti nadále. Nevhodná, či vůbec žádná, implementace těchto mechanizmů může v krajním případě způsobit i nepoužitelnost dané služby. Metriky jsou často spojovány se službami probíhajícími v reálném čase, tzv. real-time službami, které jsou jimi ovlivněny nejvíce. Zjednodušeně lze tedy říci, že metriky charakterizují stav dat přenášených v síti ovlivněný výkonem, který QoS poskytuje. Mezi základní metriky patří:

- komunikační zpoždění – Delay (D) [ms],
- kolísání zpoždění – Jitter (J) [ms],
- datová propustnost – Throughput [kb/s],
- ztrátovost paketů – Packet Loss Rate [–]

2.1.1 Komunikační zpoždění

Komunikační zpoždění (D) je v telekomunikacích chápáno jako jednosměrné zpoždění udávané v ms, které vyjadřuje čas potřebný k zpracování a přenesení dat komunikační sítí od zdroje k cíli (tzv. end-to-end) [24]. Než data doputují od zdroje k cíli, mohou být na své cestě převedena z analogové do digitální podoby, komprimovaná, vkládána do paketů, nebo zdržena při odbavování a zpracování na síťových prvcích. Suma těchto dílčích zpoždění tvoří celkové komunikační zpoždění.

Zpoždění v datových sítích lze rozdělit podle několika kritérií. Nejčastějším rozdělením je podle časové proměnlivosti a předvídatelnosti následovně [3]:

- Fixní zpoždění (D_d, deterministické) – je předvídatelné a v čase neměnné. Tvořeno fixními komponentami sítě.
- Variabilní zpoždění (D_s, stochastické) – je proměnlivé v čase a obtížně předvídatelné.

Dalším možným rozdělením je rozdělení zpoždění podle přenosových komponent, které zpoždění vyvolaly takto [1]:

- Zpoždění vzniklé zpracováním (D_p, processing delay) – vyjadřuje čas potřebný pro zpracování paketu v každém uzlu sítě. Je ovlivněno použitými protokoly a výpočetním výkonem uzlů. Jelikož se proměnlivá složka odvíjí od aktuálního vytížení uzlu, tak lze rozlišit fixní D_{pd} a variabilní D_{ps} zpoždění vzniklé zpracováním.
- Zpoždění přenosem D_t – vyjadřuje zpoždění vzniklé přenosem paketu. Je determinováno rychlostí linky a pro stejně dlouhé pakety je konstantní. Označováno jako transmission delay.
- Propagační zpoždění (D_{pr}) – charakterizuje čas, za který je přenesen jeden bit komunikačním kanálem. V paketových sítích zanedbatelné.
- Zpoždění ve frontách (D_q) – queuing delay vyjadřuje dobu, kterou paket stráví ve frontách síťových prvků.

Pro výpočet fixního zpoždění 2.1 a variabilního zpoždění 2.2 lze definovat následující vztahy [1]:

$$D_d = D_{pd} + D_t + D_{pr} \qquad [\text{ms}] \tag{2.1}$$

$$D_s = D_q + D_{ps} \qquad [\text{ms}] \tag{2.2}$$

Často se lze setkat se zaměněním pojmu *delay* za pojmy *latence* a RTT (Round-Trip Time), které však vyjadřují obousměrné zpoždění ve směru od odesílatele k příjemci a zpět [24].

2.1.2 Kolísání zpoždění

Pakety jsou ze strany odesílatele vysílány rovnoměrně v pravidelných časových intervalech po sobě. V ideální síti by ve stejných časových intervalech za sebou přišli k příjemci. To však není v reálné síti možné zaručit. Při přenosu může dojít k narušení rovnoměrnosti zpoždění mezi pakety, které může být způsobeno vlivem zatížení sítě, zdržením se paketu ve frontách síťových prvků, nebo špatnou konfigurací sítě.

Jitter i-tého paketu je definován jako absolutní hodnota rozdílu jednosměrného zpoždění daného paketu D_i a paketu předcházejícího D_{i-1} [3].

$$J_i = |D_i - D_{i-1}| \qquad [\text{ms}] \tag{2.3}$$

Jitter silně ovlivňuje real-time služby. Pro jeho potlačení se na přijímací straně využívá vyrovnávací paměť, tzv. de-jitter buffer.

Kolísání zpoždění bývá mnohdy chybně zaměňováno s metrikou variace ve zpoždění PDV (Packet Delay Variation). PDV vyjadřuje rozdíl jednosměrného zpoždění zvoleného paketu a referenčního zpoždění, přičemž nejsou uvažovány ztracené pakety [3].

$$PDV_i = |D_i| - |D_{ref}| \qquad [\text{ms}] \tag{2.4}$$

2.1.3 Datová propustnost

Datová propustnost vyjadřuje objem dat, které lze přenést přenosovým kanálem za jednu sekundu. Často se nepřesně užívá pojem šířka pásma, která souvisí spíše s analogovými signály, kde je uváděna v Hz. V telekomunikačních systémech je vhodné využít pojmu datová propustnost, která je udávaná zejména v kb/s, Mb/s a Gb/s.

2.1.4 Ztrátovost a chybovost paketů

Při překročení kapacity sítě může dojít k zahození paketů vlivem přetečení front síťových prvků, nebo nesprávnému zpracování a směrování paketů. Částečně tomu lze zabránit již při konfiguraci síťových prvků a návrhu sítě.

Důležitou metrikou je v tomto ohledu bitová chybovost BER (Bit Error Rate), která je charakteristická pro přenosy s nepřetržitým datovým tokem a od ní odvozená paketová chybovost PER (Packet Error Rate). BER je udávaná v procentech a vyjadřuje poměr chybně přenesených bitů ku celkovému počtu přenesených bitů. Obdobně tedy PER vyjadřuje poměr chybně přenesených paketů ku celkovému množství přenesených paketů a je udávaná též v procentech. Za chybně přenesený paket lze považovat paket, který byl:

- zahozen,
- přijat s chybami,
- přijat několikanásobně,
- směrován jinam.

2.2 Quality of Experience – QoE

Telekomunikační společnosti investují mnoho prostředků na analýzu spokojenosti uživatelů s poskytovanou službou – QoE. Hlavním cílem výzkumu QoE koncových zákazníků je dosáhnout vyváženého poměru mezi kvalitou poskytované služby, spokojeností koncových zákazníků se službou a v neposlední řadě cenou. QoE tedy

vyjadřuje subjektivní dojem uživatele z poskytované služby. Výsledná QoE je ovlivněna následujícími faktory [15].

1. Kvalitou zdrojového audia/videa.
2. QoS parametry.
3. Lidským vnímáním.

Kvalita zdrojového videa je ovlivněna např. použitými kodeky, nebo bitovou rychlostí nahrávky. QoS parametry charakterizující přenos již byly popsány v předchozí kapitole 2.1. Velmi specifický je však lidský faktor, který nelze jednoduše kvantifikovat. Lidské vnímání je silně ovlivněno sociálním faktorem a také předchozími zkušenostmi účastníků se službou.

Pro vyhodnocení QoE se zpravidla používá dvou parametrů, které lze mezi sebou navzájem přepočítat. Jedná se o MOS faktor a R faktor.

2.2.1 MOS

MOS charakterizuje na stupnici 1 až 5 lidské vnímání kvality poskytované služby. Jednotlivé stupně jsou doplněny slovním vyjádřením kvality, kdy 1 = bad, 2 = poor, 3 = fair, 4 = good, 5 = excellent. Pro představu je například pro VoIP hovory doporučována hodnota MOS alespoň 4,4. Pod hodnotu MOS = 3 už bývají zejména real-time služby nepoužitelné a např. pro VoIP telefonii dochází ke ztrátě porozumění mezi účastníky relace. [24]

Parametr MOS lze v základu získat pomocí dvou metod hodnocení služby. Jedná se o metody subjektivní a objektivní.

Subjektivní hodnocení kvality služby se provádí za pomoci reprezentativního vzorku uživatelů, kteří hodnotí kvalitu služby. Požadavky pro výběr vzorku respondentů a metodika testování jsou popsány ve standardu ITU-T P.800.1. I přesto, že se jedná o hodnocení nejpřesnější, tak v praxi není díky své cenové a časové náročnosti využívané.

Objektivní hodnocení staví na matematických algoritmech pro výpočet MOS. Zpravidla bývá výpočet založený na analýze chyb v přijatém datovém toku vůči referenčnímu datovému toku, nebo odhadu na základě QoS parametrů.

2.2.2 E-model

Druhou možnou metodou pro vyhodnocení QoE je odhadový E-model, jehož výstupní hodnotou je R-faktor. Na rozdíl od MOS charakterizuje celý přenosový kanál od zdroje k cíli, včetně účastnických terminálů a rušení. R faktor nabývá hodnot od 0 po 100, ale kvůli použitelnosti služeb uvažujeme pouze 50–100. Výsledný faktor R

lze popsat rovnicí 2.5

$$R = R_0 - I_S - I_D - I_E + A \qquad [-] \quad , \tag{2.5}$$

kde R_0 vyjadřuje hodnotu odvozenou ze SNR, I_S lineární zkreslení vzniklé přenosem hlasu, I_D zkreslení vzniklé zpožděním, I_E vliv kodeku a A zohledňuje výhody různých terminálů (pevný $A = 0$, mobilní GSM $A = 10$). [23, 8]

Faktor R a MOS lze mezi sebou vzájemně přepočítávat. V tabulce 2.1 je uvedeno porovnání obou parametrů vzhledem ke spokojenosti zákazníků se službou.

Tab. 2.1: Porovnání stupnic uživatelské spokojenosti pomocí MOS a R. [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 Požadavky služeb na QoS/QoE

Různé telekomunikační služby se odlišují specifickými požadavky na zpoždění, jitter, propustnost a ztrátovost paketů. Při nedodržení těchto kritických hodnot dochází k degradaci kvality služby, nebo může nastat úplný výpadek služby. Obzvlášť specifickými nároky se vyznačují multimediální služby pracující v reálném čase, které k přenosu dat často využívají transportního protokolu UDP.

2.3.1 VoIP telefonie

Pro přenos dat se využívá nespolehlivý transportní protokol UDP, u kterého nedochází k potvrzování přijetí dat a opakovanému přenosu chybně přenesených či nedoručených dat. Samotná hlasová informace je přenášena pomocí aplikačního protokolu RTP (Real-Time Protocol). Služba VoIP vyžaduje vysoké nároky zejména na zpoždění a jitter. Doporučení ITU-T G.114 uvádí, že pro VoIP telefonii je přijatelná hranice jednosměrného zpoždění mezi 150 ms a 400 ms. Pokud je zpoždění nižší, hovor je považován za velice kvalitní. Naopak při zpoždění větším než 400 ms dochází k problémům s porozuměním mezi účastníky hovoru, nebo k úplnému výpadku spojení [22].

VoIP hovory ovlivňuje také ztrátovost paketů. Ta by se v ideálním případě měla pohybovat do 1 %. Přijatelné jsou však hodnoty až do 2 %. Pro ztrátovost je velmi

důležitá vhodná volba kodeku. Kodeky totiž využívají různé metody pro maskování účinku ztracených nebo zahozených paketů [22].

Pro docílení ideálního nastavení služby je nutné vhodně nastavit velikosti dejitter bufferu, který slouží pro vyrovnání odlišného zpoždění jednotlivých paketů jdoucích po sobě. Dejitter buffer mění kolísavé zpoždění na konstantní zpoždění. Nesprávně nastavený buffer může způsobit jeho přetečení či podtečení, a tím zvýšit celkové zpoždění end-to-end. Hodnota jitteru by pro správnou funkci služby neměla přesahovat 30 ms [22].

Pro VoIP hovory je vyžadována datová propustnost mezi 21 až 320 kb/s, jejíž konkrétní velikost z rozsahu se liší podle použitého kodeku, vzorkovací frekvence a režie linkové vrstvy ISO/OSI modelu. Provoz VoIP by měl být v datových sítích s mechanizmy DiffServ značkovaný s nejvyšší prioritou EF (Expedited Forwarding) označenou v poli DSCP [22].

2.3.2 Video streaming

Video streaming nevyžaduje nízké hodnoty zpoždění a obecně vykazuje spíše mírné požadavky na QoS. Zpoždění se pohybuje okolo 4-5 sekund, což na přijímací straně umožňuje využít větších vyrovnávacích pamětí. Využití velkých vyrovnávacích pamětí má za následek to, že video stream není takřka vůbec citlivý na jitter. Ztrátovost paketů by se pro správnou funkci služby měla pohybovat do 5 % [22].

V sítích s nasazeným QoS mechanizmem diferencovaných služeb je doporučené využit značkování DSCP CS4 (Class Selector 4) [22].

2.3.3 Videokonference

Pro videokonference by měla být deklarována ztrátovost paketů do 1 %, jitter do 30 ms a jednosměrné zpoždění do 150 ms, obdobně jako je tomu u VoIP telefonie. Doporučené značkování pro normální videokonference je DSCP AF41 (Assured Forwarding). Pro datově náročné videokonference je vhodné snížit prioritu na DSCP AF42 nebo AF43 [22].

2.3.4 Služby přenosu dat

Pro služby přenosu dat (e-mail, databázové služby, FTP, internetové bankovnictví, atp.) se využívá transportní protokol TCP. Ten umožňuje spolehlivý přenos dat na úkor vyššího zpoždění. V případě služeb přenosu dat vyžadujeme, aby data byla přenesena všechna, tedy bez jakékoliv ztráty paketů, které nejsou tolerovány už z principu protokolu TCP. Pokud dojde při přenosu k chybě, nastává opakovaný přenos dat. Data jsou přenášena s využitím zbývající šířky pásma [22].

2.3.5 Online gaming

Jedná se o interaktivní hry, které využívají datovou síť pro interakci s ostatními hráči. Požadavky na interaktivní hry jsou specifické v závislosti na zvolené hře. Zpravidla jsou závislé zejména na zpoždění a šířce pásma. Během relace může docházet k přenosu velkého objemu dat. Vysoké hodnoty zpoždění např. nad 150 ms nemusí být herními servery tolerovány a může dojít k vyloučení hráče z relace. Vysoké zpoždění také snižuje požitek ze hry, kdy může docházet např. k trhavému pohybu, v hráčském prostředí označovaném jako „lagy“.

2.3.6 Web-browsing

Pro služby vyhledávání na internetu pomocí webového prohlížeče je důležitá doba odezvy, za kterou se načte požadovaná stránka. Přijatelné hodnoty jsou okolo 2-4 sekund, ideální je však doba okolo 0,5 sekundy [22]. Využívá se transportního protokolu TCP a není tedy tolerována žádná ztráta dat.

2.3.7 IPTV

Jedná se o službu poskytovanou operátory v rámci triple play služeb (VoIP telefonie, data, IPTV), kdy jsou QoS priority řešené pro každou službu zvláště. IPTV umožňuje sledování televizního vysílání přes protokol IP. Pro příjem musí být uživatel (uživatelský přijímač) přihlášený do multicastové skupiny, neboť přenos probíhá pomocí multicastového vysílání. IPTV je relativně náročná na šířku pásma. V podstatě se jedná o audio-video stream, jehož šířka pásma je silně ovlivněna použitými kodeky. Při přenosu může vlivem např. interferencí docházet ke ztrátám paketů či chybám v paketech, které snižují požitek ze služby. Pro částečné odstranění chyb jsou přijímače vybyveny FEC dekodéry. Doporučená hodnota zpoždění je 200 ms a jitteru do 50 ms [22].

2.4 QoS mechanizmy a traffic engineering

V současných paketových sítích můžeme rozlišit několik úrovní kvality služeb QoS. Těchto úrovní je dosaženo za využití odlišných modelů pro zajištění kvality služeb. QoS modely pracují zejména na síťové vrstvě referenčního modelu OSI/ISO, přičemž některé zásady lze aplikovat i na linkové vrstvě. Popsány budou pouze mechanizmy a technologie využité v praktické části diplomové práce, kterými jsou:

- Best-effort,
- Differencované služby – DiffServ,
- Multiprotokolové přepínání podle návěští – MPLS.

2.4.1 Best-effort

Jedná se o základní model, na kterém byl vybudován internet, a který je dodnes využíván ve značné části sítí. Jak již z názvu vyplývá, tento model se snaží data doručit k cíli co nejrychleji, tedy „s největším úsilím“, bez využití QoS politiky a jakýchkoli garancí. Nedochází ke klasifikaci datových toků a nelze tak prioritizovat určité služby.

V moderních datových sítích je pro zajištění jejich stability a předvídatelné funkce nutné přistoupit k aplikace sofistikovanějších mechanizmů pro zajištění kvality služeb.

2.4.2 Diferencované služby – DiffServ

Mechanizmus DiffServ (DS) byl vyvinut, aby poskytoval různé způsoby zacházení s pakety na směrovačích, a tím i různé úrovně kvality služeb pro rozmanitý síťový provoz. Snahou bylo vytvořit model, který by podporoval širokou škálu aplikací a vyhověl jejich specifickým požadavkům. Tento mechanizmus neumožňuje rezervaci síťových prostředků podél celé přenosové cesty, což představuje nižší zatížení síťových prvků a větší flexibilitu systému. S paketem je individuálně zacházeno dle pravidel domény na každém směrovači v cestě, tzv. „per-hop“.

DiffServ doména

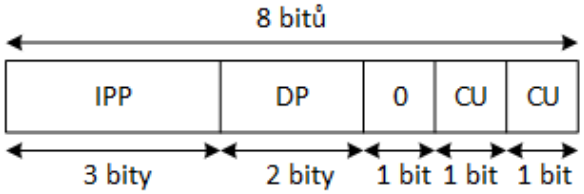
V rámci mechanizmu DS je síť dělena do menších autonomních oblastí s vlastní politikou, tzv. DS domén, ve kterých směrovače dělíme na hraniční a vnitřní.

Hraniční směrovače se nachází na vstupu do DS domény. Jejich úlohou je klasifikace datových toků a přidělení síťových prostředků na základě příslušnosti datového toku k třídě, která je indikována v poli DSCP. Při vstupu paketu do DS domény můžeme rozlišit dva typy případů. 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 pakety mají stejný identifikátor, není třeba nic měnit. V případě stejných pravidel, ale odlišných identifikátorů stačí pouze aktualizovat identifikátor. Může však nastat případ, že v obou doménách budou zcela odlišná pravidla. Potom je tedy nutné přeznačkovat identifikátor dle pravidel DS domény, do které paket vstupuje.

Vnitřní směrovače již žádné značkování neprovádí. Příchozí pakety řadí do tříd a front podle DSCP značky přidělené hraničními směrovači.

DSCP (Diferentiated Services Code Point)

DSCP je název pro prvních 6 nejvýznamnějších bitů nacházejících se v jednobajtovém poli ToS (Type of Service) IPv4 paketu. V případě mechanizmu diferencovaných služeb je toto pole nazýváno DiffServ pole. Pro IPv6 paket je pole ToS nazýváno CoS (Class of service).



Obr. 2.1: DiffServ pole.

První 3 nejvýznamnější bity IPP (IP Precedence) značí prioritu přenášených dat a jsou plně kompatibilní s IP Precedence dle standardu IETF RFC 1349. Další 3 bity se nazývají Class Selector, z nichž první dva významnější bity značí pravděpodobnost zahození paketu (DP – Drop Probability) a nejméně významný bit této trojice má vždy hodnotu 0. Dva nejméně významné bity (CU – Currently Unused) oktetu nejsou dle standardu IETF 2474 definovány a využívány. Novější standard IETF RFC 3168 upravuje jejich využití pro signalizaci přetížení mezi koncovými uzly ECN – Explicit Congestion Notification [2].

Pomocí zmíněných 6 bitů může tedy DSCP pole nabývat hodnot 0–63, což značí, že jednotlivé služby lze rozdělit až do 64 tříd. Výchozí hodnotou DSCP je 000000 značící třídu best-effort a tedy nejnižší prioritu.

2.4.3 MPLS

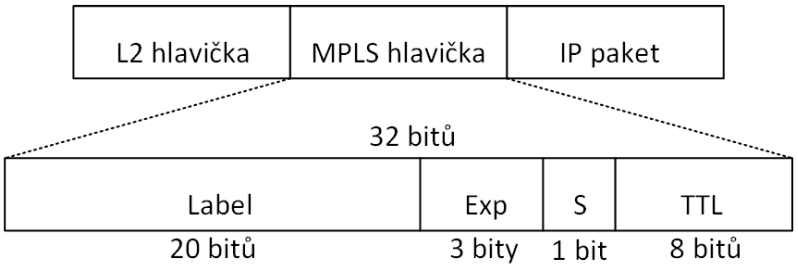
Technologie MPLS (Multi Protocol Label Switching) kombinuje výhody IP sítí a sítí ATM. Z IP sítí přebírá jednoduchost a snadnost implementace protokolů. Ze sítí ATM potom techniky řízení síťového provozu. Z pohledu referenčního modelu OSI/ISO pracuje MPLS mezi síťovou a linkovou vrstvou, díky čemuž bývá MPLS označováno jako vrstva 2,5.

Jedná se o protokolově nezávislou technologii s cílem maximálně zjednodušit směrování paketů a optimalizovat rozdělení zátěže v síti, tzv. traffic engineering (TE). Paketům je přiděleno návěští (label), podle něhož probíhá následné směrování. Není tak třeba kontrolovat celý paket, ale pouze návěští paketu, díky čemuž odpadá také nutnost kontrolovat směrovací IP tabulky na směrovačích v rámci domény.

MPLS doména

Na vstupu do MPLS domény se nacházejí hraniční směrovače LERs (Label Edge Routers), jejichž úkolem je klasifikace datových toků, přidělení návěští příchozím paketům a odebrání návěští paketům opouštějících doménu. Mezi LERs, uvnitř MPLS domény, se nachází směrovače LSRs (Label Switching Routers). Jednoduché MPLS tabulky na směrovačích podle vstupní hodnoty návěstí určují, kudy bude 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 je pak vytvořen tak, že se všechny LSR vytvoří vazbu mezi příchozím a odchozím návěštím pro datové toky v rámci FEC.

O distribuci návěští v MPLS doméně se v základní implementaci stará protokol LDP (Label Distribution Protocol). Při využití traffic engineeringu je LDP nahrazen protokolem RSVP-TE



Obr. 2.2: Hlavička MPLS paketu.

- **Label** – pole nesoucí aktuální hodnotu návěští.
- **EXP** – *Experimental* slouží pro experimentální využití, nebo lze využít pro nastavení QoS.
- **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.

2.4.4 VPLS (Virtual Private LAN Service)

VPLS je technologie virtuální privátní sítě na linkové vrstvě (L2VPN) založená na principech MPLS, jejíž účelem je poskytnout vícebodovou privátní službu typu ethernet. V podstatě se jedná o emulovanou lokální síť LAN nad MPLS. O distribuci návěští se obdobně jako u MPLS stará protokol LDP.

Technologie VPLS přináší způsob, jak doručit mnohabodovou transparentní službu na úrovni L2 přes ethernet infrastrukturu za pomoci MPLS. Zjednodušuje se tak hranice mezi zákazníkem a poskytovatelem služeb, což umožňuje rychlé a flexibilní poskytování služeb. Všechny služby ve VPLS se zdají být ve stejné síti LAN bez ohledu na jejich umístění.

Výhodou VPLS je možnost sdílení broadcastové domény geograficky odděleným místům tak, že tato místa propojí pomocí pseudovláken PW (Pseudo Wires). PW jsou vytvořeny mezi všemi hraničními směrovači PE, které náleží dané instanci. Síť VPLS pak emuluje jediný přepínač či most, a zdánlivě je vytvořena jedna síť LAN. Nevýhodou je, že pro n VPLS instanci musí být sestaveno n*(n-1)/2 PW mezi PE směrovači, což s sebou přináší velkou režii.

2.4.5 MPLS-TE

MPLS-TE (Traffic Enginneering) je zásadní pro poskytovatele služeb (ISP), protože podporuje vysoké využití přenosové kapacity. Taková síť se také výborně vypořádává s výpadky uzlů a poruchami spojů. V rámci MPLS-TE jsou funkce traffic engineeringu implementovány do síťové vrstvy z důvodu optimalizace směrování paketů.

MPLS-TE tedy :

- vylepšuje standardní IGP protokoly (OSPF, IS-IS), aby automaticky mapovali pakety k příslušným datovým tokům,
- přenáší pakety sítí pomocí technologie MPLS,
- určuje trasy pro datové toky v síti na základě zdrojů, které datový tok vyžaduje, a zdrojů dostupných v síti,
- využívá „směrování založené na omezení“, ve kterém je cesta pro datový tok nejkratší cestou, která splňuje požadavky na zdroje. U MPLS-TE má datový tok požadavky na propustnost, médium a prioritu,
- obnovuje primární spojení po jeho výpadku.

MPLS-TE automaticky vytváří a udržuje LSP v MPLS doméně pomocí protokolu RSVP-TE, který slouží také k rezervaci zdrojů podél celé přenosové cesty. Cesta využívaná daným LSP se určuje na základě požadavků na zdroje (zejména na propustnost) a dostupných síťových prostředků. Prostřednictvím rozšíření protokolů IGP jsou dostupné zdroje neustále záplavově oznamovány síti. Na základě požadavků datového toku na zdroje je sestaven TE tunel mezi směrovači, do kterého je datový tok směrován.

K automatickému vytvoření tunelu mezi TE rozhraními je výhodné použít např. rozšíření protokolu OSPF pro TE, která využívá techniku CSPF (Constrained Shortest Path First). CSPF najde nejkratší cestu sítí při úvaze dostupné šířky pásma, požadované šířky pásma, metriky a priority.

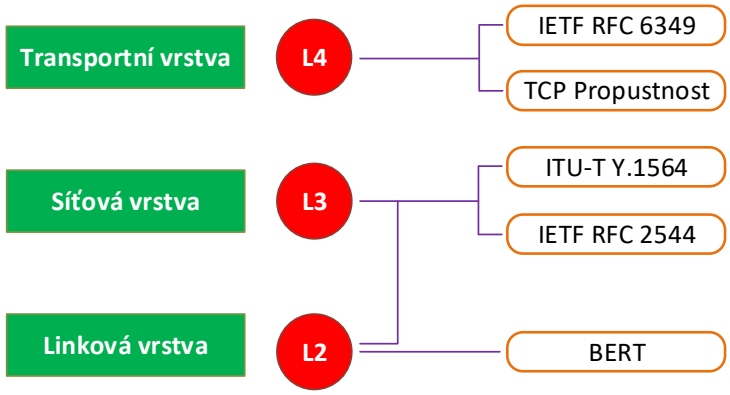
Tunel lze nakonfigurovat také manuálně pomocí explicitního vytváření cesty, kdy jsou zadávány IP adresy uzlů, přes které bude vytvořen TE tunel. Vhodné je také explicitně nebo automaticky nakonfigurovat záložní cestu (tunel) pro přepnutí v případě výpadku spoje či uzlů.

Pokud není datový provoz na síti přesně znám, je vhodné využívat automatickou konfiguraci šířky pásma (auto-bandwidth), pro rezervaci prostředků v rámci TE tunelu, která garantuje datovému toku požadovanou nebo větší šířku pásma, pokud je dostupná. Tato metoda také zabraňuje zbytečné blokaci síťových prostředků jinými tunely při jejich nevyužití.

3 TESTOVÁNÍ PŘENOSOVÝCH PARAMETRŮ V TELEKOMUNIKAČNÍCH SÍTÍCH

Testování přenosových parametrů je popsáno v řadě doporučení, která se liší metodikou a složením jednotlivých testů. Nejznámějším doporučením je IETF RFC 2544, ze kterého se následně vyvinuly další testy, které potírají nedostatky tohoto testu.

Dalším odlišností je, že testy dle různých doporučení probíhají na různých vrstvách referenčního modelu ISO/OSI. Rozdělení jednotlivých doporučení podle vrstev ISO/OSI modelu, na kterých probíhají jednotlivé testy znázorňuje obrázek 3.1. Podle situace a testované služby je tedy nutné zvolit vhodný test.



Obr. 3.1: Rozdělení jednotlivých doporučení podle vrstev ISO/OSI modelu.

3.1 Metodika pro měření a vyhodnocování přenosových parametrů

Níže popsaná metodika vychází z doporučení ČTÚ pro měření a vyhodnocování přenosových parametrů pevných a semi-pevných datových sítí (např. bezdrátových sítí s pevným předávacím rozhraním). Metodiku lze aplikovat i pro měření a analýzu pevných sítí za účelem kontroly parametrů stávajících NGA sítí a nově budovaných sítí NGA.

3.1.1 Měřící mód

Před začátkem měření je nutné vhodné zvolení měřícího módu. Základními módy jsou:

a) jednosměrné měření v sestupném či vzestupném směru.
b) měření ve smyčce (loopback).
c) obousměrné měření ve vzestupném a sestupném směru zároveň.

Vlastní měření je zároveň doporučeno provádět v pracovních dnech mezi 7. a 22. hodinou v délce alespoň 5 minut. Zajištěna by měla být také diversifikace v čase tak, že měření bude probíhat 1 min ve špičce a 1 min mimo špičku [17].

3.1.2 Identifikace demarkačních bodů

Samotné měření by mělo probíhat mezi demarkačními body. Měřící terminál by měl být připojen přímo k měřené síti, nejlépe v místě, které je co nejblíže předávacímu rozhraní služby mezi zákazníkem a poskytovatelem, ale stále v subsíti zákazníka.

V ideálním případě by měl být měřící terminál připojen přímo k předávacímu rozhraní služby, aby došlo k co největší eliminaci externích vlivů, které by mohly měření ovlivnit [17].

3.1.3 Měření v sítích s podporou IPv6

Pokud je v měřené síti podporovaná technologie IPv6 a IPv4 současně, je nutné provést měření pro oba protokoly.

Pokud je v měřené síti dostupný pouze protokol IPv6, měření se provede pouze pro něj.

3.1.4 Volba transportního protokolu

Volba měřícího protokolu na transportní vrstvě je silně ovlivněna charakterem měřené služby a tím, jaké informace chceme měřením získat. Např. měření dle standardu ITU-T Y.1564 probíhá pomocí UDP protokolu.

Protokol UDP s sebou nese také možná bezpečnostní rizika, a měření pak může být vyhodnoceno např. jako potenciální DoS útok. V zásadě je doporučeno postupovat dle následujících bodů [17]:

a) V případě, že je měřená síť pod cizí správou s níž není měření koordinováno, je doporučeno postupovat dle IETF RFC 6349. Tím se eliminuje riziko identifikace UDP datagramů jako útok. UDP se doporučuje využít jen tehdy, pokud to daná služba vyžaduje, nebo je to nezbytné.
b) V případě, že je měřená síť pod vlastní správou nebo je měření koordinováno s provozovatelem služby, pak je možné provést měření s protokolem UDP. I tak však nelze vyloučit případnou blokaci rozhraní bezpečnostním prvkem v síti.

3.1.5 Definice parametrů generátoru provozu

Před začátkem měření je nutné stanovit maximální hodnotu MTU, která je následně prohlášena za referenční. Od hodnoty MTU se následně odvíjí velikost generovaných rámců a propustnost na síťové vrstvě. Z důvodů objektivity je maximálního hodnota MTU pro testování dle standardu ITU-T Y.1564 a IETF RFC 2544 omezena na 1518 B.

Lze volit i jinou velikost rámců v souladu s charakterem poskytované služby. Např. 1518 B pokud měřená přípojka odpovídá službě přístupu k internetu, nebo nižší s hodnotou typickou pro provoz dané služby v dané síti (typicky hlasové a televizní služby) [17].

3.1.6 Postup testování

V této sekci kapitoly je uveden postup samotného měření přenosových parametrů v testované síti [17].

1. Stanovit měřící protokol transportní vrstvy, konkrétně TCP nebo UDP viz 3.1.4 a 3.1.5.
2. Zvolit vhodné doporučení pro měření viz IETF RFC 2544, ITU-T 1564, IETF RFC 6349.
3. Určit verzi protokolu IP, v případě IPv6 postupovat dle 3.1.3.
4. Stanovit demarkační body viz 3.1.2.
5. Zvolit sekvenci měření odpovídající charakteru testované služby viz 3.1.1.
6. Nastavení komunikujících stran.
7. Nastavení parametrů měření.
8. Inicializace měření a automatický výpočet parametrů TCP relace.
9. Provedení měření se zvolenými parametry v bodech 1) až 8).
10. Ukončení měření, uložení a zpracování výsledků.

3.2 IETF RFC 2544

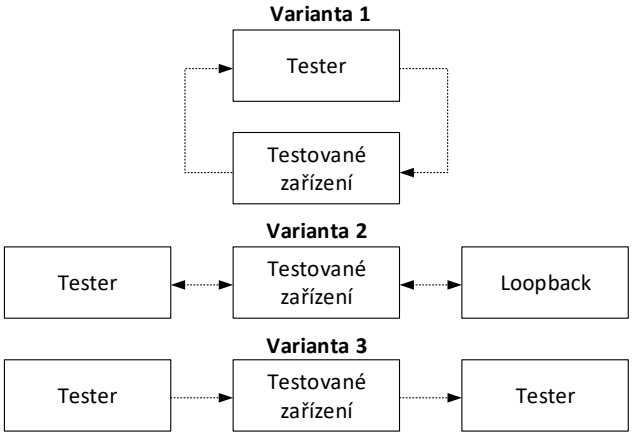
Standard RFC 2544 byl vyvinut organizací IETF. Jedná se o nejstarší a nejznámější standard pro testování síťové infrastruktury. Celý název dokumentu zní „Benchmarking Methodology for Network Interconnect Devices“. V dokumentu je popsána metodika měření, jednotlivé testy a způsoby pro zpracování a reprezentaci výsledků.

Celkový test je složen z několika dílčích subtestů popsaných v kapitole 3.2.1. Z pravidla bývá test proveden pro ethernetového rámce o velikosti 64 B, 128 B, 256 B, 512 B, 1024 B, 1280 B, 1518 B. Zároveň by také mělo testování probíhat obousměrně, čehož lze jednoduše docílit využitím dvou analyzátorů, nebo jednoho analyzátoru opatřeného vysílacím a přijímacím portem.

RFC 2544 byl vyvinut zejména pro testování síťových prvků a datových okruhů v laboratorních podmínkách, což se ukázalo být jedním z mnoha jeho nedostatků. Dalším nedostatkem je časová náročnost celého testu a nemožnost měření parametrů sledovaných v moderních sítích. Celkový test může trvat až 4 hodiny. To by pro operátory znamenalo měření triple play služeb v PON sítí až 12 h, což je nepřijatelné. Nevhodná je také skladba testů, kdy například pro zpoždění je uvažována pouze jeho absolutní hodnota, nikoliv také jeho kolísání a změna v čase, které jsou důležité zejména pro multimediální služby [16]. Díky výše zmíněným nedostatkům je RFC 2544 dnes již plně nahrazeno novými testy, zejména jsou to testy podle standardu ITU-T Y.1564 SAM.

3.2.1 Metodika testování

V dokumentu RFC 2544 jsou popsány tři schémata pro testování sítí a síťových prvků, znázorněná na obrázku 3.2. Schémata jsou rozdílná z důvodu odlišného vybavení techniků a výhodnosti nasazení v dané síti. Při testech je na testované zařízení, spoj, nebo několik zařízení za sebou nahlíženo jako na černou skříňku bez znalosti jejího obsahu [16].



Obr. 3.2: Možnosti zapojení pro testování dle standardu RFC 2544 [6].

Varianta 1 je vhodná pro měření s jedním analyzátorem opatřeným vysílacím portem generující testovací provoz a přijímacím portem pro analýzu dat. U většiny testerů je také možné použít 1 port pro vysílání a příjem signálu a druhý port využít jako obraceč síťového provozu (loopback) viz *varianta 2*. Pro měření v režimu loopback lze také využít speciální speciální zařízení pro obrácení datového toku zpět na přijímací port analyzátoru. Poslední možností je *varianta 3*, která využívá dvou

testerů, kdy jeden je zapojený jako generátor testovací sekvence a druhý jako analyzátor. Testování podle varianty 3 je výhodné pro datových okruhů s asymetrickými přenosovými parametry [14, 6].

3.2.2 Výkonnostní testy

Test propustnosti (Throughput)

Test slouží pro zjištění maximální rychlosti přenosu rámců, při které ještě nedochází k jejich ztrátě a provádí se rámci o velikosti 64 B, 128 B, 256 B, 512 B, 1024 B, 1280 B, 1518 B. Principem testu je vyslat do testovaného zařízení (sítě) určitý počet rámců s určitou přenosovou rychlostí. Následně je porovnáváno množství odeslaných a přijatých rámců z/do testeru. Test je zpravidla zahájen vysláním rámců s největší možnou přenosovou rychlostí. Pokud je detekována ztráta rámců, dochází ke snížení přenosové rychlosti zpravidla na polovinu původní přenosové rychlosti. Pokud po není po snížení přenosové rychlosti detekována ztráta, tak dochází k opětovnému zvýšení přenosové rychlosti o polovinu [6].

Po proběhnutí všech iterací je sestavena tabulka a graf, které znázorňují závislost maximální propustnosti rámců za sekundu na velikosti rámce. [6]

Test latence (Latency)

Při testu se uvažuje obousměrné zpoždění RTT, které zahrnuje také čas potřebný pro zpracování a opětovné odeslání dat zařízením v loopback režimu [14].

Test je prováděn pro standardní velikosti ethernetového rámce, kdy pro každou velikost rámce musí být proveden dvacetkrát. Obdobně jako při testu propustnosti je vytvořen datový tok s maximální propustností při které nedochází ke ztrátám rámců složený z rámců stejné velikosti. Test je prováděn minimálně po dobu 120 s, kdy po 60 s je do sekvence vložen rámec s časovým razítkem svého vysílání, které je přijímačem detekováno. Dílčí hodnota latence je pak určena jako rozdíl mezi časem odeslání a časem přijetí rámce. Výsledná latence pro danou velikost rámce je dána aritmetickým průměrem dílčích latencí z minimálně 20 měření [6].

Test ztrátovosti rámců (Frame loss rate)

Výsledkem testu je procentuální vyjádření závislosti ztracených rámců na přenosové rychlosti vztažené k velikosti rámců. Tento typ testu je důležitý zejména pro služby využívající transportního protokolu UDP, které běží v reálném čase, protože protokol UDP neumožňuje opakování přenosu dat. Principem testu je vyslání předem definovaného počtu rámců určené velikosti do zařízení (spoje) a následně analyzovat, kolik rámců se vrátí zpět. Test je započat s maximální možnou přenosovou

rychlostí (FPS) pro danou technologii, která je při detekci ztrátovosti iteračně snižována zpravidla o 10 % (nebo méně) až do doby, kdy je ztrátovost nulová a test je ukončen [16, 6].

Test zatížitelnosti (Back-to-back)

Cílem testu je zjistit maximální počet rámců ve shluku (s minimální mezirámcovou mezerou), které je zařízení schopno zpracovat s nulovou ztrátou rámců. Do testovaného zařízení je vyslán shluk rámců a následně je porovnáván počet odeslaných a přijatých rámců ve shluku. Pokud počet přijatých a odeslaných rámců nesouhlasí, tak dochází ke snížení počtu rámců ve shluku. Pokud se rovná, dochází ke zvýšení počtu rámců ve shluku. Standard uvádí, že minimální délka testovacího shluku by měla být alespoň 2 s a test by měl být opakován alespoň 50krát [16, 6].

Test obnovy systému po přetížení (System Recovery)

Jedná se o zátěžový test, který má odhalit dobu, za kterou dojte k normální funkci zařízení po jeho přetížení. Test spočívá v zahlcení zařízení vysláním rámců s rychlostí minimálně 100% ze změřené propustnosti po dobu alespoň 60 s. Následně je přenosová rychlost skokově snížena na polovinu a začíná odpočítávání času, které je zastaveno až v době, kdy testované zařízení nevykazuje žádnou ztrátovost rámců. Test je prováděn několikanásobně a pro různé délky rámců. Výsledkem je tabulka obsahující průměrné hodnoty času zotavení pro dané velikosti rámců [16, 6].

Test obnovy systému po restartu (Reset)

Poslední test slouží k měření času, který potřebuje daný spoj (zařízení) pro zotavení se po jeho restartu. Principem testu je do testovaného zařízení kontinuálně vysílat tok rámců. V určitém okamžiku je testované zařízení restartováno a je měřen čas mezi přijetím posledního rámce před restartem a přijetím prvního rámce po restartu [6, 16].

3.3 ITU-T Y.1564

V roce 2011 bylo organizací ITU zveřejněno nové doporučení ITU-T Y.1564 s pracovním názvem Y.156sam. Kompletní název tohoto standardu je Ethernet Service Activation Test Methodology. Standard byl vyvinut, aby pokryl nedostatky zastaralého testu RFC 2544, jehož podpora je však i v moderních analyzátorech samozřejmostí. Výrobci nabízejí testery s podporou testu podle standardu Y.1564 pod

odlišnými obchodními názvy, a tak se lze setkat s názvy EtherSAM, SAMcomplete nebo V-SAM [16].

Hlavní výhodou testu je možnost měření širokého spektra přenosových parametrů, kterými jsou propustnost (Throughput), zatížitelnost spoje (Burstability), ztráta rámců při přenosu (Frame Loss), zpoždění (Latency), kolísání zpoždění (Jitter), dostupnost služby (Avilability) a doba potřebná pro přepnutí na záložní spoj (Protection Switching) [16, 10]. Test tedy poskytuje kompletní vyhodnocení výkonnosti zařízení (sítě) s ohledem na garantovanou úroveň kvality poskytovaných služeb na základě smlouvy SLA (Service Level Agreement) mezi zákazníkem a operátorem.

S nasazením testu došlo také k výraznému zkrácení doby testu, která bývá zpravidla 2 hodiny, ale může být rozšířena až na 24 hodin nebo zkrácena až na 2 minuty. Velkým posunem vpřed je možnost testování paralelních datových toků, což umožňuje zkrátit dobu měření pro pro triple play služby až na třetinu času RFC 2544, neboť lze testovat všechny služby najednou.

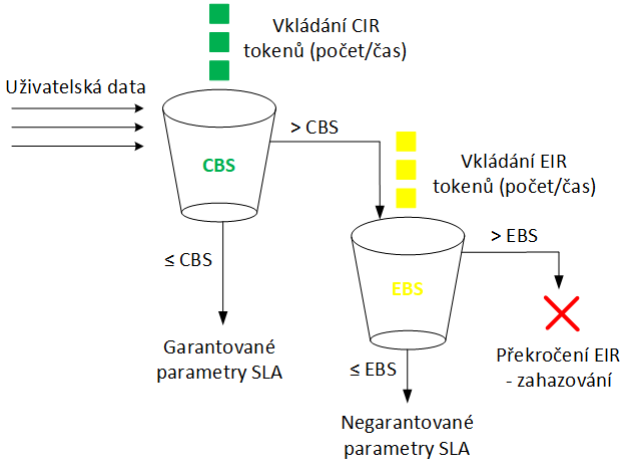
Novinkou, kterou doporučení přináší je i možnost jednosměrného a obousměrného testování, nebo také simultánního testu. Jednosměrné testování je vhodné pro datové spoje či asymetrické služby (např. triple play), které často vykazují odlišné hodnoty parametrů v jednotlivých směrech. Při standardním obousměrném testování se využívá zapojení s loopback zařízením na konci sítě, které zrcadlí datový provoz zpět k analyzátoru. Pro simultánní testování se využívají dva analyzátory, kdy na každém konci sítě je umístěn jeden analyzátor individuálně testující oba směry. V praxi se může stát, že hodnoty KPI budou pro oba směry vyhovující, ale při současném zatížení v obou směrech by mohlo dojít k problémům v jednom ze směrů, což by klasický obousměrný test neodhalil.

3.3.1 Profily datové propustnosti

Z pohledu uživatele definují profily datové propustnosti průměrné množství závazných a přebytečných paketů služby v síti poskytovatele. Po identifikaci datového toku, pro který byly sjednány podmínky dané SLA, probíhá měření, zda-li datový tok splňuje podmínky dohodnuté v SLA. Podle výsledků měření je paket následně označený příslušnou značkou. Tento proces se nazývá barvení paketů a je prováděný algoritmem Token Bucket popsaným na obrázku 3.3.

Pokud pakety vyhovují danému profilu propustnosti definovanému pro službu v SLA (in-profile), pak jsou obarveny zeleně, nemohou být zahozeny a jsou pro ně garantovány KPI parametry. Žlutě jsou obarveny pakety vyhovující EBS, které však nevyhovují CBS a nelze tak u nich zaručit parametry dané SLA. Tyto pakety jsou označovány jako out-of-profile a může docházet k jejich zahození např. v případě zahlcení sítě. Červeně označené pakety jsou též out-of-profile, nevyhovují CBS ani

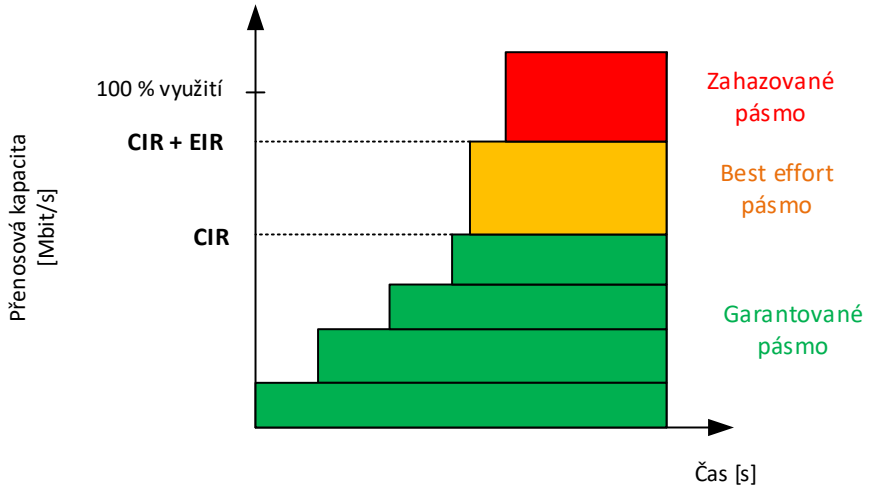
EBS a jsou zahazovány vždy.



Obr. 3.3: Definovaní profilů propustnosti algoritmem Tocken Bucket.

CIR (Commited Information Rate) určuje horní hranici garantovaného pásma přenosové kapacity pro vybranou službu, jsou zaručeny kvalitativní parametry pro službu dle SLA.

EIR (Excess Information Rate) určuje pásmo, ve kterém již nejsou pro danou službu garantovány kvalitativní parametry přenosu. Po překročení hranice EIR jsou veškeré datové toky zahazovány. Pro testy je uvažována hranice CIR + EIR + 25 %.



Obr. 3.4: Vysvětlení základních pojmů dle standardu ITU-T Y.1564.

CBS (Commited Burst Size) určuje maximální kapacitu datového toku pro kterou platí SLA.

EBS (Excess Burst Size) vyjadřuje velikost datového toku, při kterém není zaručena SLA. Může se uplatňovat ztrátovost paketů a zpoždění.

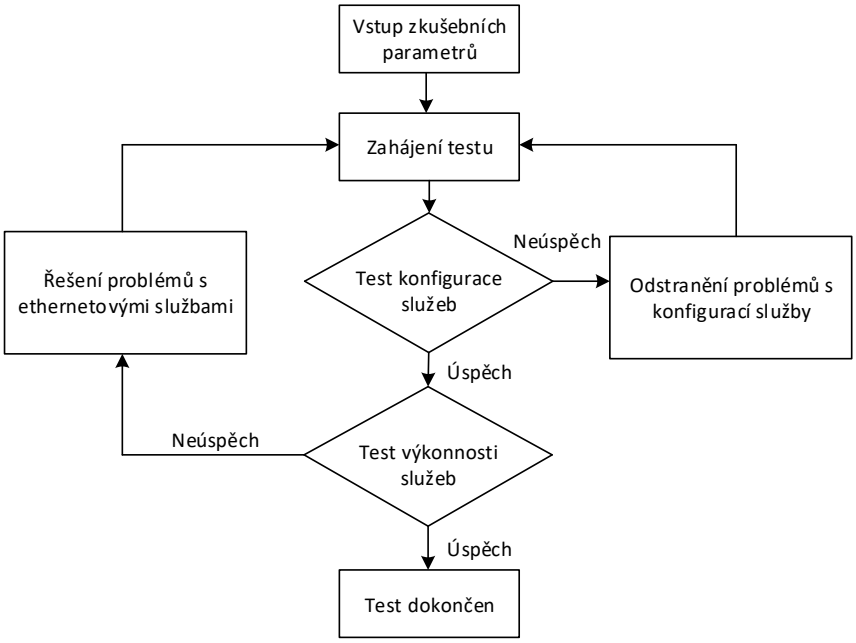
KPI (Key Performance Indicator) charakterizuje klíčové výkonnostní indikátory kterými jsou míněny klasické kvalitativní parametry jako: propustnost, ztrátovost rámců, zpoždění a jitter. Platí, že v pásmu CIR (garantované pásmo) musí být KPI plně garantovány, v pásmu CIR-EIR (best effort pásmo) už nemusí být garance KPI zaručena a v pásmu EIR (zahazované pásmo) nejsou KPI vůbec definovány.

3.3.2 Metodika testování

Testování podle standardu ITU-T Y.1564 probíhá ve dvou fázích. Kompletní postup testování uvedený v doporučení je zobrazen na obrázku 3.5.

V první fázi je testována správnost nastavení parametrů garantovaných SLA, kdy dochází ke zjišťování prahových hodnot CIR a EIR pro dané zařízení (síť). Tento test se nazývá tzv. ramp test a probíhá za plného provozu pro každou službu individuálně. Ramp test je typicky prováděn rámci o velikosti 512 bajtů (nebo možné zvolit i jinou velikost rámce) a dochází při něm ke krokovému zvyšování přenosové rychlosti. Pro každou hodnotu přenosové rychlosti trvá test od 1 sekundy do 60 sekund a jsou při něm vyhodnoceny parametry KPI a jejich soulad s SLA v pásmu CIR. V pásmu mezi CIR a EIR mohou být indikátory KPI horší a v pásmu EIR + CIR by mělo dojít k zahazování provozu. Maximální hodnota přenosové rychlosti je stanovena na hodnotu rovnou součtu CIR + EIR + 25 %. V pásmu CIR + EIR však musí být stále zaručen provoz do hranice CIR, přesahující datové toky musí být zahozeny. Pokud by přijatý datový toku převyšoval hodnotu EIR, znamená to, že je síť chybně nakonfigurovaná [10, 16]. Výsledkem testu je zpravidla tabulka znázorňující hodnoty indikátorů KPI pro zvolené přenosové rychlosti. Volitelnou možností v první fázi je burst test, při kterém jsou do testovaného zařízení (spoje) vysílány shluky rámců s náhodnou přenosovou rychlostí [10, 16].

Druhá fáze je založena na testu výkonnosti služeb. Cílem testu je ověřit mechanizmy pro prioritizaci či omezování určitých datových toků. Při testu výkonnosti služeb je na služby generované paralelně nahlíženo jako na jeden datový tok, kdy dochází k hromadnému testování parametrů KPI pro všechny nakonfigurované služby najednou do jim odpovídajícím parametrům CIR. To umožňuje ověření parametrů v prostředí, které se blíží reálnému provozu. Výsledkem testu by měla být přehledná tabulka znázorňující hodnoty KPI pro danou službu a různé velikosti rámců. Často bývá také barevně nebo symbolicky rozlišeno, zda testovaný spoj pro danou službu a velikost rámce vyhověl požadavkům SLA [10, 16].



Obr. 3.5: Schéma metodiky testování dle doporučení ITU-T Y.1564 [10].

3.4 BERT

Jedná se o testování bitové chybovosti BERT – Bit Error Rate Test, které je popsané v doporučení ITU-T O.151. Test je možné provést na fyzické, linkové a síťové vrstvě a probíhá pro různé velikosti rámců. BERT spočívá ve vyslání sekvence bitů do zařízení (spoje) a následné analýzy přijatých bitů, kdy výsledná bitová chybovost je vypočítána jako podíl počtu přijatých bitů v sekvenci ku celkovému počtu odeslaných bitů v sekvenci do zařízení (spoje) [9]. Umožňuje tak relativně jednoduchý a rychlý způsob testování, zda optický či metalický spoj pracuje správně. V závislosti na výhodnosti použití pro dané zařízení či spoj existuje velké množství standardizovaných testovacích sekvencí, které lze pro test zvolit. Vybírat lze například z pseudonáhodné sekvence, sekvence samých nul či jedniček, různou hustotou jedniček a nul v sekvenci a dalších.

Většina zařízení pro měření bitové chybovosti dokáže také vytvářet diagram oka, který je silným nástroje pro analýzu toho, jak jsou bity přijímány na vzdáleném konci kanálu.

3.5 IETF RFC 6349

Jedná se o doporučení vydané organizací IETF. Hlavní výhodou oproti většině ostatních testů je, že pro testování je využíváno transportního protokolu TCP. Test je tedy vhodný pro testování non-realtime služeb využívajících spolehlivý protokol TCP. Naopak zcela nevýhodné je jeho využití pro měření služeb probíhajících v reálném čase, které zpravidla využívají pro transport dat protokolu UDP.

Dalším důvodem pro vznik standardu RFC 6349 byl fakt, že testování prováděné na linkové (L2) a síťové (L3) vrstvě není pro operátory dostatečné. Vyžadovali také možnost testování sítí na transportní vrstvě, kterou standart RFC 6349 přináší.

Pro získání korektních výsledků z testu RFC 6349 je však nutné provést správná nastavení [7]:

- vysílacích oken – TCP CWND (congestion windows),
- přijímacích oken – TCP RWND (receive windows),
- vysílacích a přijímacích bufferů,
- velikosti rámců.

Výše zmíněná nastavení plynou z principu protokolu TCP, zejména pak ze struktury jeho hlavičky. Při nastavování parametrů testu je také nutné vzít v úvahu fakt, že reálný provoz může být ovlivněn opakovaným přenosem nedoručených segmentů, což plně koresponduje s reálným vnímáním služby přístupu k síti Internet. Metoda měření podle standardu RFC 6349 je tedy silným nástrojem pro měření komunikačních sítí za provozu nebo při troubleshootingu.

3.5.1 Metodika testování

Na začátek je nutné zmínit, že testy jsou vhodné zejména pro řízené IP sítě různých architektur a topologií. Dalším vymezením je, že nelze provést přesné měření TCP propustnosti dat v dysfunkční síti. Měření také nebude mít patřičnou vypovídací hodnotu pokud síť vykazuje vysokou ztrátovost paketů nebo jitter. Doporučeno je jako vodítko pro přesné měření považovat ztrátovost paketů do 5 % a jitter do 150 ms [7].

Speciální požadavky jsou kladeny na testovací nástroje. Kdy testovací host může být buď standardní počítač, nebo nástroj pro testování komunikace (analyzátor). V obou případech však musí být zajištěna schopnost zařízení emulovat klientskou i serverovou část.

Samotné testování probíhá v následujících třech krocích [7]:

1. Identifikace MTU linky.
2. Změření RTT a přenosové kapacity.
3. Testování TCP propustnosti při vypočítané velikosti okna.

Identifikace MTU

TCP implementace využívají pro identifikaci MTU techniku Path MTU Discovery (PMTUD). Tato technika spoléhá na ICMPv4 zprávu o „potřebě fragmentace“ dat. Princip je následující: Zařízení do sítě vyšle paket s příznakem DF (Don't Fragment), aby nedocházelo k jeho fragmentaci pokud bude jeho velikost větší než next-hop MTU. Pokud MTU paketu bude větší než next-hop MTU, pak dojde k zahození paketu a informování odesílatele ICMP zprávou, ve které je uvedena potřeba fragmentace dat a informace, že daný paket byl zahozen. Po fragmentaci na nižší hodnotu MTU je celý cyklus opakován až do doby, kdy je odesílatelem přijato potvrzení o doručení paketu k cíli a aktuální hodnota MTU je uložena jako MTU trasy. Nevýhodou tohoto řešení je, že spousta administrátorů v sítích zakazuje ICMP zprávy [7].

Identifikace MTU trasy je velice důležitá pro správnou konfiguraci TCP TTD (Throughput Test Device) a zejména proto, aby nedocházelo k fragmentaci dat při dalších částech testu. Případná fragmentace dat v průběhu testů by mohla silně ovlivnit celkový výsledek testu.

Měření RTT a šířky pásma

Před začátkem testování TCP propustnosti musí být změřeno zpoždění RTT a přenosová kapacita testované sítě (BB – Bottleneck Bandwidth), ze kterých je vypočítána hodnota BDP (Bandwidth-Delay Product) viz rovnice 3.1 [7]. Ta slouží k výpočtu a správnému odhadu velikosti okna odesílatele TCP RWND a SocketBufferu odesílatele, které jsou dále použity v dalších krocích testu.

$$BDP\ [\text{bit}] = RTT\ [\text{s}] * BB\ [\text{bit/s}] \tag{3.1}$$

Je také nutné nastavit velikost vyrovnávací paměti odesílatele (Send Socket Buffer) a velikost TCP okna příjemce (TCP RWND) na hodnotu větší, než je BDP, jinak bude výkon TCP omezen. Minimální hodnotu TCP RWND lze spočítat z BDP dle rovnice 3.2 [7].

$$TCP\ RWND\ [\text{B}] = BDP\ [\text{bit}]\ /\ 8 \tag{3.2}$$

RTT vyjadřuje dobu uplynulou od odeslání prvního bitu TCP segmentu ze strany odesílatele po přijetí posledního bitu potvrzení odeslaného segmentu na straně odesílatele. Pro přesné výsledky testu zpoždění je doporučeno měření provádět mimo přenosovou špičku, ve které může docházet k dalším zpožděním vlivem vytížení vyrovnávacích pamětí. Dále by jako referenční RTT by měla být použita minimální hodnota z naměřených vzorků, která nejlépe vystihuje reálné RTT [7].

Nejpřesnější možnost měření RTT je měření s vyhrazeným analyzátorem a loopback zařízením na vzdáleném konci sítě, kdy je datový tok obracen zpět k testeru a výsledné zpoždění je určenu pomocí protokolů měření zpoždění (např. protokol

TWAMP) uvedených v doporučení RFC 5357. Dalšími méně přesnými metodami měření RTT jsou měření pomocí ICMP zprávy „ping“, MIB statistik nebo speciálních aplikací (např. Linux - „iperf“) [7].

Měření přenosové kapacity testované sítě ***BB*** by se naopak mělo provádět za plného provozu a mělo by být prováděno v obou přenosových směrech, zejména pak u asymetrických přístupových sítí (např. ADSL). Dále by test měl být prováděn v průběhu celého dne v určitých intervalech po sobě, aby bylo dále možné lépe charakterizovat TCP propustnost sítě.

Operátoři standardně provádějí testy přenosové kapacity sítě na L2 a L3 vrstvách referenčního modelu ISO/OSI pomocí testu RFC 2544 navzdory tomu, že se jedná o test určený pro laboratorní účely. Správně by se testy přenosové kapacity testované sítě měly provádět dle standardu RFC 5136 [7].

Testování TCP propustnosti

Test TCP propustnosti využívá RTT a BB změřené v kroku 2, a může být prováděn pro jedno či několik TCP spojení v závislosti na charakteru testované TCP služby. Ve standardu je důrazně doporučeno provést test propustnosti v obou směrech nezávisle na sobě a poté testy spustit v obou směrech současně. Výpočet TCP propustnosti lze provést z vypočítané velikosti okna z rovnice 3.2 a změřené RTT v bodě 2 následovně [7]:

$$TCP\ propustnost\ [\text{bit/s}] = (TCP\ RWND\ [\text{B}] * 8)\ /\ RTT\ [\text{s}] \tag{3.3}$$

V rámci třetí fáze testu dle standardu RFC 6349 jsou dále vypočítány další TCP metriky, které budou uvedeny v další sekci níže.

3.5.2 TCP Metriky

TCP metriky jsou vypočítávány v rámci třetí fáze testu dle doporučení RFC 6349. Slouží pro lepší porovnání a porozumění výsledkům měření. Metriky navíc umožňují porovnání TCP propustnosti v různých podmínkách v testované síti a při různých nastaveních měřících stran. Jedná se o tři základní metriky, kterými jsou [7]:

- TCP Efficiency [%],
- Transfer Time Ratio (TTR) [–],
- Buffer Delay [%].

TCP Efficiency

Vyjadřuje efektivitu protokolu TCP v procentech. Výpočet reprezentuje počet bitů, které nemusely být opakovaně přeneseny a tím udává představu o chybovosti celého

TCP spojení. Výpočet TCP efektivity *TCP Eff* lze provést dle rovnice 3.4 [7].

$$TCP\ Eff\ [\%] = \frac{TB\ [\text{bit}] - rTB\ [\text{bit}]}{TB\ [\text{bit}]} * 100 \tag{3.4}$$

V rovnici 3.4 vyjadřuje *TB* celkový počet odeslaných bitů, který zahrnuje všechny původní i znovu odeslané bity, a *rTB* vyjadřuje celkový počet opakovaně přenesených bitů.

Transfer Time Ratio

TCP TTR vyjadřuje poměr mezi aktuální hodnotou TT (Transfer Time) – *aTT* a ideální hodnotou TT – *iTT*.

$$TCP\ TTR\ [-] = \frac{aTT\ [\text{s}]}{iTT\ [\text{s}]} \tag{3.5}$$

Aktuální hodnota TT vyjadřuje skutečnou dobu přenosu celého datového bloku přes TCP spojení, zatímco ideální hodnota TT je dána výpočtem, který určuje, za jak dlouho by za dané situace měl datový blok být teoreticky přenesen přes TCP spojení. Ideální TT je odvozena od maximálního možného toku TCP dat na síťové vrstvě ISO/OSI modelu. Výpočet ideální hodnoty TT je dán rovnicí

$$iTT\ [\text{s}] = \frac{TBS\ [\text{bit}]}{maxATT\ [\text{bit/s}]} \quad , \tag{3.6}$$

kde *TBS* vyjadřuje celkovou velikost přenášeného datového bloku a *maxATT* určuje maximální dosažitelnou TCP propustnost sítě [7].

Buffer Delay

Buffer delay (BD) určuje zpoždění vyrovnávací paměti. Reprezentuje vztah mezi nárůstem/poklesem RTT během testu propustnosti dat a ideální RTT. Ideální hodnota RTT (*iRTT)* znamená takové RTT, které je vlastní přenosové cestě za ideálních podmínek (bez zahlcení).

Hodnotou RTT je při výpočtu BD míněna průměrná hodnota RTT jednotlivých vzorků daná jejich aritmetickým průměrem. Výslednou hodnotu zpoždění bufferu pak lze získat výpočtem z rovnice 3.7 [7].

$$BD\ [-] = \frac{RTT\ [\text{s}] - iRTT\ [\text{s}]}{iRTT\ [\text{s}]} \quad , \tag{3.7}$$

3.6 Metro Ethernet Forum (MEF)

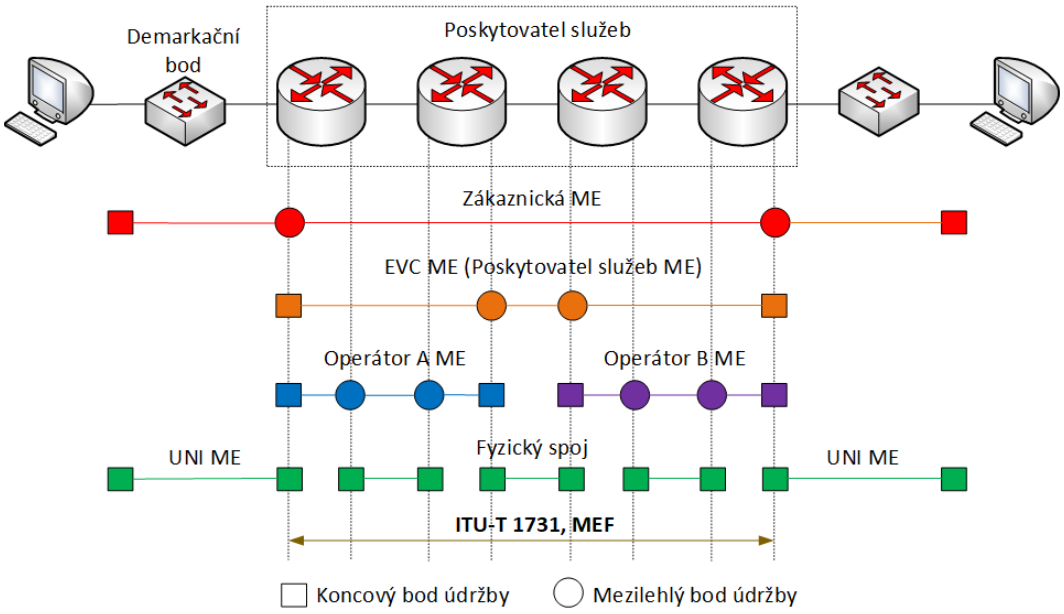
Jedná se o neziskovou organizaci, která se zaměřuje na zavádění technologie optického ethernetu v metropolitních sítích po celém světě. Fórum MEF zastřešuje

více než 210 významných telekomunikačních operátorů, dodavatelů síťových prvků a dalších společností, které sdílí zájem o metro-ethernet. Klíčovými cíli fóra jsou:

- Sjednotit poskytovatele služeb, dodavatele zařízení a koncové zákazníky do skupiny využívající služeb optického ethernetu.
- Usnadnit implementaci optických ethernetových standardů pro urychlení nasazení služeb optického ethernetu a vytvoření tříd transportních sítí založených na technologii ethernet.
- Zlepšení celosvětového podvědomí o výhodách služeb optického ethernetu.

MEF vychází ze spolehlivé a velmi dobře standardizované technologie ethernet. Cílem fóra není výrazná změna stávajících standardů, ale vyplnění mezer mezi stávajícími standardy pro standardizaci sítí metro ethernet, jejichž architektura úzce souvisí s architekturou sítí NGN.

Fórum se zaměřuje na několik dílčích oblastí týkajících se budování a nasazení sítí metro-ethernet. Níže bude rozebrána pouze část zabývající se měřením výkonnosti datových sítí a ověřováním parametrů SLA. Ve standardech MEF je uváděno testování sítí pomocí metrik a postupů uvedených v doporučení ITU-T Y.1731.



Obr. 3.6: Multidoménový model sítě metro-ethernet s údržbovými entitami a body.

Na obrázku 3.6 je znázorněn multidoménový model sítě metro-ethernet s oblastmi údržby (ME – Maintenance Entity), které jasně vypovídají o tom, kdo je zodpovědný za management a údržbu dané části sítě. Jednotlivé ME jsou vymezeny koncovými body údržby (MEP – Maintenance End Point), mezi kterými se v rámci

jedné ME mohou nacházet mezilehlé body údržby (MIP – Maintenance Intermediate Point). Koncový zákazníci jsou k síti metro ethernet připojeni prostřednictvým uživatelských rozhraní sítě (UNI – User Network Interface). Testování konektivity a výkonnosti sítě je prováděno mezi dvěma body MEP. Samotné end-to-end testování výkonnosti sítě a ověření SLA parametrů se pak provádí mezi dvěma MEP v rámci zákaznické domény.

3.6.1 Datová propustnost

Dle MEF se měření datové propustnosti provádí za zkušebních podmínek, tzn. mimo provoz testované služby. Pro měření datové propustnosti ve fázi aktivace služeb je doporučován test dle standardu ITU-T Y.1564, který umožňuje test profilů šířky pásma a dalších atributů. Pro testy v jiných fázích je doporučován test dle standardu IETF RFC 2544 [11].

Profily šířky pásma a barvení paketů související s SLA, které vyhovují standardu MEF 23.1, byly popsáno v kapitole 3.3.1. MEF rozlišuje dva módy rozhraní UNI. Jedná se o Color-blind a Color-aware UNI.

Color-blind UNI ignoruje značky (např. DSCP, 802.1Q), které již byly datovému toku přiděleny dříve a odkazují na určitou barvu. S pakety je tedy zacházeno, jako by nebyly již dříve obarveny a k jejich obarvení dochází až v tomto bodě.

Color-aware UNI bere na vědomí indikaci barvy, kterou již byl paket označen. Například podnikové sítě využívají k zajištění kvality služeb mechanizmus DiffServ, kde jsou pakety označeny v poli DSCP (Differentiated Services Code Point), které indikuje barvu paketu a třídu služeb – CoS (Class of Service). Směrovač (CE – Customer Edge) na rozhraní sítě účastníka a poskytovatele pak může mapovat barvu a CoS indikované polem DSCP do pole VLAN CoS (802.1p) v ethernetovém rámci. Mapování do pole VLAN CoS umožní sdělit poskytovateli, které rámce mohou být zahozeny v případě zahlcení sítě. Tato prvotní informace o značkovaní je tedy následně zohledněna i při přeznačkování a barvení.

3.6.2 Obousměrné zpoždění

Pokud nejsou koncové body (MEP) v rámci jedné skupiny údržby (MEG – Maintenance Entity Group) časově synchronizovány, lze jednosměrné zpoždění aproximovat z obousměrného zpoždění vydělením dvěma.

Postup měření obousměrného zpoždění je následující. Lokální MEP odešle zprávu DMM (Delay Measurement Message) jednou za časový interval (1 s, 10 s, 1 min). Vzdáleny MEP na tyto zprávy odpovídá pomocí zprávy DMR (Delay Measurement Reply), přičemž obě zprávy musí putovat shodnou cestou v rámci jedné sledované jednotky EVC (Ethernet Virtual Channel).

Každá zpráva DMM obsahuje v DMM PDU časové razítko *TxTimeStampf* s časem odeslání DMM PDU. Po přijetí zprávy DMM vzdáleným MEP je časové razítko *TxTimeStampf* zkopírováno do DMR zprávy a odesláno zpět k odesílateli DMM zprávy, který k ní přiřadí časové razítko přijetí DMR zprávy, tzv. *RxTimeStampb*. Výsledné obousměrné zpoždění je pak spočítáno z rozdíl mezi časem přijetí DMR zprávy *RxTimeStampb* a časem odeslání zprávy DMM *TxTimeStampf* jako *RxTimeStampb* – *TxTimeStampf* [11].

Výše zmíněný vztah platí pouze v ideálním případě, kdy je veškeré zpracování paketů a časové značení prováděno hardwareově bez vloženého zpoždění spojeného se softwareovým zpracováním. Zvýšení přesnosti měření lze dosáhnout přidáním dalších časových razítek na straně vzdáleného MEP, který přidá do zprávy DMR razítka:

- *RxTimeStampf* – Časové razítko s časem přijetí DMM PDU.
- *TxTimeStampb* – Časové razítko s časem odeslání DMR PDU.

Výsledné obousměrné zpoždění je pak zpřesněno odečtením zpoždění vlivem zpracování rámce na vzdáleném MEP (*TxTimeStampb* – *RxTimeStampf*) od celkové hodnoty obousměrného zpoždění [11].

3.6.3 Jednosměrné zpoždění

Pokud jsou síťové prvky časově synchronizovány, pak může měření zpoždění probíhat pouze v jednom směru, což je mnohem jednodušší proces.

Kontrolér vyšle zprávu 1DM PDU, která obsahuje pouze časové razítko svého odeslání *TxTimeStampf*. Vzdálený MEP pak vypočítá jednosměrné rámcové zpoždění jako *RxTimeStampf* – *TxTimeStampf* [11].

3.6.4 Měření ztrátovosti rámců – LM

Toto měření je vhodné pro periodické měření ztrátovosti rámců mezi dvěma rozhraními v rámci EVC, za předpokladu, že oba MEP náleží do shodného subjektu údržby.

Budeme-li uvažovat postup „s jedním koncem“, kdy veškeré výpočty provádí řídící koncový bod MEP, tzv. MEP kontrolér, pak je princip výpočtu ztrátovosti rámců následovný: Vzdálený MEP zaznamenává, kolik rámců s uživatelskými daty přijal a lokální MEP kontrolér kolik těchto rámců odeslal. MEP kontrolér odesílá periodicky (např. jednou za 1 s, 10 s, 1 min) na unicastovou adresu MEP zprávy LMM (Loss Measurement Message). Vzdálený MEP na tuto zprávy odpovídá zprávou LMR (Loss Measurement Reply). Tyto zprávy slouží ke shromáždění informací o tom, kolik uživatelských dat bylo odesláno a přijato mezi dvěma MEP, neboť ztrátovost rámců je u metody LM vypočítávána za pomoci uživatelských dat. Pro

každého člena MEP a každou službu s odlišným CoS ID (Class of Services IDentity) musí existovat dva lokální čítače [11].

- *TxFCl*: Čítač pro rámce odeslané ke vzdálenému MEP.
- *RxFCl*: Čítač pro rámce přijaté od vzdáleného MEP.

Zpráva LMM PDU obsahuje hodnotu čítače [11]:

- *TxFCf* – zkopírováno z lokálního čítače *TxFCl*.

Zpráva LMR PDU obsahuje hodnoty čítačů [11]:

- *TxFCf* – Hodnota *TxFCf* zkopírovaná z rámce LMM.
- *RxFCf* – Hodnota lokálního čítače *RxFCl* v době příjmu rámce LMM.
- *TxFCb* – Hodnota lokálního čítače *TxFCl* v době odeslání rámce LMR.

Po přijetí zprávy LMR MEP kontrolérem dochází k výpočtu ztrátovosti rámců na obou koncích (blízký konec – near-end, vzdálený konec – far-end). V rovnici 3.8 a 3.9 označuje t_c aktuální čas a t_p čas přijetí/odeslání posledního rámce).

$$\text{Ztrátovost}_{\text{far-end}} = |\text{TxFCb}[t_c] - \text{TxFCb}[t_p]| - |\text{RxFCb}[t_c] - \text{RxFCb}[t_p]| \quad (3.8)$$

$$\text{Ztrátovost}_{\text{near-end}} = |\text{TxFCf}[t_c] - \text{TxFCf}[t_p]| - |\text{RxFCl}[t_c] - \text{RxFCl}[t_p]| \quad (3.9)$$

3.6.5 Syntetické měření ztrátovosti rámců – SLM

SLM (Synthetic Loss Measurement) slouží k měření ztrátovosti rámců mezi dvěma koncovými body MEP v rámci jedné MEG skupiny. K měření se využívá syntetických metod [11].

Na rozdíl od metody měření ztrátovosti LM (Loss Measurement), která pro určení ztrátovosti rámců využívá uživatelských dat, využívá syntetická metoda SLR pro určení ztrátovosti rámců standardizované syntetické rámce SLM PDU a SLR PDU (Synthetic Loss Reply PDU). Tyto syntetické rámce jsou tedy určeny jak pro měření ztrátovosti rámců, tak pro sběr dat. Principem je vysílání měřících rámců přes EVC, a měření ztráty rámců, kterou tyto zprávy zaznamenávají.

V rámci měření pomocí postupu „s jedním koncem“ provádí výpočet pouze řídící MEP nazývaný jako MEP kontrolér. Kontrolér vyšle zprávu SLM jednou za stanovený interval na unicastovou adresu vzdáleného MEP, který odpovídá zprávou SLR. Zprávy se používají ke shromáždění počtu vyslaných SLM a SLR a počtu SLM a SLR obdržených oběma MEP. Pro každého MEP tedy existují dva lokální čítače, což platí i pro různé služby s odlišným CoS ID. Velmi důležitá je tedy synchronizace čítačů na obou koncových zařízeních [11].

- *TxFCl*: Čítač pro SLM zprávy odeslané ke vzdálenému MEP.
- *RxFCl*: Čítač pro odpovědi SLR od vzdáleného MEP.

Zpráva SLM PDU obsahuje hodnoty čítačů [11]:

- *TxFCf* – zkopírováno z lokálního čítače *TxFCl*.

Zpráva SLR PDU obsahuje hodnoty čítačů [11]:

- *TxFCf* – Hodnota *TxFCf* zkopírovaná z rámce SLM.
- *RxFCf* – Hodnota lokálního čítače *RxFCl* v době příjmu rámce SLM.
- *TxFCb* – Hodnota lokálního čítače *TxFCl* v době odeslání rámce SLR.

Po přijetí zprávy SLR MEP kontrolérem dochází k výpočtu ztrátovosti rámců na obou koncích (blízký konec – near-end, vzdálený konec – far-end). V rovnici 3.10 a 3.11 označuje t_c aktuální čas a t_p čas posledního vzorku).

$$\text{Ztrátovost}_{\text{far-end}} = |\text{TxFCf}[t_c] - \text{TxFCf}[t_p]| - |\text{TxFCb}[t_c] - \text{TxFCb}[t_p]| \quad (3.10)$$

$$\text{Ztrátovost}_{\text{near-end}} = |\text{TxFCb}[t_c] - \text{TxFCb}[t_p]| - |\text{RxFCl}[t_c] - \text{RxFCl}[t_p]| \quad (3.11)$$

4 PRAKTICKÁ ČÁST DIPLOMOVÉ PRÁCE

Praktická část diplomové práce se zabývá měřením výkonnosti přístupových IP sítí, návrhem a ověřením funkčnosti zásad pro zajištění kvality služeb QoS a traffic-engineeringu. Pro tyto účely bylo vytvořeno 6 scénářů využívajících různých technologií, které jsou popsány v kapitole 4.2.

Pro samotné měření a vyhodnocení výkonnosti sítě byly použity dva přístroje EXFO FTB-1 Pro opatřené testovací aplikací NetBlazzer V2.

Předmětem měření jsou navržené scénáře aplikované na testovací síť složenou ze směrovačů simulujících přístupovou síť NGA, ve které jsou QoS parametry měřeny a vyhodnocovány dle standardů IETF RFC 2544, IETF RFC 6349 a ITU-T 1564. Výsledky měření jsou vždy vzájemně porovnány v rámci daného testu.

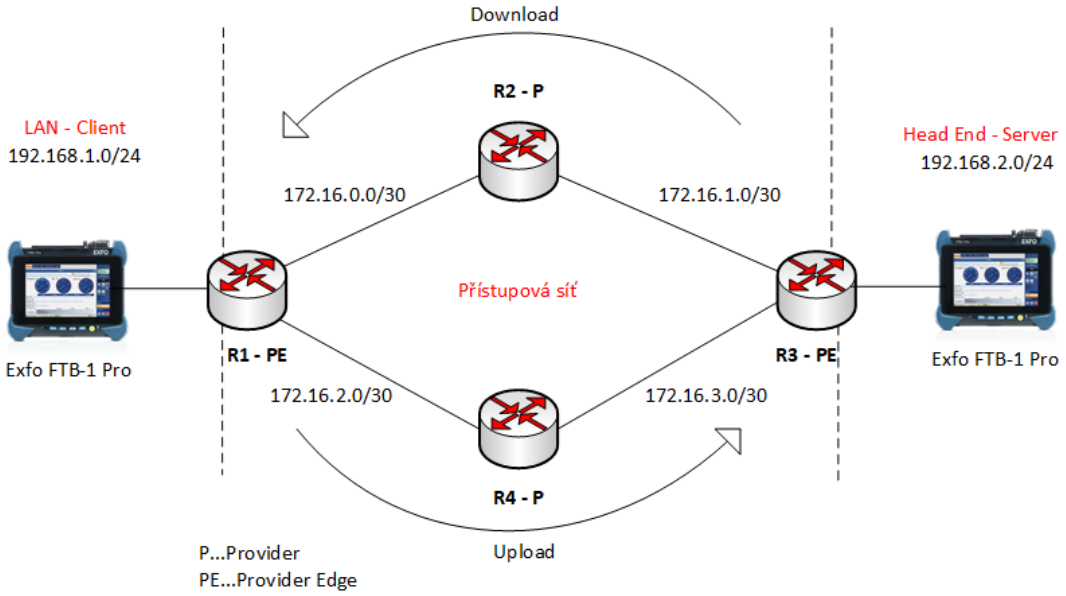
Testování přenosových parametrů v datových sítích je nezbytné pro ověření úrovně kvality poskytovaných služeb garantované v SLA mezi poskytovatelem služeb a zákazníkem. Každý z uvedených testů se však potýká s limity omezujícími jeho využití v konkrétních podmínkách. Tyto limity budou v praktické části diskutovány.

Obr. 4.1: Fotografie měřícího pracoviště.

4.1 Topologie sítě

Základní fyzická topologie testované laboratorní sítě je uvedena na obrázku 4.2. Síťové prvky jsou propojeny strukturovanou kabeláží UTP Cat. 5e. Síť je poskládána ze SOHO (Self-Office Home-Office) zařízení platformy MikroTik viz tabulka 4.1. Jedná se o symetrickou síť s propustností 100 Mbit/s ve směru upload i download,

která modeluje NGA přístupovou síť ethernet. Zvolená propustnost koresponduje s požadavkem pro budování NGA sítí, který uvádí 100 megabitové přístupové sítě.



Obr. 4.2: Základní topologie testovací sítě.

Síť je uspořádána do kruhové topologie s downloadem přes router R2 a uploadem přes router R4 z pohledu klientské LAN sítě. Důvody pro zvolení této varianty jsou:

1. Zálohované spojení mezi sítěmi v případě výpadku R2, R4 a příslušných linek.
2. Rozdělení zátěže a šetření HW prostředků na méně výkonných směrovačích R2 a R4. Zejména šetření prostředků CPU, neboť rozsáhlé značkování paketů, mapování do tříd a obsluha front spotřebují velké množství prostředků CPU. Vysoké zatížení CPU by mohlo vést ke zbytečnému nárůstu zpoždění a jitteru.

Zálohování spojení mezi R1 a R3 je provedeno způsobem zálohování rout mezi sítěmi pro scénáře `OSPF-noQoS`, `DSCP-HTB` a `MPLS-LDP`, tak, že jsou vytvořeny duplicitní routy mezi sítěmi, každá s jinou výchozí bránou inverzně dle směru download či upload (R2 nebo R4), které se liší metrikou. Při správné funkci sítě probíhá přenos po kruhové topologii viz obrázek 4.2, v případě výpadku R2 či R4 probíhá přenos v obou směrech pouze přes jeden z těchto směrovačů, který je momentálně aktivní.

U dalších scénářů využívajících technologií MPLS-TE je zálohování spojení řešeno v rámci traffic-engineeringu, kde je konfigurován primární a sekundární (záložní) tunel. Při výpadku primárního tunelu dochází automaticky k sestavení tunelu záložního a směrování provozu do něj. Primární tunel je sestaven explicitně, pevně nastavenými hopy. Sekundární tunel je sestaven automaticky pomocí technologie CSPF rozšiřující OSPF popsané výše.

Tab. 4.1: Tabulka rozhraní a IP adres.

Směrovač	Rozhraní	IP adresa	Adresa sítě	HW Mikrotik
R1-PE	*eth1* *eth2* *LAN-GW* *Loopback*	172.16.0.1/30 172.16.2.1/30 192.168.1.1/24 1.1.1.1	172.16.0.0/30 172.16.2.0/30 192.168.1.0/24 1.1.1.1	RB962UiGS-5HacT2HnT Verze OS: 6.41.4
R3-PE	*eth1* *eth2* *LAN-GW*	172.16.1.2/30 172.16.3.2/30 192.168.2.1/24 3.3.3.3	172.16.1.0/30 172.16.3.0/30 192.168.2.0/24 3.3.3.3	RB3011UiAS-RM Verze OS: 6.41.4
R2-P	*eth1* *eth2* *Loopback*	172.16.0.2/30 172.16.1.1/30 2.2.2.2	172.16.0.0/30 172.16.1.0/30 2.2.2.2	RB750Gr3 hEX Verze OS: 6.41.4
R4-P	*eth1* *eth2* *Loopback*	172.16.2.2/30 172.16.3.1/30 4.4.4.4	172.16.2.0/30 172.16.3.0/30 4.4.4.4	RB952Ui-5ac2nD Verze OS: 6.41.4

4.2 Popis navržených scénářů

4.2.1 OSPF-noQoS

Jedná se o základní scénář, který slouží jako referenční pro scénáře ostatní. Směrování je prováděno pomocí dynamického směrovacího protokolu OSPF. Dle obrázku topologie sítě 4.2 je využívána kruhová topologie se zálohováním rout v případě výpadku jednoho ze směrovačů R2 nebo R4.

Ve scénáři nejsou nastaveny žádné mechanizmy pro zajištění kvality služeb – QoS. S daty je zacházeno podle mechanizmu best-effort.

Tento scénář je základním scénářem, ze kterého vychází všechny ostatní scénáře, které navíc využívají dalších síťových technologií a zásad QoS.

4.2.2 DSCP HTB

Scénář vychází z předchozího scénáře a topologie na obrázku 4.2. Odlišnost spočívá v aplikaci zásad QoS s využitím mechanizmu diferencovaných služeb.

Pro všechny scénáře byl nakonfigurován univerzální strom front řešící každý směr přenosu individuálně, kdy v každém směru je definováno 8 prioritních tříd. Do těchto tříd je provoz mapován podle DSCP hodnoty. DSCP hodnota je jednotlivým datovým tokům přidělena dle politiky na hraničních směrovačích (R1 a R3) značkováním jednotlivých paketů viz tabulka 4.2. Na vnitřních směrovačích (R2 a R4) jsou pakety

klasifikovány a tříděny do tříd podle hodnoty DSCP, nedochází už ke značkování a změnám DSCP hodnot.

Tab. 4.2: DSCP mapa tříd a značkování provozu v síti.

Třída QoS	**Služba**	**DSCP hodnota**	**DSCP rozsah**	**DSCP třída**	**HTB priorita**
Routine	Ostatní HTTP HTTPS	0 7 7	0 – 7	CS0	8
Priority	FTP	10	8 – 15	CS1, AF11-13	7
Immediate	Exfo-data	18	16 – 23	CS2, AF21-23	6
Flash	–	–	24 – 31	CS3, AF31-33	5
Flash Override	VLC Exfo-IPTV	32 34	32 – 39	CS4, AF41-43	4
Critical	Exfo-VoIP	46	40 – 47	CS5, EF	3
Internetwork Control	OSPF RSVP-TE LDP	48 – –	48 – 55	CS6	2
Network Control	ICMP	56	56 – 63	CS7	1

U mechanizmu diferencovaných služeb dochází k řešení kvality služeb na každém směrovači v rámci DiffServ domény („per-hop“), tudíž je nutná implementace DSCP mapy viz tabulka 4.2 a stromu front viz obrázek 4.6 na každém směrovači. O přidělení DSCP hodnoty paketům se starají hraniční směrovače PE, kterými putuje provoz z/do DiffServ domény.

4.2.3 MPLS-LDP

Scénář koncepčně vychází ze základního scénáře a topologie 4.2. Změnou je využití technologie MPLS, která kombinuje výhody IP sítí a sítí ATM. Jedná se o protokolově nezávislou technologii s cílem maximálně zjednodušit směrování paketů v síti. MPLS pakety jsou směrovány podle návěští (label), které je přiděleno (push) provozu bez návěští na hraničních směrovačích LER. Při směrování pak není třeba kontrolovat celý paket, ale pouze návěští paketu, díky čemuž odpadá také nutnost kontrolovat směrovací IP tabulky na směrovačích.

O distribuci návěští se stará protokol LDP. Pakety se stejným návěštím jsou vždy směrovány stejnou cestou LSP. Pro správnou funkci je nutné na všech směrovačích:

1. Povolit a inicializovat LDP protokol.

2. Přidat rozhraní, která budou využívat LDP v rámci MPLS domény.

Výhodou řešení kvality služeb s technologií MPLS je možnost značení priority dat v 3bitovém experimentálním poli (EXP) záhlaví MPLS rámce. Platforma Mikrotik toto umožňuje nastavením akce `set-priority` při značkování paketů.

Tab. 4.3: Nastavení značkování priority do pole EXP v záhlaví MPLS paketu.

Třída QoS	**Služba**	**DSCP hodnota**	**Nastavení EXP bitů**	**HTB priorita**
Routine	Ostatní HTTP HTTPS	0 7 7	111 (7)	8
Priority	FTP	10	110 (6)	7
Immediate	Exfo-data	18	101 (5)	6
Flash	–	–	100 (4)	5
Flash Override	VLC Exfo-IPTV	32 34	011 (3)	4
Critical	Exfo-VoIP	46	010 (2)	3
Internetwork Control	OSPF RSVP-TE LDP	48 – –	001 (1)	2
Network Control	ICMP	56	000 (0)	1

Další výhodou je řešení QoS a značkování paketů pro oba směry pouze na LER směrovačích. Na směrovačích uvnitř domény pak postačuje nastavit pravidla pouze pro data generovaná směrovačem (*OUTPUT*) a data určená pro směrovač (*INPUT*), což je vhodné řešit i na LER směrovačích.

Veškeré pakety vstupující do MPLS domény jsou tedy klasifikovány, opatřeny návěštím a hodnotou priority zapsanou do EXP pole, mapovány do příslušných tříd a front, ve kterých jsou odbaveny, a podle hodnoty návěští jsou směrovány na další směrovač.

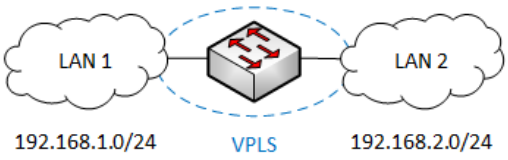
Pakety vystupující z domény jsou klasifikovány podle priority značené v EXP poli, zbaveny návěští (pop), obslouženy v příslušných frontách a směrovány k cíli.

4.2.4 MPLS-VPLS

Tento scénář využívá technologie virtuální privátní sítě na linkové vrstvě (L2VPN), která využívá principů technologie MPLS. Jedná se o emulovanou lokální síť LAN nad MPLS. O distribuci návěští se stará protokol LDP.

Výhodou tohoto řešení je možnost sdílení broadcastové domény geograficky odděleným místům tak, že tato místa propojí pomocí pseudovláken PW (Pseudo Wires). Všechny služby ve VPLS se pak zdají být ve stejné síti LAN bez ohledu na jejich umístění.

Celá VPLS síť se z pohledu koncového zákazníka tváří jako jediný přepínač či most viz obrázek 4.3 . Principy klasifikace, značkování a mapování paketů do tříd a front jsou shodné se scénářem `MPLS-LDP`. Výhodné je obdobně jako u scénáře předchozího, že QoS je řešeno pouze na hraničních směrovačích VPLS domény.



Obr. 4.3: VPLS síť z pohledu koncového uživatele.

Pro zajištění zálohy spojení při výpadku směrovačů R2, R4 a příslušných spojů, byly pro transport VPLS využity TE tunely v obou směrech. Konkrétně se tedy jedná o technologii VPLS-over-TE. TE tunely slouží také k omezení množství pseudovláken mezi PE směrovači. Samotná pseudovlákna by komplikovala směrování po kruhové topologii, neboť by data v naší síti putovala jedním ze dvou možných pseudovláken bez možnosti výběru. Nastavení TE tunelů bude rozebráno u dalšího scénáře. Pro nastavení MPLS-VPLS je nutné:

1. Nastavit CSPF na všech směrovačích pro využití TE.
2. Konfigurovat VPLS rozhraní na R1 a R3.
3. Vytvořit síťový most pro L2VPN na R1 a R3, a přidat LAN porty a VPLS rozhraní do mostu.
4. Nastavit MPLS-TE rozhraní na všech směrovačích.
5. Konfigurovat TE tunely (hlavní a záložní).
6. Konfigurovat TE rozhraní a přidělit TE tunely k rozhraním na R1 a R3.
7. Směrovat provoz do VPN mostu mezi sítěmi LAN.

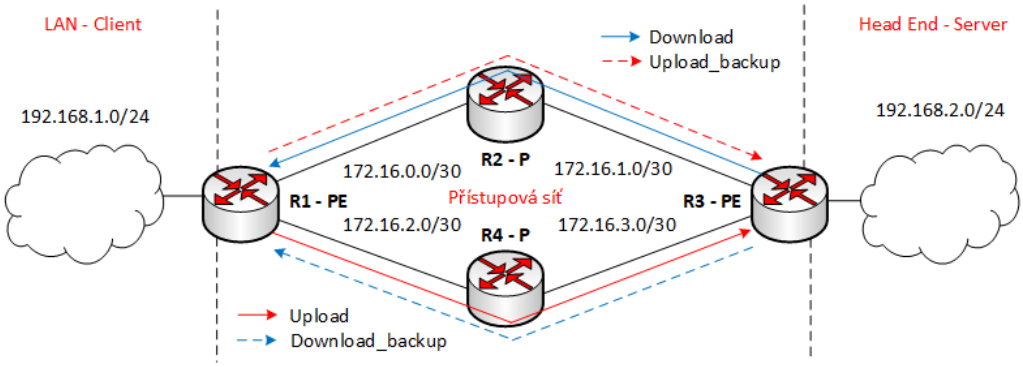
4.2.5 MPLS-TE-D-U

MPLS-TE podporuje vysoké využití přenosové kapacity. Taková síť se výborně vypořádává s výpadky uzlů a poruchami spojů. V rámci MPLS-TE jsou funkce traffic engineeringu implementovány do síťové vrstvy z důvodu optimalizace směrování paketů.

MPLS-TE automaticky vytváří a udržuje LSP v MPLS doméně pomocí protokolu RSVP-TE, který slouží také k rezervaci zdrojů podél celé přenosové cesty. Výhodou

je, že mezi hraničními směrovači je vytvořen TE tunel a veškerá konfigurace a správa propustnosti, priority atp. již probíhá pouze na hraničních směrovačích.

Klasifikace, značkování a mapování paketů probíhá stejným principem jako u scénáře MPLS-LDP dle tabulky 4.3. Výhodné je, že zásady QoS jsou aplikovány pouze na vstupech a výstupech do/z TE tunelů v obou směrech.



Obr. 4.4: Topologie sítě s TE tunely pro download a upload.

Na každém hraničním směrovači (R1 a R3) bylo vytvořeno jedno TE rozhraní, ke kterému byly přiřazeny dva tunely s propustností 100 Mbit/s v každém směru – primární a záložní tunel.

Primární (výchozí) tunel je vytvořen explicitně, tak, že jsou pevně nastaveny hopy, kudy má být tunel sestaven. Konkrétně upload přes R4 a download přes R2. Sekundární tunel je automaticky sestaven po výpadku primárního tunelu s využitím technologie CSPF (Constrained Shortest Path First), která najde nejkratší cestu sítí při úvaze dostupné šířky pásma, požadované šířky pásma, metriky a priority. Stejný princip je zvolen i u tunelů ve scénáři s VPLS.

Pro nastavení MPLS-TE tunelů je nutné:

1. Nastavení CSPF na všech směrovačích pro využití TE.
2. Nastavení MPLS-TE rozhraní na všech směrovačích.
3. Konfigurace primárního a záložního TE tunelu na R1 a R3.
4. Konfigurace TE rozhraní a přidělení tunelů k rozhraním na R1 a R3.
5. Směrování provozu do TE rozhraní (vstup do TE tunelu).

4.2.6 MPLS-TE-5Tun

Koncepčně obdobný scénář jako MPLS-TE-D-U. Odlišností je vytvoření pěti TE rozhraní a tunelů v každém směru provozu, což umožňuje větší flexibilitu sítě a snazší správu jednotlivých datových toků směrovaných do příslušných tunelů. Ke každému TE rozhraní jsou přiřazeny dva TE tunely – primární a záložní. Na obrázku 4.5 nejsou záložní tunely znázorněny, neboť jsou sestavovány automaticky

pomocí technologie CSPF až po výpadku směrovačů R2 či R4. V rozsáhlé síti by bylo velmi obtížné předvídat, kudy bude záložní tunel sestaven, v měřené síti je situace o poznání jednodušší a záložní tunel je sestaven vždy přes směrovač, který není ve výpadku.

Tab. 4.4: Mapování služeb do TE tunelů.

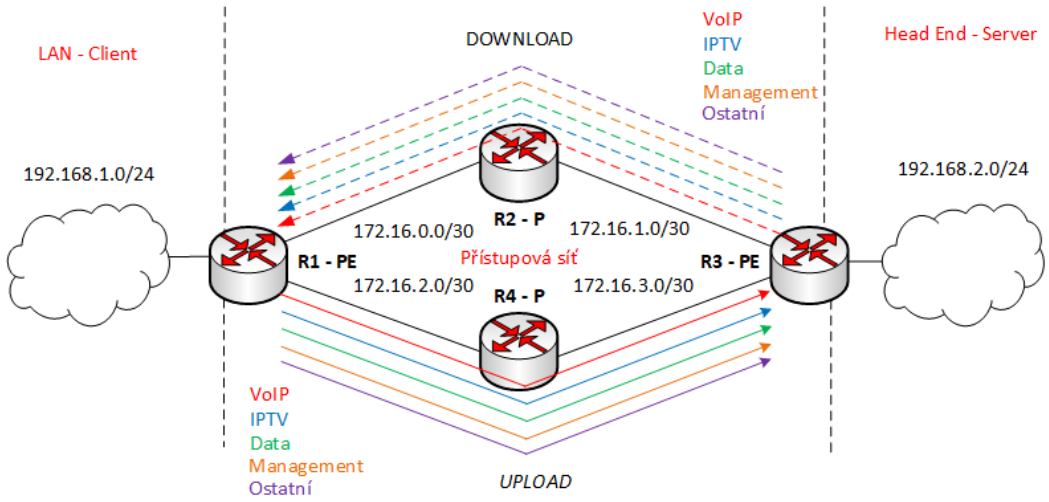
Služba	**Chain**	**MPLS-TE tunel**	**Propustnost [Mbit/s]**
End-to-End			
Exfo-VoIP	forward	VoIP	15
Exfo-IPTV VLC	forward	IPTV	30
Exfo-Data FTP HTTP/HTTPS	forward	Data	25
ICMP	forward	Management	5
Ostatní	forward	Other	25
Router-Router			
OSPF	input output	–	–
LDP	input output	–	–
RSVP-TE	input output	–	–

Konkrétně jsou vytvořeny zvláštní TE rozhraní a tunely pro služby typu VoIP, IPTV (video), data, management a ostatní provoz dle tabulky 4.4, jak je znázorněno na obrázku 4.5. Řídící informace vzájemně si vyměňované mezi směrovači nejsou řazeny do žádného tunelu.

QoS a značkování paketů je řešeno podle tabulky 4.3 obdobně jako v případě předchozího scénáře se dvěma tunely a scénáře MPLS-LDP. Navíc je přidána akce `routing-mark`, aby bylo možné směrovat každý provoz do příslušného tunelu.

4.3 QoS třídy a strom front

Všechny scénáře s nastavenou podporou mechanizmů QoS využívají navržený strom front s nastaveními vyplývajícími z obrázku 4.6. Strom řeší každý směr provozu



Obr. 4.5: Topologie sítě s TE tunely pro jednotlivé služby.

(download a upload) zvlášť, a spolu s klasifikací a značkováním paketů je nejdůležitějším prvkem návrhu QoS. Pro návrh stromu byla zvolena metoda HTB (Hierarchical Token Bucket). Jedná se o metodu řazení paketů do front podle tříd, která umožňuje manipulaci s různými druhy provozu.

HTB umožňuje vytvářet hierarchickou strukturu front a určovat vztahy mezi frontami, například „rodič-potomek“ nebo „potomek-potomek“.

Jakmile má fronta alespoň jednoho potomka, stane se vnitřní frontou (fronty upload a download), všechny fronty bez potomků jsou „listy stromu“. Listy pak obsluhují jednotlivé třídy. Vnitřní fronty jsou zodpovědné pouze za distribuci provozu.

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters

Name	Parent	Packet Marks	Queue Type	Priority	Limit At (b...	Max Limit ...
QoS_Download	global	Download_packet_mark	default-small	1	100M	100M
1_Network_Control_Dwl	QoS_Download	Network_Control_DWL	default-small	1	5M	100M
2_Internetwork_Control_Dwl	QoS_Download	Internetwork_Control_DWL	default-small	2	5M	100M
3_Critical_Dwl	QoS_Download	Critical_DWL	pcq-download-default	3	15M	75M
4_Flash_Override_Dwl	QoS_Download	Flash_Override_DWL	pcq-download-default	4	20M	75M
5_Flash_Dwl	QoS_Download		default-small	5	5M	50M
6_Immediate_Dwl	QoS_Download	Immediate_DWL	default-small	6	10M	50M
7_Priority_Dwl	QoS_Download	Priority_DWL	default-small	7	15M	30M
8_Other_Dwl	QoS_Download	Routine_DWL	default-small	8	25M	30M
QoS_Upload	global	Upload_packet_mark	default-small	1	100M	100M
1_Network_Control_Upl	QoS_Upload	Network_Control_UPL	default-small	1	5M	100M
2_Internetwork_Control_Upl	QoS_Upload	Internetwork_Control_UPL	default-small	2	5M	100M
3_Critical_Upl	QoS_Upload	Critical_UPL	pcq-upload-default	3	15M	75M
4_Flash_Override_Upl	QoS_Upload	Flash_Override_UPL	pcq-upload-default	4	20M	75M
5_Flash_Upl	QoS_Upload		default-small	5	5M	50M
6_Immediate_Upl	QoS_Upload	Immediate_UPL	default-small	6	10M	50M
7_Priority_Upl	QoS_Upload	Priority_UPL	default-small	7	15M	30M
8_Other_Upl	QoS_Upload	Routine_UPL	default-small	8	25M	30M

Obr. 4.6: Navržený HTB strom front.

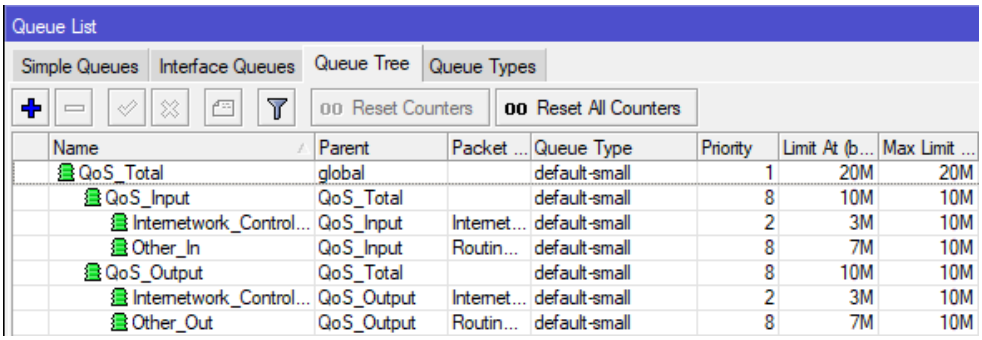
`Limit At` značí garantovanou propustnost pro danou třídu v Mbit/s. `Max-Limit` určuje maximální šířku pásma, kterou může služba využít nad rámec garantované propustnosti v případě, že není využívána jinými třídami. `Priority` určuje HTB prioritu třídy (1-8), přičemž nejvyšší prioritu značí hodnota 1. `Parent` určuje příslušnost třídy v rámci stromové struktury. `Packet Marks` definuje, jak značkované pakety přísluší dané třídě.

Pakety jsou na vstupním rozhraní nejprve klasifikovány, poté jsou značkovány podle příslušnosti paketů k třídě, odbaveny ve frontách příslušících třídě a směrovány sítí. Klasifikace a značkování paketů probíhá na základě zvolené síťové politiky uvedené v popisech jednotlivých scénářů. Pakety generované testery Exfo FTB-1 Pro přijdou dle služby k hraničnímu směrovači již označkovány hodnotou DSCP a ta jim je zachována.

Pro třídu Critical, do které jsou řazeny pakety VoIP telefonie, a pro třídu Flash Override, do které jsou řazeny video služby, byl zvolen typ fronty PCQ (Per Connection Queue). Fronta PCQ zajistí spravedlivé rovnoměrné rozdělení šířky pásma mezi jednotlivé uživatele služby. V praxi to znamená, že pokud je celková šířka pásma např. pro třídu Critical 15 Mbit/s a zároveň tuto třídu využívá 5 účastníků (5 VoIP relací), pak každému náleží 1/5 celkové šířky pásma, tedy 3 Mbit/s. Ostatní služby využívají výchozí frontu na platformě Mikrotik – default-small.

Klasifikace, mapování paketů do tříd, značkování paketů, návrh propustností tříd a parametrů front vychází z doporučení společnosti Cisco viz [22] a MikroTik viz [18] s ohledem na provoz v měřené síti. Názvy tříd jsou převzaty z názvů tříd IPP (IP Precedence).

Jak již bylo zmíněno, scénář DSCP využívá navržený strom na každém směrovači. Scénáře využívající technologii MPLS pouze na hraničních směrovačích. Z tohoto důvodu byl pro vnitřní MPLS směrovače sestaven zvláštní zjednodušený strom pro podporu QoS při přenosu řídících a směrovacích informací mezi směrovači v rámci domény viz obrázek 4.7. Do tohoto stromu jsou mapovány protokoly OSPF, RSVP-TE a LDP, podle toho, které protokoly jsou v daném scénáři využívány.



Name	Parent	Packet ...	Queue Type	Priority	Limit At (b...	Max Limit ...
QoS_Total	global		default-small	1	20M	20M
QoS_Input	QoS_Total		default-small	8	10M	10M
Internetwork_Control...	QoS_Input	Internet...	default-small	2	3M	10M
Other_In	QoS_Input	Routin...	default-small	8	7M	10M
QoS_Output	QoS_Total		default-small	8	10M	10M
Internetwork_Control...	QoS_Output	Internet...	default-small	2	3M	10M
Other_Out	QoS_Output	Routin...	default-small	8	7M	10M

Obr. 4.7: QoS na vnitřních (provider) směrovačích.

4.4 Základní měření QoS parametrů

Základní měření, určené pro ověření funkčnosti nastavených mechanizmů, proběhlo pro všechny nakonfigurované scénáře na zatížené i nezatížené síti.

Zatížení bylo simulováno videostreamem v obou směrech z jedné LAN sítě do druhé pomocí programu VLC a stahováním dat z FTP serveru v obou směrech pomocí programu FileZilla.

Testování spočívalo v měření hodnoty latence pomocí stanice Linux Ubuntu 14.10 LTS a nástroje ping, který využívá pro měření latence pakety ICMP. Stanice byla umístěna v serverové LAN síti za R3. Naměřená hodnota latence je průměrem latence z 60 paketů ICMP Ping (1 paket/sekunda).

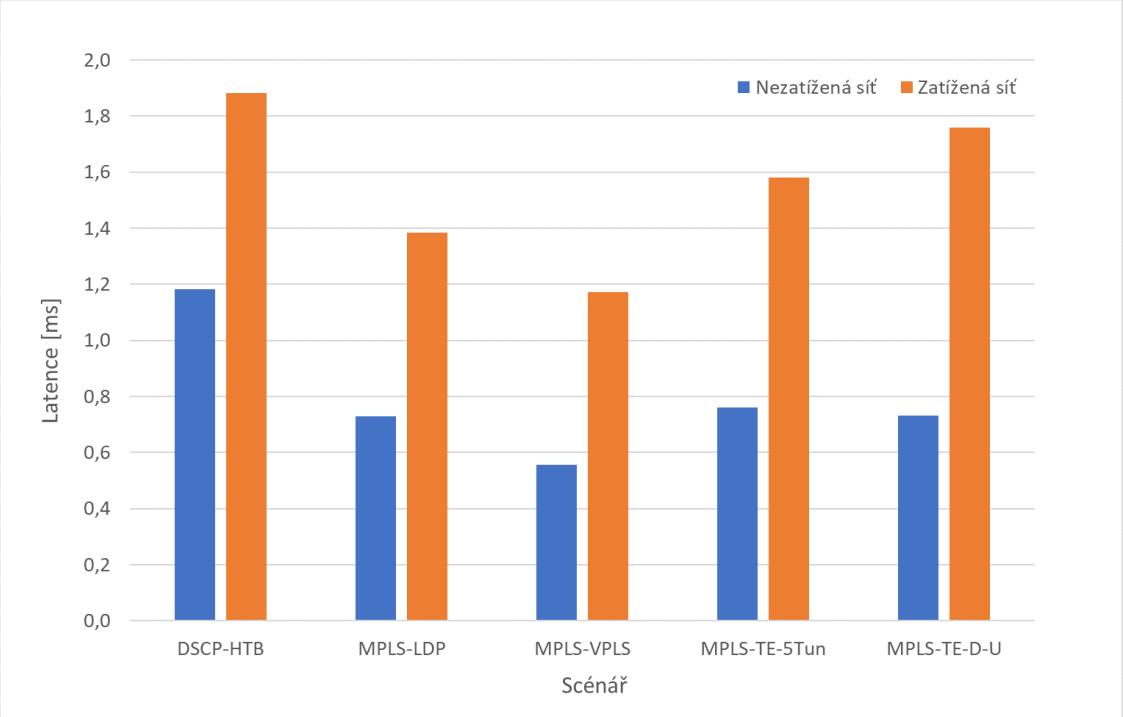
Naměřené hodnoty jsou uvedeny v tabulce 4.5 a porovnání latence jednotlivých scénářů je znázorněno na grafu 4.8. Z grafu byla záměrně vyloučena hodnota latence základního scénáře bez zásad QoS – `OSPF-noQoS`, neboť tato best-effort síť při zatížení vykazovala několikanásobně větší latenci, než scénáře s aplikovanými zásadami QoS, což by snižovalo úroveň porozumění grafu. To také značí vhodně nastavené zásady QoS, neboť se u ostatních scénářů podařilo hodnotu obousměrného zpoždění snížit cca 30x oproti scénáři bez QoS.

Zároveň byla sledována i subjektivní kvalita videí, která u scénářů se zásadami QoS nebyla při zatížení sítě pocitově nijak zhoršena oproti kvalitě na nezatížené síti. Při výše zmíněném zatížení došlo zejména k omezení přenosové rychlosti stahování dat z FTP serveru, což je ale žádaný jev, protože služby přenosu dat by měly využívat zbytkovou šířku pásma a být obsluhovány ve frontách s nižší prioritou. Video služba jevila v síti best-effort občasné známky trhání obrazu při uvedeném zatížení.

Tab. 4.5: Tabulka základních náměrů latence pomocí ICMP paketů.

	Latence [ms]	
Stav sítě	*Nezatížená*	*Zatížená*
OSPF-noQoS	0,547	53,586
DSCP-HTB	1,182	1,883
MPLS-LDP	0,729	1,383
MPLS-VPLS	0,555	1,172
MPLS-TE-D-U	0,732	1,758
MPLS-TE-5Tun	0,760	1,580

Nejnižší hodnotu latence vykazuje nezatížená síť v základní konfiguraci, což je dáno tím, že nedochází ke klasifikaci, značkování a zpracování paketů ve frontách. Stejný důvod se však negativně projeví na velikosti latence již při relativně nízkém zatížení sítě, natož pak při přetížení sítě.



Obr. 4.8: Porovnání základních náměrů nezatížené a zatížené sítě.

Nejnižší latenci ze sítí se zásadami QoS vykazuje VPLS síť, která oproti ostatním scénářům využívajícím směrování paketů na L3 umožňuje rychlejší přenos na L2, a s tím spojené nižší obousměrné zpoždění. Scénáře s technologií MPLS a MPLS-TE vykazují téměř shodné hodnoty latence. Nejvyšší latenci ze všech scénářů s QoS vykazuje scénář `DSCP-HTB`, což je dáno tím, že klasifikace paketů do tříd a zpracování ve frontách je prováděno na každém směrovači v rámci DiffServ domény.

4.5 Testování dle IETF RFC 2544

Pro generování a vyhodnocování testovacího provozu testu RFC 2544, který byl proveden v loopback módu, slouží měřící přístroj EXFO FTB-1 Pro umístěný v serverové LAN síti. Druhý měřící přístroj EXFO FTB-1 Pro umístěný v klientské LAN síti slouží jako loopback zařízení v režimu smart loopback.

Jednotlivé subtesty testu RFC 2544 již byly uvedeny v teoretické části práce. Součástí testu není test kolísání zpoždění (Jitter), který doporučení nedefinuje. Test je poměrně rozsáhlý, proto z něho jsou vybrány pouze podstatné údaje.

Při testování byly vypnuty HTB stromy front zajišťující funkce QoS. Tento test není vhodný pro testování jednotlivých služeb a QoS. Pokud bychom v každém scénáři chtěli testovat triple-play služby, znamenalo by to cca 18 testů, což při dlouhé době trvání jednoho testu a omezené době zapůjčení měřícího přístroje nebylo časově

možné. Zachována však byla klasifikace a značkování paketů, které se promítají do výsledků. Výše zmíněný zvolený přístup tak umožňuje náhled na vlastnosti samotné technologie, kterou daný scénář využívá.

Pojmem zpoždění je ve všech částech textu míněno obousměrné zpoždění, nazývané také jako latence a RTT.

4.5.1 Naměřené hodnoty dle RFC 2544

Tab. 4.6: Naměřené hodnoty dle RFC 2544 – scénář OSPF-noQoS.

Velikost rámce [B]	**Latence [ms]**	**Ztrátovost [%]**	**Propustnost L2 [Mbit/s]**	**Propustnost L3 [Mbit/s]**
64	0,1710	0,542	59,6190	42,8511
128	0,9186	0,082	85,4053	73,3952
256	0,4556	0	92,7536	86,2318
512	1,2581	0	96,2406	92,8571
1024	1,4457	0	98,0842	96,3601
1280	1,6466	0	98,4615	97,0769
1518	1,7520	0	98,6996	97,5292

Tab. 4.7: Naměřené hodnoty dle RFC 2544 – scénář DSCP-HTB.

Velikost rámce [B]	**Latence [ms]**	**Ztrátovost [%]**	**Propustnost L2 [Mbit/s]**	**Propustnost L3 [Mbit/s]**
64	0,2177	4,853	49,4254	35,5241
128	0,3952	3,772	65,0655	55,9155
256	1,4824	1,566	89,6333	83,3310
512	2,1368	0,364	95,1656	91,8199
1024	2,4787	0,212	98,0843	96,3602
1280	3,2232	0	98,4615	97,0769
1518	2,8613	0	98,6996	97,5292

Tab. 4.8: Naměřené hodnoty dle RFC 2544 – scénář MPLS-LDP.

Velikost rámce [B]	**Latence [ms]**	**Ztrátovost [%]**	**Propustnost L2 [Mbit/s]**	**Propustnost L3 [Mbit/s]**
64	0,1842	5,431	14,9523	10,7470
128	0,2215	2,538	18,0534	15,5146
256	0,3039	1,096	54,7826	50,9307
512	1,2966	0,226	95,6390	92,2767
1024	2,7659	0	98,0842	96,3601
1280	2,5641	0	98,4615	97,0769
1518	2,5089	0	98,6996	97,5292

Tab. 4.9: Naměřené hodnoty dle RFC 2544 – scénář MPLS-VPLS.

Velikost rámce [B]	**Latence [ms]**	**Ztrátovost [%]**	**Propustnost L2 [Mbit/s]**	**Propustnost L3 [Mbit/s]**
64	0,1977	66,619	4,3809	3,1418
128	0,2514	29,437	18,9189	16,2584
256	0,3304	10,537	36,2651	33,7152
512	0,4650	10,202	38,4962	37,1428
1024	0,7672	3,525	69,2720	68,0543
1280	0,9365	2,092	85,5384	84,3355
1518	1,1012	17,153	66,6222	65,8322

Tab. 4.10: Naměřené hodnoty dle RFC 2544 – scénář MPLS-TE-D-U.

Velikost rámce [B]	**Latence [ms]**	**Ztrátovost [%]**	**Propustnost L2 [Mbit/s]**	**Propustnost L3 [Mbit/s]**
64	0,1972	55,284	33,8095	24,3005
128	0,2393	4,593	78,5945	67,5422
256	2,4075	1,475	91,5941	85,1539
512	1,6536	0,243	95,6390	92,2767
1024	4,01221	0	98,0842	96,3601
1280	4,0285	0	98,4615	97,0769
1518	3,1435	0	98,6996	97,5292

Tab. 4.11: Naměřené hodnoty dle RFC 2544 – scénář MPLS-TE-5Tun.

Velikost rámce [B]	**Latence [ms]**	**Ztrátovost [%]**	**Propustnost L2 [Mbit/s]**	**Propustnost L3 [Mbit/s]**
64	0,2732	96,538	3,5238	2,5327
128	0,2867	89,979	10,8108	9,2905
256	0,3532	68,020	13,3333	12,3958
512	0,4748	27,346	38,4962	37,1428
1024	0,7499	5,730	77,8543	76,4858
1280	3,2195	0	95,3845	94,0432
1518	2,7159	0	98,6996	97,5292

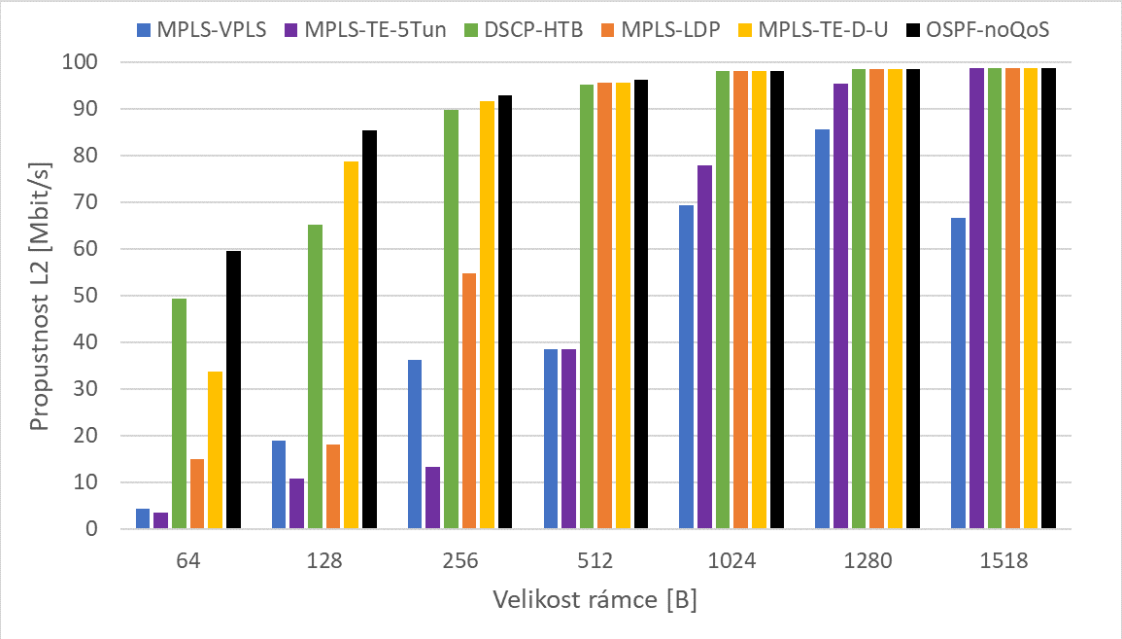
4.5.2 Vyhodnocení testu RFC 2544

Propustnost

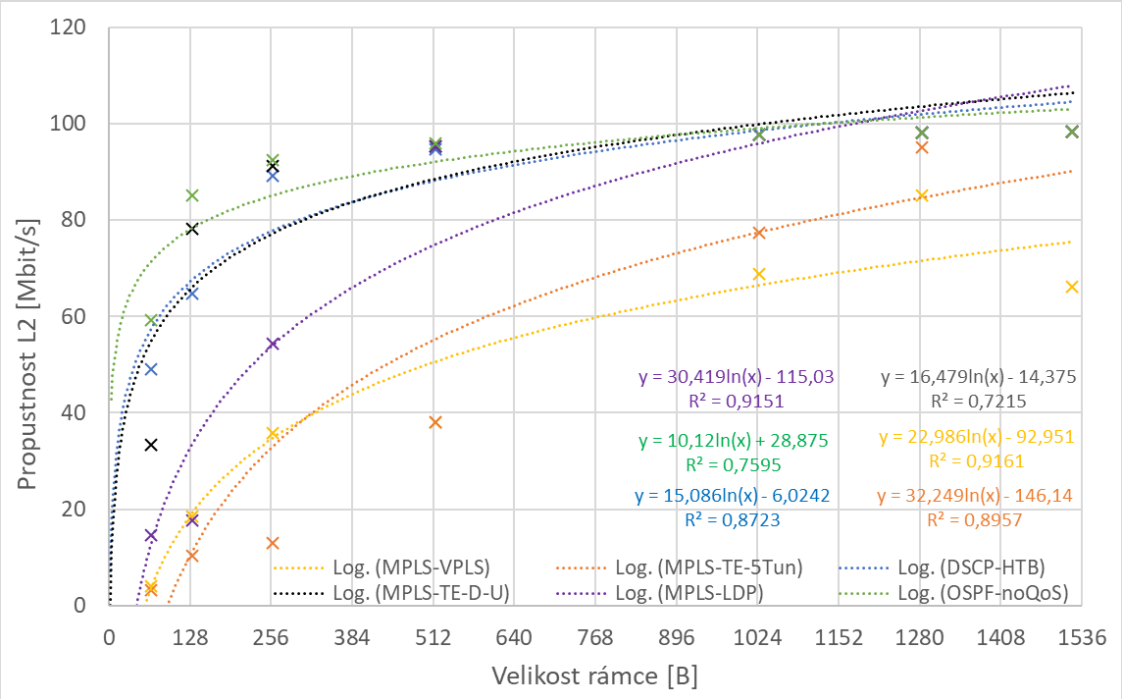
Zajímavostí je rozdíl mezi propustností na síťové (L3) a linkové (L2) vrstvě referenčního modelu OSI/ISO. Propustnost na linkové vrstvě je logicky vyšší. Princip plyne z fungování jednotlivých vrstev modelu. Směrovače pracující na síťové vrstvě s logickými adresami, kde směrování probíhá zpravidla softwareově, což navyšuje i celkové zpoždění oproti hardwareovému přepínání u switchů. Při příchodu paketu ke směrovači je nutné rozbalit IP paket, ze záhlaví zjistit kam má být paket dále směrován, snížit hodnotu TTL a přepočítat kontrolní součet. Poté je paket znovu zabalen s novými hodnotami záhlaví a směrován dále směrem k cílové IP adrese. Směrovač musí navíc udržovat a prohledávat dvě tabulky. První tabulka udržuje záznamy pro relace mezi MAC adresou, logickou adresou a rozhraním pro přímo připojené uzly. Druhá tabulka udržuje seznam sítí s rozhraním kudy je k dané síti nejvýhodnější cesta. K těmto úkonům u přepínačů, které provádí přepínání rámců zpravidla hardwareově, a na linkové vrstvě, nedochází. Při příchodu rámce na přepínač dochází pouze k nahlédnutí do MAC záhlaví rámce pro zjištění cílové adresy MAC a porovnání cílové adresy se záznamy v jediné tabulce na přepínači. Pokud je cílová MAC adresa známá, přepínač odešle rámec na rozhraní, kde se host s cílovou MAC adresou nachází. Pokud není cílová MAC adresa známá, směrovač se zachová jako hub a broadcastově vyšle rámec na všechny porty bez většího zpoždění. Hardwareové přepínání s přepínači na L2 tedy výrazně přispívá snížení zpoždění.

Rozdíly propustnosti mezi L2 a L3 jsou nejvyšší pro rámce velikosti 64 B, kde je pro všechny scénáře rozdíl propustností cca 28 %. Pro rámce velikostí 128 B pak cca 14 %, 256 B pak cca 7 % a 512 B pak cca 3,5 %. Pro velké rámce velikosti 1024 B, 1280 B a 1518 B se hodnoty liší pouze minimálně s rozdíly v intervalu od 1,18 % do 1,76 %. Pravidelnost a závislost procentuálních rozdílů na velikostech rámců

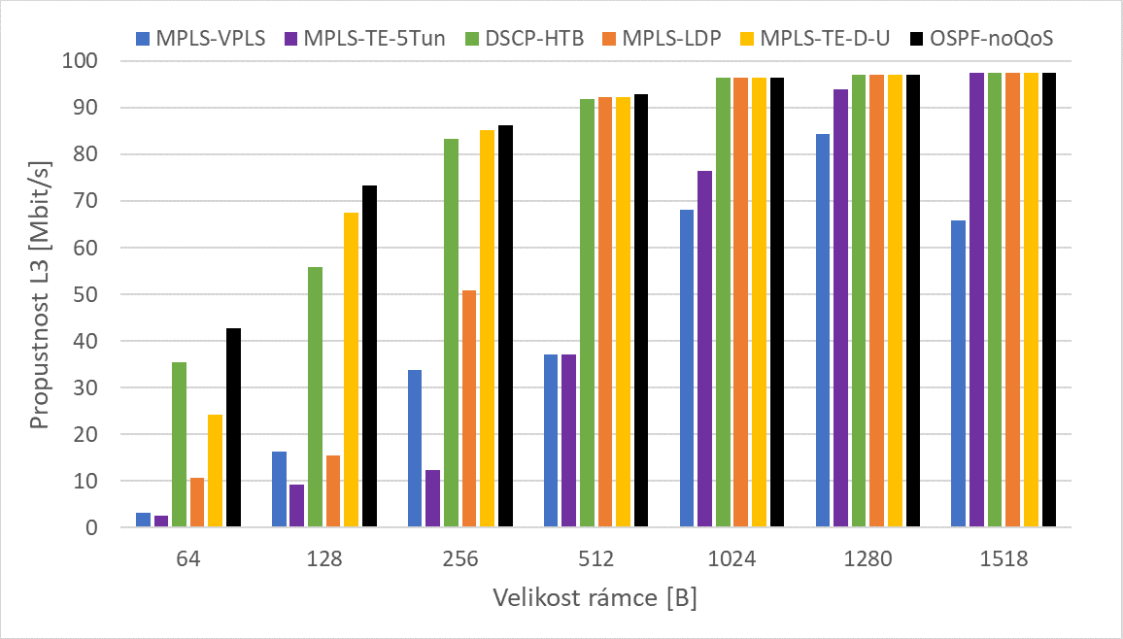
ve všech scénářích vyplývá nejspíše z principu algoritmu měření a vyhodnocování propustností.



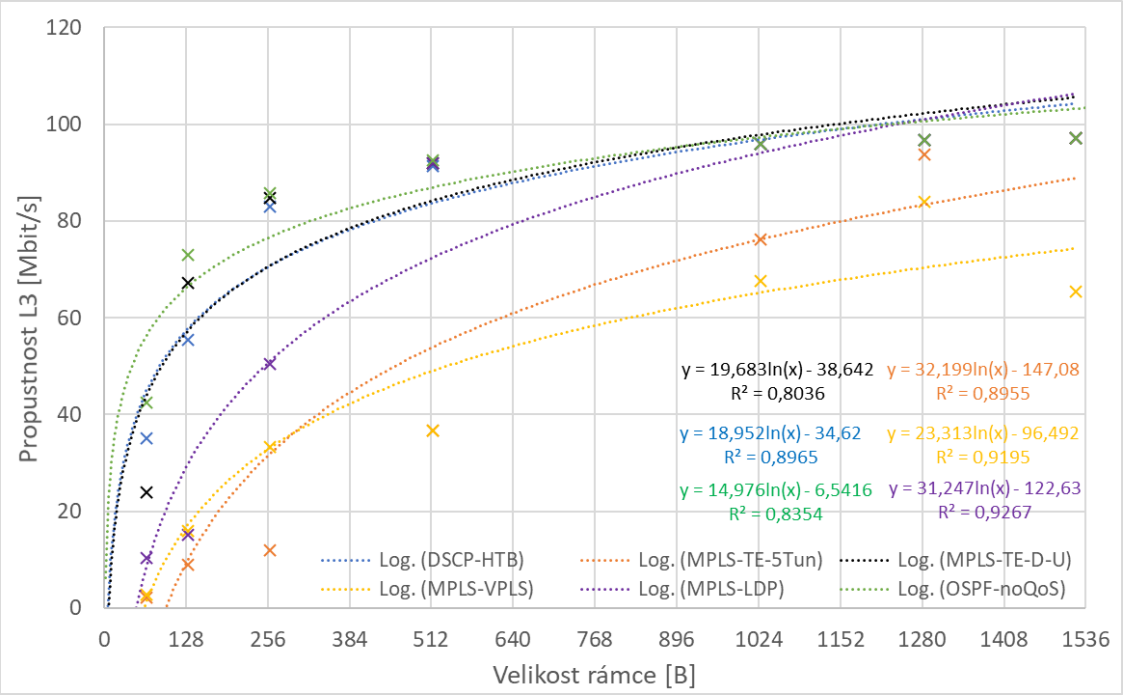
Obr. 4.9: Porovnání propustnosti na L2 pro všechny scénáře dle RFC 2544.



Obr. 4.10: Závislost L2 propustnosti na velikosti rámce dle RFC 2544 – všechny scénáře.



Obr. 4.11: Porovnání propustnosti na L3 pro všechny scénáře dle RFC 2544.



Obr. 4.12: Závislost L3 propustnosti na velikosti rámce dle RFC 2544 – všechny scénáře.

Naměřené hodnoty v grafech 4.10 a 4.12, jsou aproximovány logaritmickou funkcí, která vystihuje trend zvyšování propustnosti s rostoucí velikostí ethernetového rámce. Celková propustnost na L2 i L3 vrstvě tedy roste logaritmicky s velikostí etherne-

tového rámce. To je dáno tím, že při stejném objemu přenesených dat je proces směrování/přepínání prováděn méněkrát, než pro menší rámce. Zvýšená režie pro menší rámce a případné zahlcení síťového prvku těmito rámci pak způsobují nižší propustnost. Na druhou stranu však přenos větších rámců trvá déle než přenos rámců menších kvůli delší době zpracování na směrovačích. U velkých rámců může navíc docházet k fragmentaci, která se odvíjí od maximální nastavené hodnoty MTU v síti, a negativně se projeví na celkovém zpoždění.

Nejvyšší propustností pro všechny velikosti rámců obecně disponovala základní síť s nastaveným OSPF směrováním – `OSPF-noQoS`, která však vykazovala obdobné hodnoty jako scénáře `MPLS-TE-D-U`, `DSCP-HTB` a od velikosti rámců 512 B i `MPLS-LDP`. Nízké hodnoty propustnosti, zejména pro rámce velikosti 64–512 B, vykazují scénáře `MPLS-VPLS`, `MPLS-TE-5Tun`. U scénáře s pěti tunely bude na vině zpracování paketů, konkrétně značkování směrování (`routing-mark`) pro nastavení směrování provozu do příslušného tunelu, které vytěžuje CPU. Usuzujeme tak, neboť scénář `MPLS-TE-D-U` využívá stejnou technologii, ale pouze 1 tunel v každém směru, přičemž do 1 tunelu není nutné datový přenos nijak klasifikovat. U scénáře s technologií VPLS může být nižší propustnost způsobena vytížením CPU a paměti, nebo vinou softwareové implementace VPLS v RouterOS, se kterou se Mikrotik potýkal od verze 6.37.

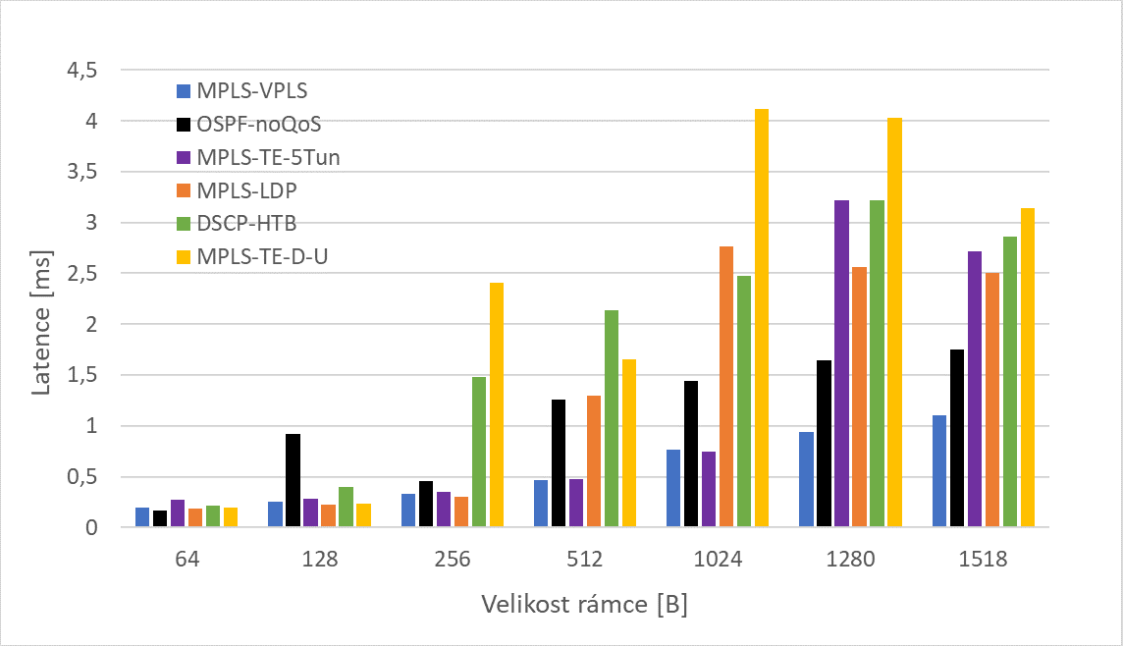
Latence

Jak již bylo uvedeno, přenos větších rámců je pomalejší než přenos rámců menších kvůli pomalejšímu odbavení na směrovačích. Vliv hraje také fragmentace na L3, která zvyšuje celkové zpoždění.

Z grafu 4.13 vyplývá, že nejnižší hodnotu latence vykazuje scénář s technologií VPLS. Je to dáno tím, že technologie VPLS vytváří L2 VPN spojení mezí LAN sítěmi, umožňující rychlejší přenos dat na úrovni L2. Síla technologie VPLS je patrná zejména u rámců větších než 1024 B, kde vykazuje latenci i více než o 50 % nižší než ostatní technologie, vyjma scénáře `OSPF-noQoS`. Tento scénář vykazuje nízkou hodnotu latence kvůli tomu, že nevyužívá značkování a klasifikaci paketů.

Podle testu RFC 2544 je dle náměrů latence vhodnější posílat data pěti tunely než tunelem jedním, což je nejspíš způsobeno vzájemným ovlivňováním se velkého množství dat v jednom tunelu. Data v jednotlivých tunelech se nijak ovlivňovat nemohou. Scénář `MPLS-TE-D-U` vykazuje nejvyšší latenci ze všech testovaných.

Vyšší hodnoty latence vykazuje také scénář `DSCP-HTB`, což je zapříčiněno značkováním a klasifikací paketů na hraničních směrovačích, a klasifikací paketů na směrovačích ostatních. Dle výsledků se však klasifikace na každém hopu výrazně nepromítá do celkové latence v porovnání s ostatními technologiemi při současném zatížení. La-



Obr. 4.13: Porovnání závislostí latence na velikosti rámce dle RFC 2544 – všechny scénáře.

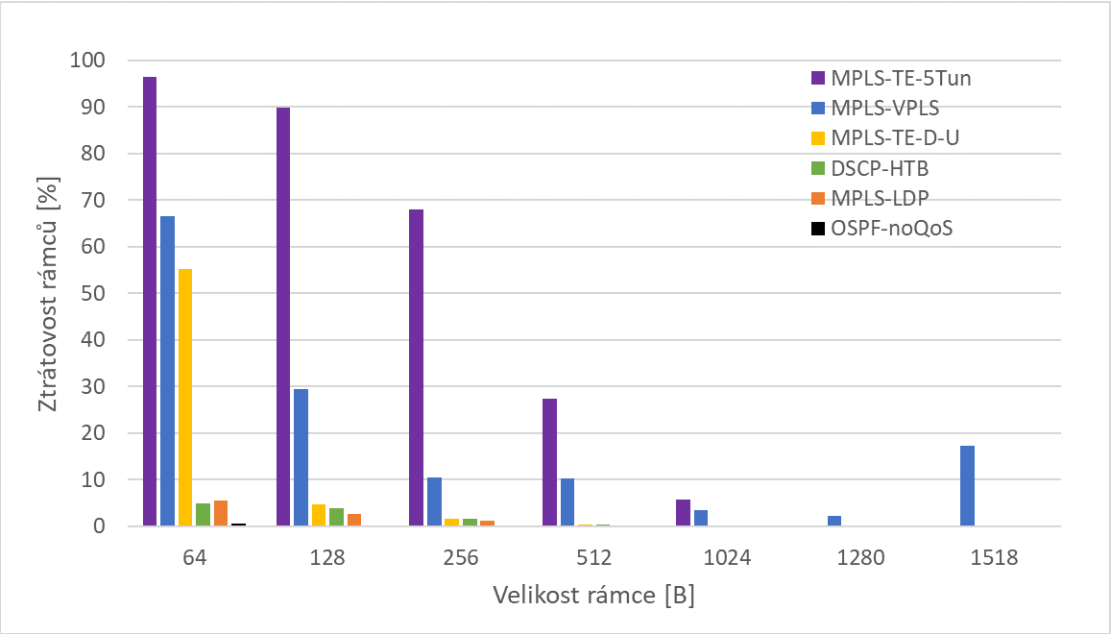
tence by oproti ostatním scénářům ještě nepatrně narostla v případě využití QoS, tedy HTB stromu front a zpracování paketů v nich na každém hopu v cestě.

Střední hodnoty latence vykazuje scénář `MPLS-LDP`, který využívá technologii MPLS a distribuci návěští pomocí protokolu LDP.

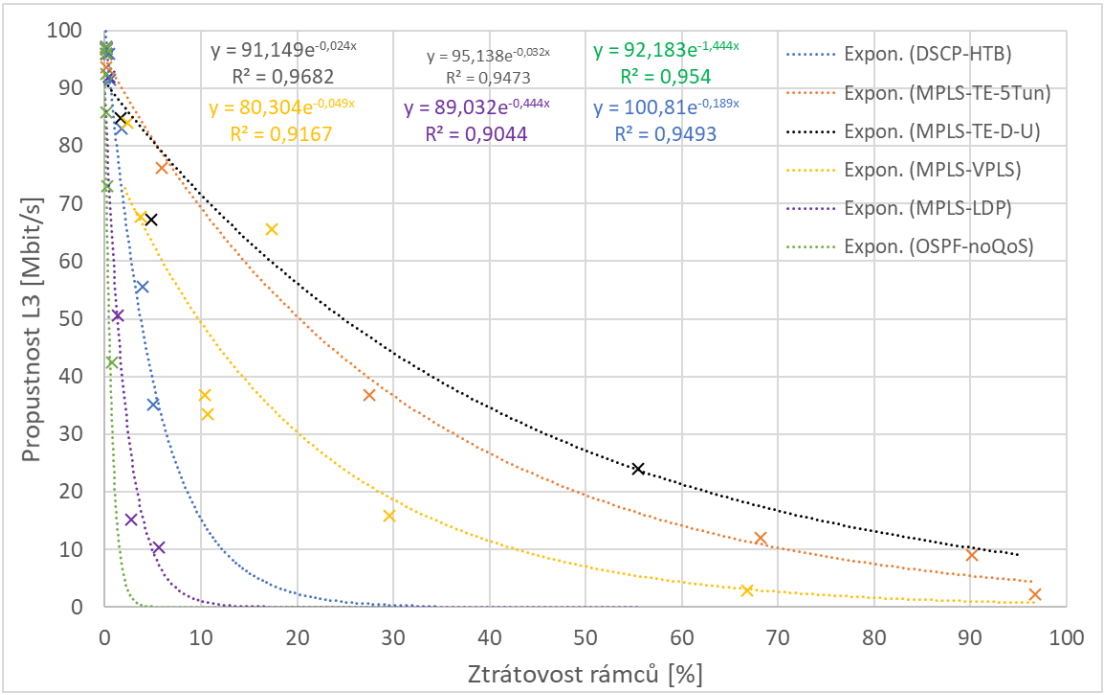
Ztrátovost rámců

Všechny scénáře vykazují nejvyšší míru ztrátovosti pro rámce malé velikosti 64 B a 128 B. Vysoká míra ztrátovosti malých rámců je způsobena zahlcením směrovačů velkým množstvím malých rámců, a s tím spojenou vyšší režií než u rámců vetší velikosti. Router při zahlcení již není schopen zpracovávat množství příchozích paketů, a tak dochází k jejich zahazování.

Zajímavostí je souvislost datové propustnosti na L2 a L3 a ztrátovosti rámců. Scénáře `MPLS-VPLS` a `MPLS-TE-5Tun` vykazovali nízkou datovou propustnost viz graf 4.11. Na grafu 4.14 je patrná ekvivalentní vysoká ztrátovost rámců. Obecně lze z grafu 4.15 usoudit, že L3 propustnost pro všechny scénáře exponenciálně roste se snižující se ztrátovostí rámců. Exponenciální závislost bude obdobně platit i pro závislost L2 propustnosti na ztrátovosti rámců. Důvody nízké propustnosti již byly zmíněny u hodnocení propustnosti a váží se i ke ztrátovosti rámců. Ostatní scénáře vykazovali nízkou či nulovou hodnotu ztrátovosti při vysoké propustnosti, zejména pak pro rámce velikosti 512 B – 1518 B.



Obr. 4.14: Porovnání závislostí ztrátovosti rámců na velikosti rámce dle RFC 2544 – všechny scénáře.



Obr. 4.15: Závislost L3 propustnosti na ztrátovosti rámců dle RFC 2544 – všechny scénáře.

4.6 Testování dle ITU-T Y.1564 SAM

Test EtherSAM dle doporučení ITU-T Y.1564 byl proveden ve dvou částech za použití režimu smart-loopback. V první části byla síť proměřena z LAN za R3 (R3 –> R1), tedy s měřícím a vyhodnocovacím testerem v serverové LAN a testerem v režimu loopback v klientské LAN. V druhé části naopak.

Pro EtherSAM test byly nastaveny tři standardní služby nabízené v rámci triple play. Jedná se o hlasovou službu (10 hovorů, kodek G.711), přenos videa simulující IPTV (5 kanálů, MPEG-2) a standardní službu přenosu dat. Parametry nastavení jednotlivých služeb včetně jejich prahových hodnot dle standardu MEF 23.1 jsou uvedeny v tabulce 4.12.

Tab. 4.12: Nastavení parametrů testovaných služeb dle MEF 23.1.

Služba	**Frame Size [B]**	**CIR [Mbit/s]**	**Jitter [ms]**	**Latency [ms]**	**Frame Loss Rate [–]**	**DSCP**
VoIP	138	1,264	20	120	0,001	46
Video	1374	19,8613	30	150	0,001	34
Data	Random	10,000	55	200	0,001	18

Všechny služby mimo VoIP byly testovány do hranice CIR, která je ve frontách na směrovačích MikroTik nazývána jako `Limit-At`. Konkrétně video služby přísluší do třídy Flash-Override s Limit-At 20 Mbit/s, služby přenosu dat do třídy Immediate s Limit-At 10 Mbit/s a VoIP do třídy Critical s Limit-At 15 Mbit/s.

Po ukončení testu je možné vygenerovat rozsáhlý a podrobný report s výsledky testů. Tento report je pro prezentaci příliš rozsáhlý, proto byla vybrána pouze důležitá data z testu výkonnosti služeb, při němž jsou testovány všechny služby současně. Výsledky jsou uvedeny v tabulkách 4.13 a 4.14.

Pojmem zpoždění je při hodnocení míněno obousměrné zpoždění, nazývané také jako latence a RTT.

4.6.1 Vyhodnocení testu EtherSAM

Test dle standardu ITU-T Y.1564 je prováděn na síťové vrstvě s využitím UDP datagramů. Nejnižší hodnoty latence ve všech případech vykazovala služba VoIP, pro kterou je tento parametr společně se ztrátovostí a jitterem kritický. Služba VoIP totiž využívá ze všech služeb nejmenší velikost datových jednotek. Pro menší datové jednotky je přenos rychlejší a latence nižší. Hodnoty jitteru byly pro všechny služby ve všech testovaných scénářích velmi nízké.

Tab. 4.13: Naměřené hodnoty pomocí testu EtherSAM – část I.

	OSPF-noQoS		**DSCP-HTB**		**MPLS-TE-D-U**	
Směr	L -> R	R -> L	L -> R	R -> L	L -> R	R -> L
BER [–]	0	0	0	0	0	0
VoIP						
CIR [Mbit/s]	1,264	1,264	1,264	1,264	1,264	1,264
Latence [ms]	0,788	0,785	1,194	1,105	1,034	1,057
Jitter [ms]	0,151	0,150	0,196	0,229	0,220	0,228
Ztrátovost [–]	0	0	0	0	0	0
Propustnost [Mbit/s]	1,2639	1,2640	1,2615	1,2620	1,2630	1,2634
Video						
CIR [Mbit/s]	19,8613	19,8613	19,8613	19,8613	19,8613	19,8613
Latence [ms]	0,930	0,927	1,349	1,313	1,173	1,198
Jitter [ms]	<0,015	<0,015	0,080	0,106	0,066	0,074
Ztrátovost [–]	0	0	0	0	0	0
Propustnost [Mbit/s]	19,8602	19,8613	19,8229	19,8440	19,8466	19,8521
Data						
CIR [Mbit/s]	10	10	10	10	10	10
Latence [ms]	0,808	0,804	1,238	1,186	1,064	1,088
Jitter [ms]	0,155	0,155	0,179	0,195	0,187	0,194
Ztrátovost [–]	0	0	0	0	0	0
Propustnost [Mbit/s]	9,9995	10	9,9806	9,991	9,9923	9,9954

Pozn.: L...serverová LAN (R3), R...klientská LAN (R1)

VoIP provoz je vhodné odesílat v menších paketech, neboť se přenáší relativně malé množství dat. Důvodem je narůst zpoždění při plnění větších paketů do hodnoty MTU a nastavení vyrovnávacích pamětí na straně příjemce. Při příjmu větších paketů by mohlo dojít k přetečení vyrovnávací paměti a nárůstu jitteru, který je pro VoIP službu kritický.

Naopak pro přenos videa je lepší zvolit větší velikost paketu, neboť se přenáší velké množství dat. Spojování velkého množství jednotlivých fragmentů by znamenalo zbytečné navýšení zpoždění.

Porovnání scénářů

Z grafů 4.16 a 4.17, které porovnávají latenci v obou směrech měření, vyšly nejlepší a téměř shodné hodnoty obousměrného zpoždění pro scénáře `MPLS-VPLS` a `MPLS-LDP`. Uplatňují se zde výhody rychlosti přenosu technologie VPLS vytvářející L2 VPN

Tab. 4.14: Naměřené hodnoty pomocí testu EtherSAM – část II.

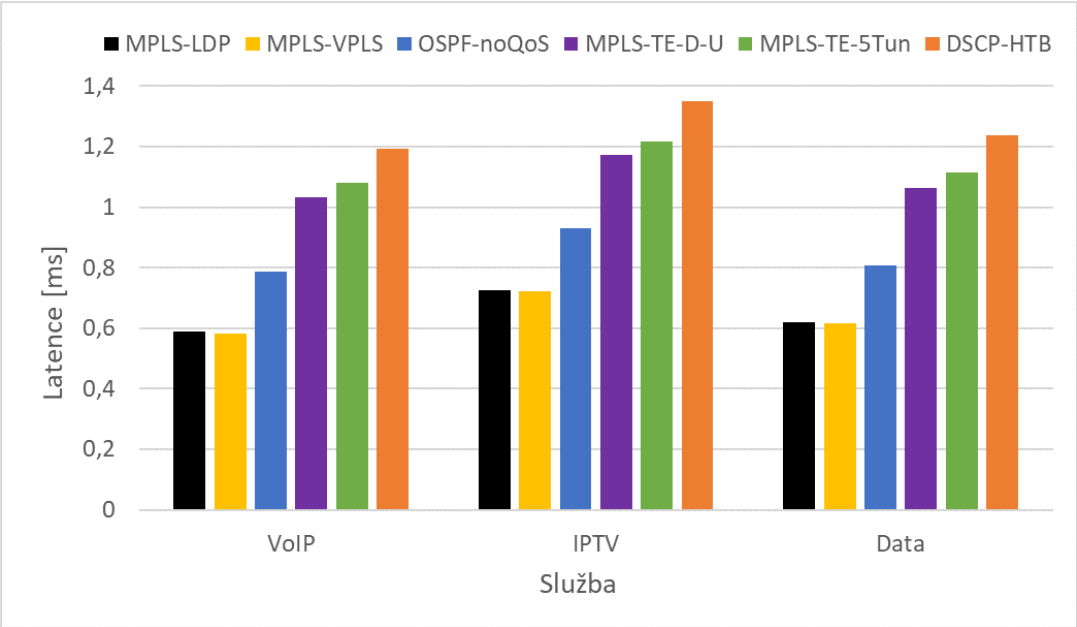
	MPLS-LDP		**MPLS-VPLS**		**MPLS-TE-5Tun**	
Směr	L -> R	R -> L	L -> R	R -> L	L -> R	R -> L
BER [–]	0	0	0	0	0	0
VoIP						
CIR [Mbit/s]	1,264	1,264	1,264	1,264	1,264	1,264
Latence [ms]	0,588	0,605	0,581	0,629	1,079	0,972
Jitter [ms]	0,160	0,173	0,163	0,199	0,223	0,209
Ztrátovost [–]	0	0	0	0	0	0
Propustnost [Mbit/s]	1,2639	1,2630	1,2628	1,2630	1,2620	1,2628
Video						
CIR [Mbit/s]	19,8613	19,8613	19,8613	19,8613	19,8613	19,8613
Latence [ms]	0,725	0,811	0,722	0,851	1,217	1,116
Jitter [ms]	0,026	0,026	0,022	0,033	0,067	0,061
Ztrátovost [–]	0	0	0	0	0	0
Propustnost [Mbit/s]	19,8595	19,8590	19,8441	19,8600	19,8365	19,8497
Data						
CIR [Mbit/s]	10	10	10	10	10	10
Latence [ms]	0,619	0,680	0,615	0,729	1,113	1,001
Jitter [ms]	0,147	0,157	0,146	0,187	0,190	0,183
Ztrátovost [–]	0	0	0	0	0	0
Propustnost [Mbit/s]	9,9960	9,9980	9,9912	9,9920	9,9851	9,9928

Pozn.: L...serverová LAN (R3), R...klientská LAN (R1)

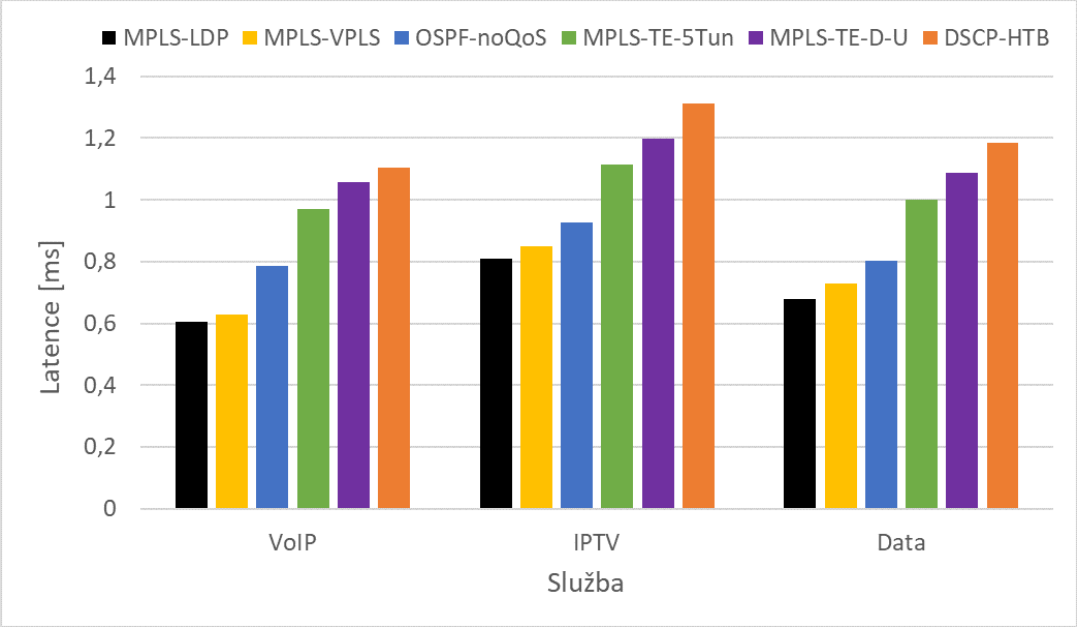
spojení mezi LAN sítěmi a výhody multiprotokolového přepínání rámců podle návěští pomocí protokolu LDP. Latence pro tyto scénáře je přibližně o 50 % nižší než u scénáře `DSCP-HTB`, který vykazuje nejvyšší hodnotu latence, jejíž příčinou je, jak již bylo zmíněno u RFC 2544, klasifikace a zpracování paketů v HTB stromu front na každém směrovači v přenosové cestě.

Nízké hodnoty latence vykazují i scénáře s MPLS-TE tunely. Nepatrně vyšší latenci jeví scénář `MPLS-TE-5Tun`, což je způsobeno značkováním paketů pro směrování dat do příslušného TE tunelu (`routing-mark`).

Střední hodnoty latence vykazuje scénář `OSPF-noQoS`. Je to dáno tím, že byl zvolen přístup testování do hranice 100 % CIR, neboť je tato hodnota definována ve smlouvě SLA. Síť tedy byla celkově zatížena pouze cca z 30 %, což nemohlo výrazně zhoršit naměřené hodnoty jitteru a latence. Pokud by se však taková síť bez mechanizmů QoS přetížila více, nastal by nekontrolovatelný nárůst zpoždění a jitteru,



Obr. 4.16: Porovnání latence pro jednotlivé služby – směr R3 –> R1.



Obr. 4.17: Porovnání latence pro jednotlivé služby – směr R1 –> R3.

jak je možné pozorovat u základního měření viz tabulka 4.5, kde byla síť zatížena pro ověření funkčnosti QoS. U ostatních scénářů QoS by došlo pouze k nepatrnému nárůstu latence a jitteru v řádu maximálně několika jednotek milisekund.

Test nachází své uplatnění zejména ve fázi aktivace služeb a při ověřování úrovně kvality poskytovaných služeb definované v SLA. V měřených scénářích všechny služby vyhověly s dostatečnou rezervou prahovým hodnotám definovaným v do-

poručení MEF 23.1. Scénář `OSPF-noQoS` však pouze podmínečně, a to při nízkém zatížení sítě.

4.7 Testování dle IETF RFC 6349

Scénáře byly proměřeny také pomocí testu ExacTCP dle standardu RFC 6349. Tento test umožňuje provádět měření na transportní (L4) vrstvě OSI/ISO modelu, s využitím TCP segmentů pro transport dat, což předchozí testy neumožňovaly. S výhodou lze provádět testování non-realtime end-to-end služeb, pro které je charakteristický bezchybný přenos dat s využitím spolehlivého TCP protokolu.

Test nelze provést jinak než v obousměrném režimu (DTS), neboť je nutná vzájemná komunikace testovacích stran a sestavení TCP relace.

Naměřená hodnota MTU není žádným překvapením. Jedná se o typickou hodnotu 1500 B, která je charakteristická pro technologii ethernet. Velikost okna byla automaticky nastavena na 6 kB (2x3kB). Testovány byly dvě TCP spojení v každém směru, pro něž byla nastavena garantovaná propustnost CIR 10 Mbit/s. Měření probíhalo na nezatížené laboratorní síti, díky čemuž je efektivita TCP protokolu ve všech případech téměř stoprocentní.

Pojmem zpoždění je při hodnocení míněno obousměrné zpoždění, nazývané také jako latence a RTT.

Aktuální propustnost

Hodnota aktuální propustnosti znázorněná v grafu 4.18 značí propustnost na transportní vrstvě (L4). Hodnoty naměřené propustnosti na L2 a L3 testem RFC 2544 při porovnání s hodnotami naměřenými testem ExacTCP na L4 znázorňují odlišnosti testů. Zatímco RFC 2544 měří propustnost pro jednotlivé velikosti rámců, ExacTCP řeší propustnost komplexně pro službu. Moderní test ExacTCP měří celkovou propustnost na L4, tak i zdali je testovaným TCP spojením dostupná garantovaná propustnost CIR a KPI parametry dle SLA s využitím různých velikostí rámců, tak jak se běžně děje na reálné síti. Test RFC 2544 navíc stejně jako EtherSAM využívá protokolu UDP.

Nevhodnost měření propustnosti testem RFC 2544 u technologie VPLS značí porovnání propustnosti v tabulkách 4.9 a 4.15. Ze srovnání je patrné, že hodnota propustnosti na L4 by převyšovala propustnost na L3 a ještě vyšší propustnost na L2, což je vyloučené. Ostatní scénáře také vykazují nižší propustnosti na L2 a L3 než L4, ovšem pouze pro rámce malé velikosti.

Z testu ExacTCP vyplývá, že nejvyšší L4 propustnost vykazuje základní scénář, což je dáno absencí klasifikace a značkování paketů, a také zpracováním paketů ve

Tab. 4.15: Naměřené hodnoty testem dle doporučení IETF RFC 6349.

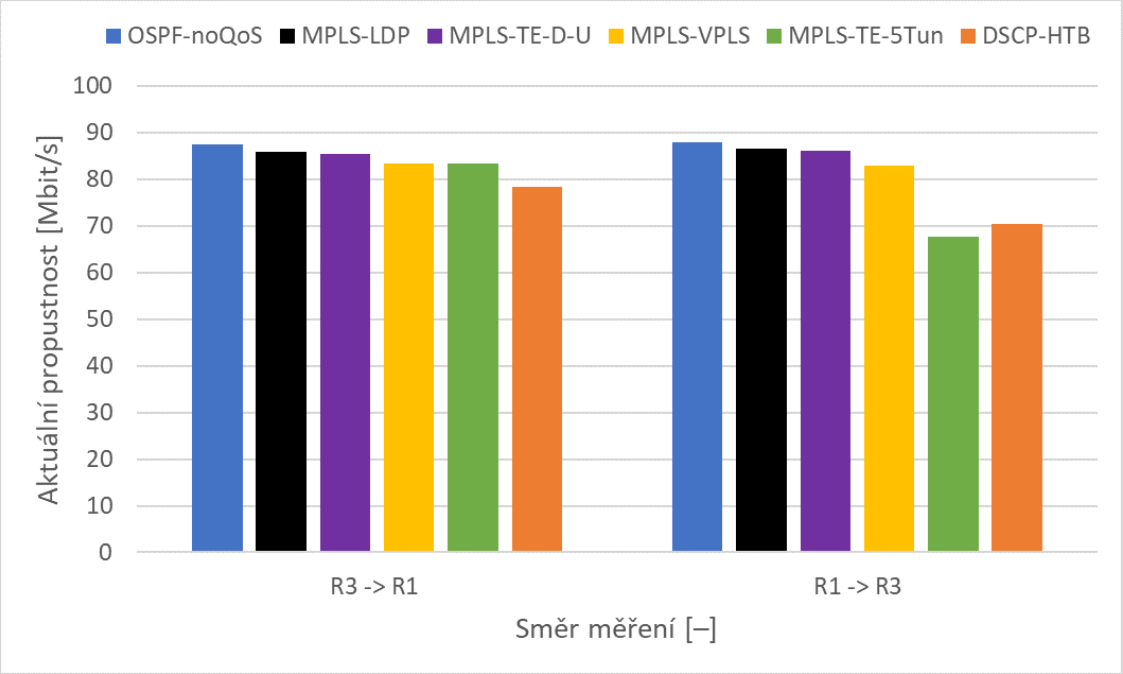
	OSPF-noQoS		**DSCP-HTB**	
Směr	L ->R	R ->L	L ->R	R ->L
MTU [B]	1500		1500	
Latence [ms]	0,632		0,706	
Aktuální propustnost [Mbit/s]	87,4	88	78,4	70,4
Ideální propustnost [Mbit/s]	9,4	9,4	9,4	9,4
TCP Efektivita [%]	99,99	99,99	99,89	99,81
Velikost okna [kB]	6	6	6	6
Zpoždění bufferu [%]	25,54	24,58	25,67	39,74
	MPLS-LDP		**MPLS-TE-D-U**	
Směr	L ->R	R ->L	L ->R	R ->L
MTU [B]	1500		1500	
Latence [ms]	0,644		0,649	
Aktuální propustnost [Mbit/s]	86	86,6	85,5	86,1
Ideální propustnost [Mbit/s]	9,4	9,4	9,4	9,4
TCP Efektivita [%]	99,99	99,99	99,99	99,99
Velikost okna [kB]	6	6	6	6
Zpoždění bufferu [%]	25,25	24,40	25,03	24,16
	MPLS-VPLS		**MPLS-TE-5Tun**	
Směr	L ->R	R ->L	L ->R	R ->L
MTU [B]	1500		1500	
Latence [ms]	0,632		0,636	
Aktuální propustnost [Mbit/s]	83,4	83	83,5	67,6
Ideální propustnost [Mbit/s]	9,4	9,4	9,4	9,4
TCP Efektivita [%]	99,99	99,99	99,88	99,91
Velikost okna [kB]	6	6	6	6
Zpoždění bufferu [%]	27,13	28,14	31,34	40,25

Pozn.: 2x TCP spojení v každém směru vel. okna 6kB (2x3kB)
L...Local (serverová LAN) R...Remote (klientská LAN)

frontách stromu. Nejnižší propustností pak disponuje scénář `DSCP-HTB`. Propustnost je snížena klasifikací paketů a zpracováním ve frontách na každém směrovači v přenosové cestě. U ostatních scénářů využívajících technologii MPLS je L4 propustnost obdobná.

Ve všech scénářích vyhověla propustnost pro vybrané služby požadavkům CIR. Testovaná spojení také s přehledem vyhověli prahové hodnotě maximálního obou-

směrného zpoždění pro služby přenosu dat rovné 150 ms dle MEF 23.1.

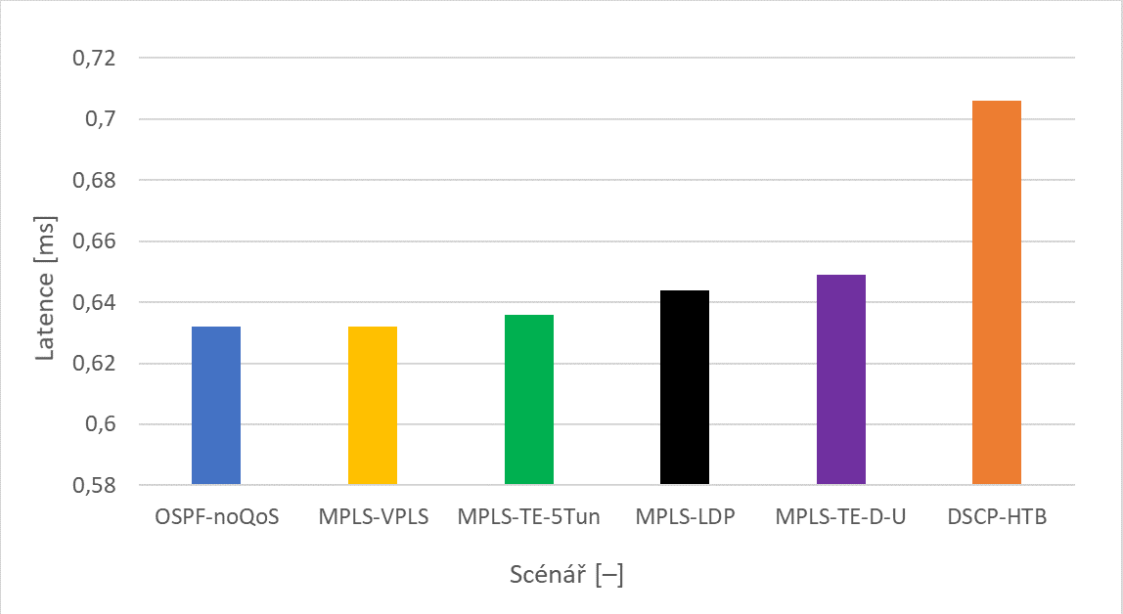


Obr. 4.18: Porovnání L4 propustnosti všech scénářů dle doporučení RFC 6349.

Latence

Graf 4.19 znázorňuje porovnání naměřených hodnot latence pro jednotlivé scénáře. Stejně jako v případě testů RFC 2544 a EtherSAM vykazuje nejnižší zpoždění základní scénář bez QoS, který není zatížen přídavným zpožděním při klasifikaci paketů, značkování paketů a odbavování paketů ve frontách. Shodné hodnoty latence však dosahuje i scénář `MPLS-VPLS`, kde se opět ukazuje výhoda L2 VPN spojení mezi LAN sítěmi. I s nastavenou klasifikací paketů, značkováním paketů a zpracováním paketů ve frontách HTB stromu tak lze dosáhnout velmi nízkého obousměrného zpoždění. Velmi nízké hodnoty latence vykazují i scénáře s TE tunely a scénář `MPLS-LDP`.

Přibližně o 10 % vyšší zpoždění než ostatní scénáře vykazuje scénář `DSCP-HTB`, což je dáno principem zpracování paketů „per-hop“. Toto zpoždění je ze všech scénářů nejvyšší, avšak dostatečně nízké, aby neovlivnilo kvalitu služby a vyhovělo MEF 23.1 jako u ostatních scénářů.



Obr. 4.19: Porovnání latence všech scénářů dle doporučení RFC 6349.

Zpoždění vyrovnávací paměti

Rozdíly jsou viditelné u zpoždění vyrovnávací paměti, které představuje nárůst RTT vůči referenční hodnotě RTT během testu TCP propustnosti. Referenční hodnota RTT je vlastní přenosové trase bez zatížení. Nejvyšší hodnoty zpoždění vyrovnávací paměti vykazuje scénář `MPLS-TE-5Tun`. Ostatní scénáře vykazují hodnoty okolo 25 %.

Porovnání propustnosti na L2, L3 a L4

V grafu 4.20 jsou porovnány maximální naměřené propustnosti v jednotlivých scénářích. Propustnost na L2 a L3 dle standardu RFC 2544 a L4 dle RFC 6349 (test ExacTCP).

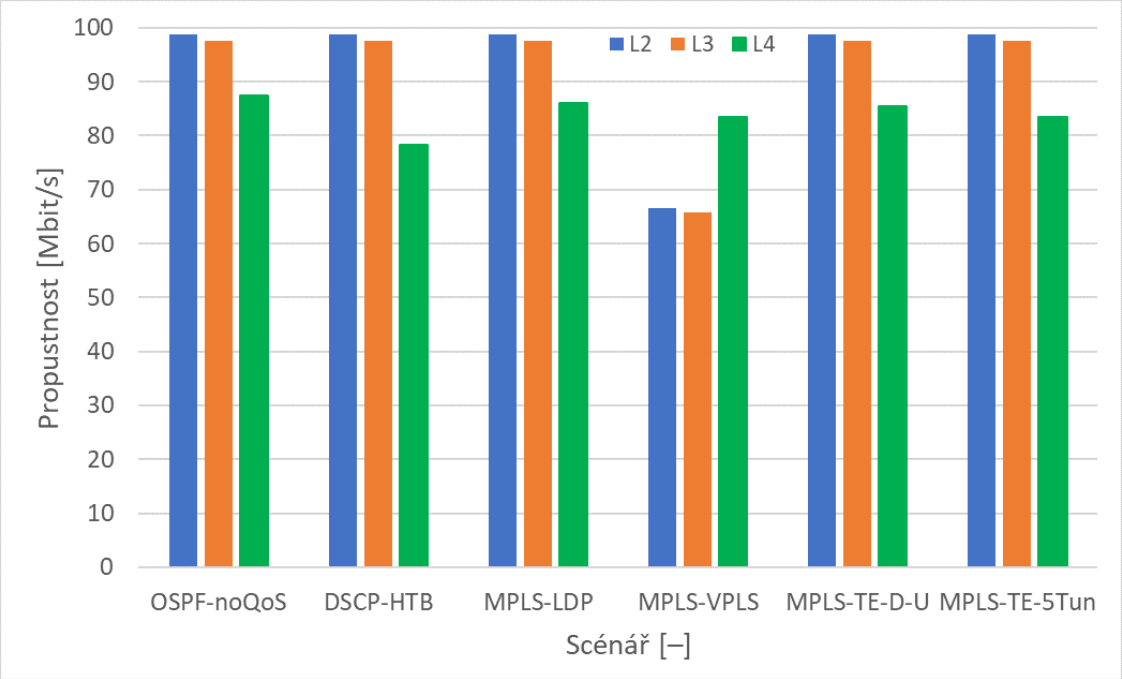
Tab. 4.16: Porovnání propustnosti na L2, L3 a L4.

	L2 [Mbit/s]	L3 [Mbit/s]	L4 [Mbit/s]	L2 vs. L3 [%]	L3 vs. L4 [%]
OSPF-noQoS	98,6996	97,5292	87,4	1,1858	10,3858
DSCP-HTB	98,6996	97,5292	78,4	1,1858	19,6138
MPLS-LDP	98,6996	97,5292	86,0	1,1858	11,8213
MPLS-VPLS	66,6222	65,8322	83,4	1,1858	-26,6857
MPLS-TE-D-U	98,6996	97,5292	85,5	1,1858	12,3339
MPLS-TE-5Tun	98,6996	97,5292	83,5	1,1858	14,3846

Tabulka 4.16 uvažuje maximální naměřené hodnoty propustnosti a demonstruje tedy maximální naměřené rozdíly propustnosti na jednotlivých vrstvách referenčního modelu OSI/ISO pro testované scénáře ve směru R3–>R1. Rozdíly propustnosti na L2 a L3 již byly diskutovány. Zatímco rozdíl mezi propustností L2 a L3 je 1,858 %, tak rozdíl propustnosti L3 a L4 je již znatelně vyšší. Je to dáno skutečným end-to-end přenosem na L4 a do jisté míry i principem funkce protokolu TCP, který test ExacTCP využívá na rozdíl od RFC 2544, který využívá UDP datagramy.

Nejnižší rozdíl maximální L3 a L4 propustnosti vykazuje scénář bez aplikovaných zásad QoS. Nejvyšší naopak scénář *OSPF-noQoS*, kde jsou zásady QoS aplikované na každém směrovači. Rozdíly cca 11–15 % vykazují ostatní scénáře.

Jak již bylo zmíněno, problémem je měření scénáře s VPLS technologií pomocí testu RFC 2544. Dle výsledků by měla být propustnost na L4 o 26,6857 % vyšší než L3, což je vyloučené. Z trendu L4 propustnosti je patrné, že problém není v měření VPLS sítě pomocí testu ExacTCP ani v konfiguraci VPLS, ale v měření testem RFC 2544, který i přes opakované spuštění vykazoval totožné hodnoty propustnosti na L2 a L3.



Obr. 4.20: Porovnání maximální propustnosti všech scénářů na L2, L3 a L4.

4.8 Vyhodnocení testování

Testované scénáře

Shrnuté výsledky všech měřených scénářů pomocí testů ExacTCP, EtherSAM a RFC 2544 ukazují, že nejlepší technologií pro nasazení v přístupových sítích NGA by měla být VPLS (scénář `MPLS-VPLS`), i přes horší výsledky testu RFC 2544. Z hlediska obousměrného zpoždění tato síť vykazovala nejlepší hodnoty a také velmi nízký jitter. Nevýhodou je nasazení v rozsáhlejších sítích, protože tato technologie vyžaduje full mesh propojení mezi hraničními směrovači PE vytvořením pseudovláken, což s sebou nese vysokou režii. Tento problém byl v našem scénáři elegantně vyřešen tak, že pro transport byl v každém směru vytvořen TE tunel a prakticky se tak jednalo o VPLS over TE. Data byla směrována do VPLS spojení sestavené skrze TE tunely. PE směrovače tak vždy vytvořili pouze jedno pseudovlákno mezi sebou v každém směru, protože logicky existovala pouze jedna cesta mezi PE směrovači i přesto, že jsou dvě fyzická spojení. TE tunel také řeší výpadky spojení a přepínání na záložní tunel.

Z hlediska traffic engineeringu, výsledků testů a subjektivního úsudku je však nejlepší volbou pro využití v přístupových NGA sítích technologie využívající TE tunely mezi PE směrovači, a to i za cenu nepatrně vyššího zpoždění oproti VPLS. Vhodnějším řešením z obou nabízených scénářů `MPLS-TE-5Tun` a `MPLS-TE-D-U` je scénář s pěti tunely, obecně s více tunely pro lepší škálovatelnost služeb. Tento způsob je vhodný pro nahrazení současného způsobu poskytování služeb, kdy často bývají služby distribuovány v jednotlivých VLAN bez výhod TE. Minimální navýšení obousměrného zpoždění vzniklé značkováním směrování pro směrování příslušného provozu do správného TE tunelu lze pominout, neboť TE tunely nabízí širokou škálu nastavení. Hlavními výhodami je možnost přepínání hlavního a záložního tunelu při výpadku, využití explicitního nastavení cesty tunelu či technologie CSPF pro automatické sestavení tunelu, nastavení propustnosti, priority, automatického zvýšení propustnosti při nevyužívání ostatních tunelů a další. Další výhodou je pouhá prvotní konfigurace TE na všech směrovačích a zbylá správa tunelů už se odehrává pouze na hraničních PE směrovačích.

Dobré parametry vykazuje i klasická MPLS síť s protokolem LDP pro distribuci návěští. Pokud však existuje možnost konfigurace VPLS či v lepším případě TE tunelů, pak je lepší přistoupit k této možnosti.

Pokud na směrovačích zejména staršího typu nelze konfigurovat MPLS, pak je jedinou rozumnou volbou k zajištění QoS využití klasického mechanizmu DiffServ. Nevýhodou je klasifikace a zpracování paketů na každém směrovači – tzv. „per-hop“, které navyšuje obousměrné zpoždění a jitter.

Obecně lze konstatovat, že nastavené mechanizmy QoS zahrnující klasifikaci paketů, značkování paketů a jejich obsluhu ve frontách směrovačů vnáší do přenosu malé vložené zpoždění. Toto přidané zpoždění je však vykoupeno správnou a předvídatelnou funkcí sítě a služeb při zatížení sítě.

Zcela nevhodné je v přístupových sítích ignorovat QoS a využít mechanizmus best-effort. Chování takové sítě je nepředvídatelné. Funkčnost a kvalita jednotlivých služeb je zajištěna pouze v případě malého zatížení sítě, což je v přístupových sítích NGA nepřijatelné.

Testy

Všechny scénáře byly proměřeny testy RFC 2544, EtherSAM dle doporučení ITU-T Y.1564 SAM a ExacTCP dle doporučení IETF RFC 6349.

Měření dle standardu RFC 2544 je nevyhovující pro moderní datové sítě. To je možné vidět u měření scénáře s VPLS, kde např. naměřené hodnoty propustnosti na L2 a L3 byly nižší, než na L4, což není možné. Tento test je spíš vhodný pro testování výkonnostních parametrů jednotlivých síťových zařízení či spojů (tzv. benchmark test), ne však komplexní sítě se zásadami QoS. Pro měření přístupových sítí NGA ho tak nelze doporučit.

RFC 2544 je výhodné plně nahradit měřením dle standardu ITU-T Y.1564, které vyhovuje požadavku současného měření více různých datových toků v obou směrech simultánně, což lépe reflektuje provoz v reálné síti. V první fázi je testován soulad naměřených hodnot KPI s parametry garantovanými v SLA, pro každou službu jednotlivě až do hodnoty CIR. V našem případě byly prahové hodnoty KPI nastaveny dle doporučení MEF 23.1, které je doporučené pro sítě metro-ethernet, ale doporučuje se i pro přístupové sítě NGA založené na technologii ethernet. V druhé fázi testu pak probíhá měření parametrů všech služeb naráz, jak je tomu v reálné síti. Test nachází své uplatnění zejména ve fázi aktivace služeb a při ověřování úrovně kvality poskytovaných služeb definované v SLA.

Zatímco test EtherSAM je vhodný zejména pro testování realtime služeb využívajících transportní protokol UDP, test ExacTCP dle standardu RFC 6349 je vhodný spíše pro testy non-realtime služeb využívajících protokol TCP pro spolehlivý přenos dat. Volba měřícího protokolu na transportní vrstvě je tedy silně ovlivněna charakterem měřené služby a tím, jaké informace chceme měřením získat. Test dle standardu RFC 6349 je vhodný provádět i v sítích pod cizí správou, s níž není měření koordinováno. Tím se eliminuje riziko identifikace testovacích UDP datagramů testu EtherSAM jako DoS útok. V případě, že je testovaná síť pod vlastní správou nebo je měření koordinováno s provozovatelem sítě, pak je lze použít měření s protokolem UDP.

Testy EtherSAM a ExacTCP nesporně nachází uplatnění při testování výkonnosti IP sítí a ověřování souladu úrovně poskytovaných služeb s SLA. V kombinaci s doporučením MEF 23.1 je tak lze označit za vhodné pro testování moderních paketových přístupových sítí NGA. Vhodné by bylo doplnit testování ještě QoE objektivními testy jednotlivých služeb, které by pomocí parametrů MOS a R vyhodnotili skutečnou kvalitu již poskytovaných služeb tak, jak ji vnímá zákazník.

Společnost EXFO nově přináší i plně automatizovanou měřící aplikaci s názvem iSAM, která sdružuje test dle IETF RFC 6349 a test ITU-T Y.1564. Je tak umožněna kompletní end-to-end validace vrstev L2, L3 a L4 (TCP). Testování pro účely DP bylo provedeno bez využití iSAM z důvodů porozumění principům a konfiguraci jednotlivých testů spouštěných jednotlivě.

5 ZÁVĚR

V úvodní teoretické části práce byl uveden popis sítí NGN/NGA. Pro sítě NGN/NGA je charakteristická konvergence stávajících telekomunikačních sítí. Zejména se jedná o konvergenci klasických telefonních sítí PSTN a telekomunikačních sítí založených na protokolu IP. Cílem je vytvoření jednotné širokopásmové sítě nové generace, založena na protokolu IP. V dalších kapitolách byly popsány charakteristické požadavky různých služeb na QoS parametry, které je nutné dodržet, aby byla koncovému zákazníkovi zaručena správná funkčnost a kvalita poskytované služby. Závěrem teoretické části jsou uvedeny doporučení pro testování QoS parametrů služeb v IP sítích. Tyto testy mají za úkol ověřit výkonnost datové sítě a odhalení možných nestandardních stavů. Testy se však setkávají s omezeními, které limitují univerzálnost jejich využití.

Cílem měření bylo seznámit se s metodami měření QoS parametrů v přístupových sítích. Měření probíhalo s využitím testů RFC 2544, EtherSAM, ExacTCP. Měření dle standardu RFC 2544 je vhodné spíše pro výkonnostní testy zařízení a spojů, než pro testování moderních datových NGA sítí. Je výhodné jej plně nahradit měřením dle standardu ITU-T Y.1564 , které vyhovuje požadavkům současného měření více různých datových toků v obou směrech a verifikace parametrů definovaných v SLA. Test EtherSAM je vhodný pro testování real-time služeb využívajících protokolu UDP, a v sítích pod vlastní správou či koordinovaně s provozovatelem sítě.

Test ExacTCP dle standardu RFC 6349 přináší možnost end-to-end testování non-realtime služeb využívajících protokol TCP pro spolehlivý přenos dat. Volba měřícího protokolu na transportní vrstvě je tedy silně ovlivněna charakterem měřené služby a tím, jaké informace chceme měřením získat. Test ExacTCP je výhodné provádět i v sítích pod cizí správou, kde nemáme informace o nastavených pravidlech firewallu. Využitím protokolu TCP se snižuje riziko identifikace testovacích UDP datagramů testu EtherSAM jako DoS útok.

Testy ExacTCP a EtherSAM jsou vynikající volbou pro testování NGN/NGA sítí a ověřování úrovně poskytovaných služeb definované v SLA. Test EtherSAM je vhodné provádět na nezatížené síti a ve fázi aktivace služeb. Test ExacTCP pak lze s výhodou využít za provozu mimo i ve špičce. Při testování je vhodné vyhovět prahovým hodnotám uvedeným v doporučení MEF 23.1. Uvedenou metodiku testování vyplývající z práce lze obecně vztáhnout k IP sítím. Konkrétně k metalickým přístupovým sítím s technologií ethernet, optickým a hybridním přístupovým sítím FTTx a přístupovým sítím typu metro-ethernet. Vhodné by však bylo doplnění těchto testů QoE subjektivním testem, který by řešil skutečnou kvalitu vnímané služby zákazníkem.

Vhodnou technologií pro nasazení v NGA přístupových sítích je technologie

VPLS, která vykazovala nejlepší hodnoty obousměrného zpoždění. Vhodnější metodou se však zdá být technologii MPLS traffic engineeringu MPLS-TE s více tunely pro jednotlivé služby. Výhodou tohoto řešení je široká škála možností konfigurace priority, propustnosti, automatického nastavení propustnosti, omezování propustnosti a jiných parametrů pro každý tunel zvlášť s využitím protokolu RSVP-TE. Mimo to technologie MPLS využívající TE tunely umožňuje konfiguraci hlavního a záložního tunelu, a to explicitně či automaticky s využitím technologie CSPF.

V moderních přístupových sítích je nutné řešit kvalitu služeb QoS, která umožňuje prioritizaci real-time datových toků s vysokými požadavky na nízké hodnoty obousměrného zpoždění a jitteru na úkor non-realtime služeb. Dodržením zásad návrhu sítí s mechanizmy QoS docílíme návrhu kvalitní sítě s předvídatelným chováním.

Závěrem je nutné konstatovat, že laboratorní síť MikroTik byla složena z dostupných SOHO zařízení, jejichž nižší HW vybavenost se promítla do celkových výsledků testů. V NGA přístupové síti by bylo vhodné využít profesionální výkonné síťové prvky MikroTik řady CRS či zařízení Cisco. Princip konfigurace a testování takové sítě by však byl stále totožný. Platforma MikroTik byla zvolena z důvodu širokého spektra možností konfigurace směrovače.

LITERATURA

[1] BOVY, C. J. a kol. 2002. *Analysis of End-to-end Delay Measurement in Internet*. In: Proceedings of ACM Conference on Passive and Active Measurement.

[2] CISCO, Inc.. *Implementing Quality of Service Policies with DSCP* [online]. 2008-02-15 [cit. 2018-02-03]. Dostupné z URL: <https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html>.

[3] CISCO SYSTEMS. *Understanding Delay in Packet Voice Networks* [online]. 2006a [cit. 2018-04-04]. Dostupný z: <https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/5125-delay-details.html>.

[4] FILKA, Miloslav. *Optoelektronika pro telekomunikace a informatiku*. Brno: M. Filka, 2009. ISBN 978-808-6785-141.

[5] GRENAR, D., FILKA, M., *Next generation access network*, QUAERE. Hradec Králové: MAGNANIMITAS, Hradec Králové, Česká republika, 2017, 2017. s. 715-722. ISBN: 978-80-87952-20-7.

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

[7] IETF. *Framework for TCP Throughput Testing*. RFC 6349. Network Working Group, 2011. ISSN: 2070-1721. Dostupné z: <https://www.ietf.org/rfc/rfc6349.txt>.

[8] ITU-T Recommendation G.107: *The E-model: a computational model for use in transmission planning* [online]. 2011a [cit. 2018-02-05]. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.107-201506-I/en>.

[9] ITU-T Recommendation O.151. *Error performance measuring equipment operating at the primary rate and above* [online]. ITU, 1992. Dostupné z URL: <https://www.itu.int/rec/T-REC-O.151-199210-I/en>

[10] ITU-T Recommendation Y.1564. *Ethernet service activation test methodology* [online]. ITU, 2016. Dostupné z URL: <https://www.itu.int/rec/T-REC-Y.1564-201602-I/en>

[11] ITU-T Recommendation Y.1731. *Operation, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks* [online]. ITU, 2015. Dostupné z URL: <https://www.itu.int/rec/T-REC-G.8013-201508-I/en>

[12] ITU-T Recommendation Y.2001. *General overview of NGN* [online]. ITU, 2004. Dostupné z URL: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2001>

[13] ITU-T Recommendation Y.2012. *Functional requirements and architecture of the NGN release 1* [online]. ITU, 2006. Dostupné z URL: <https://www.itu.int/rec/T-REC-Y.2012-200609-S/en>

[14] JAREŠ, Petr. *Diagnostika přenosových systémů a sítí využívajících technologii Ethernet* [online]. In: . České vysoké učení technické v Praze Fakulta elektrotechnická [cit. 2017-12-18]. Dostupné z: <http://data.cedupoint.cz/oppa_e-learning/2_KME/152.pdf>.

[15] 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.

[16] LAFATA, Pavel a Jiří VODRÁŽKA. *Optické přístupové sítě a přípojky FTTx*. Praha: České vysoké učení technické v Praze, 2014. ISBN 978-800-1054-635.

[17] *Metodika pro měření a vyhodnocení datových parametrů pevných sítí elektronických komunikací: (Metodický postup)*. Praha: ČTÚ, 2016.

[18] MIKROTIK, Documentation. *DSCP based QoS with HTB*. [online]. 2011, 23.6.2011 [cit. 2018-04-29]. Dostupné z: <https://wiki.mikrotik.com/wiki/DSCP_based_QoS_with_HTB>.

[19] PODHRADSKÝ, Pavol. *NGN (next generation networks) - selected topics*. Prague: Czech Technical University, 2013. ISBN 978-80-01-05294-5. Dostupné z: <http://www.digitalniknihovna.cz/mzk/uuid/uuid:6390b640-17b1-4dad-863d-3224c0d39ad5>.

[20] RUDINSKÝ, J. *Sítě nové generace - NGN* [online]. České vysoké učení technické v Praze, FEL, 2006, 15 [cit. 2017-10-08]. ISSN 1214-9675. Dostupné z URL: <http://access.fel.cvut.cz/view.php?nazevclanku=site-nove-generace-ngn&cisloclanku=2006050401>

[21] SONG, J., YOUNG CHANG, M., SEOK LEE, S., *QoS control in next-generation multimedia networks:* Overview of ITU-T NGN QoS Control. IEEE Communications Magazine [online]. Jinoo Joung, Sangmyung University: Electronics and Telecommunications Research Institute (ETRI), 2007, 8, [cit. 10. 3. 2018]. Dostupné z URL: <`http://www.ieeexplore.ieee.org/document/4342866/authors`>

[22] SZIGETI, Tim, Christina HATTINGH, Robert BARTON a Kenneth BRILEY. End-to-end QoS network design. 2nd edition. Indianapolis, IN: Cisco Press, 2014. Cisco Press networking technology series. ISBN 15-871-4369-0.

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

[24] 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

3GPP	3rd Generation Partnership Project
ATM	Asynchronous Transfer Mode
BB	Bottleneck Bandwidth
BDP	Bandwidth Delay Product
BER	Bit Error Rate
CBS	Commited Burst Size
CE	Customer Edge
CIR	Commited Information Rate
CPE	Customer Premises Equipment
COS	Class of Service
ČTÚ	Český Telekomunikační Úřad
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
EIR	Excess Information Rate
ETSI	European Telecommunications Standards Institute
EVC	Ethernet Virtual Channel
IETF RFC	Internet Engineering Task Force Requests for Comments
ICMPv4	Internet Control Message Protocol verze 4
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv6	Internet Protocol verze 6
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union - Telecommunications
KPI	Key Performance Indicator
LM	Loss Measurement
ME	Maintenance Entity
MEF	Metro Ethernet Forum
MEG	Maintenance End Group
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point
MPLS	MultiProtocol Label Switching
MTU	Media Transfer Unit
NGA	Next Generation Access
NGN	Next Generation Network
P2MP	Point to Multipoint
P2P	Point to Point
PER	Packet Error Rate

PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QOS	Quality of Services
QOE	Quality of Experience
RTT	Round Trip Time
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLM	Synthetic Loss Measurement
SS7	Signalizační systém číslo 7
TE	Traffic Engineering
TCP	Transmission Control Protocol
TTR	Transfer Time Ratio
UDP	User Datagram Protocol
UNI	User Network Interface
VPLS	Virtual Private LAN Service

SEZNAM PŘÍLOH

A OBSAH PŘILOŽENÉHO CD

- / ..... kořenový adresář přiloženého CD
  - Konfiguracni_soubory ..... zálohy konfigurací scénářů na směrovačích
    - OSPF-noQoS
      - OSPF-noQoS-R1-PE.backup
      - OSPF-noQoS-R2-P.backup
      - OSPF-noQoS-R3-PE.backup
      - OSPF-noQoS-R4-P.backup
    - DSCP-HTB
      - DSCP-HTB-R1-PE.backup
      - DSCP-HTB-R2-P.backup
      - DSCP-HTB-R3-PE.backup
      - DSCP-HTB-R4-P.backup
    - MPLS-LDP
      - MPLS-LDP-R1-PE.backup
      - MPLS-LDP-R2-P.backup
      - MPLS-LDP-R3-PE.backup
      - MPLS-LDP-R4-P.backup
    - MPLS-VPLS
      - MPLS-VPLS-R1-PE.backup
      - MPLS-VPLS-R2-P.backup
      - MPLS-VPLS-R3-PE.backup
      - MPLS-VPLS-R4-P.backup
    - MPLS-TE-D-U
      - MPLS-TE-D-U-R1-PE.backup
      - MPLS-TE-D-U-R2-P.backup
      - MPLS-TE-D-U-R3-PE.backup
      - MPLS-TE-D-U-R4-P.backup
    - MPLS-TE-5Tun
      - MPLS-TE-5Tun-R1-PE.backup
      - MPLS-TE-5Tun-R2-P.backup
      - MPLS-TE-5Tun-R3-PE.backup
      - MPLS-TE-5Tun-R4-P.backup
    - HTB_Queue_tree.rsc ..... navržený HTB strom tříd a front
    - info.txt ..... přihlašovací údaje k zálohám směrovače R3-PE
  - Reporty_Exfo ..... složka s reporty všech testů
  - DP_Gregor.pdf ..... elektronická verze diplomové práce