Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Využití QoS ve firemním prostředí

David Handlíř

Bakalářská práce

2014

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David Handlíř**
Osobní číslo:	**I10050**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Využití QoS ve firemním prostředí**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je ukázková konfigurace využití QoS ve firemním prostředí pro optimalizaci přístupu k prioritizovaným službám. Autor představí principy QoS a možnosti jeho využití včetně ukázkových konfigurací. Autor provede dotazníkové šetření v minimálně pěti firmách pro zjištění využívaných služeb a jejich významnosti pro danou firmu. Na základě vyhodnocení průzkumu autor realizuje ukázkovou komunikaci s využitím QoS pro prioritizaci vybraných služeb na serveru. Tato část bude prakticky realizována v laboratoři počítačových sítí a dokladována analýzou komunikace.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

SZIGETI, Tim. End-to-end qos network design: quality of service for rich-media. 1st Ed. pages cm. ISBN 978-158-7143-694.
ODOM, Wendell a Michael J CAVANAUGH. Cisco QOS exam certification guide: CCVP self-study. 2nd ed. Indianapolis: Cisco Press, c2005, xxxiv, 730 s. ISBN 15-872-0124-0.
HARDY, William C. QoS: measurement and evaluation of telecommunications quality of service. Chichester: John Wiley, 2001, 230 s. ISBN 04-714-9957-9.

Vedoucí bakalářské práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání bakalářské práce: **20. prosince 2013**
Termín odevzdání bakalářské práce: **9. května 2014**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2014

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 6. 5. 2014

David Handlíř

Poděkování

Na tomto místě bych rád poděkoval vedoucímu bakalářské práce Mgr. Josefu Horálkovi, Ph.D., za odborné vedení, za pomoc a rady při zpracování této práce.

Anotace

Cílem práce je ukázková konfigurace využití QoS ve firemním prostředí pro optimalizaci přístupu k prioritizovaným službám. Autor představí principy QoS a možnosti jeho využití včetně ukázkových konfigurací. Autor provede dotazníkové šetření v minimálně pěti firmách pro zjištění využívaných služeb a jejich významnosti pro danou firmu. Na základě vyhodnocení průzkumu autor realizuje ukázkovou komunikaci s využitím QoS pro prioritizaci vybraných služeb na serveru. Tato část bude prakticky realizována v laboratoři počítačových sítí a dokladována analýzou komunikace.

Klíčová slova

QoS, kvalita služeb, QoS ve firemní prostředí, IntServ, DiffServ, RSVP, integrované služby, diferencované služby

Title

The Usage of QoS in Business Environment

Annotation

The aim of this thesis is the sample configuration of QoS in business environment to optimize access to prioritized services. Author introduces principles of QoS and the possibility of its use including sample configuration. Author performs survey in at least five companies for finding used services and their importance for the company. Based on the analysis of the survey, author realizes sample communication with usage of QoS for prioritization selected services. This part will be practically realized in the laboratory of computer networks and documented by the analysis.

Keywords

QoS, quality of service, QoS in bussiness enviroment, DiffServ, IntServ, differentiated services, integrated services, RSVP

OBSAH

SEZNAM ZKRATEK

ACL	Access List
AF	Assured Forwarding
BA	Behavior Aggregate
CBWFQ	Class-Based Weighted Fair Queuing
DCE	Data Communications Equipment
DiffServ	Differentiated Services
DSCP	Differentiated Service Code Point
DTE	Data Terminal Equipment
EF	Expedited Forwarding
FEC	Forward Equivalence Class
FIFO	First In First Out
FQ	Fair Queuing
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
LER	Label Edge Router
LLQ	Low Latency Queuing
LSR	Label Switched Router

MOS	Mean Opinion Score
MPEG	Moving Picture Experts Group
MPLS	Multi Protocol Label Switching
NAK	Negative Acknowledgement
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PHB	Per Hob Behavior
PQ	Priority Queuing
QoS	Quality of Service
RED	Random Early Detection
RFC	Request for Comments
RSVP	Resource Reservation Protocol
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

ÚVOD

V současné době v závislosti na rozvoji informačních technologií, jsou sítě využívány nejen pro přenos souboru, ale přenáší nejrůznější typy dat rozdílných objemů.

Aby bylo možné efektivně využívat provoz v síti, je nutné nastavovat určitá pravidla a případná omezení. Tento princip je v rámci počítačových sítí známy jako QoS, tedy zajištění kvality služeb.

Jelikož sto lidí znamená sto chutí. Není tomu jinak i u počítačových sítí. Každá síť je dle požadavků provozující organizace zaměřena na konkrétní kvalitu určitých druhů služeb, avšak to znamená, že jiné přenosy musí být záměrně znevýhodněny.

Cílem bakalářské práce je představení principů QoS ve firemním prostředí s prioritizace vybraných služeb. Tyto služby jsou vybrány na základě dotazníku, rozeslaného do firem v pardubickém regionu. Na základě výsledků je v laboratorních podmínkách síť navržena a otestována s využitím kvality služeb i bez ní.

První teoretická část bakalářské práce je zaměřena na objasnění základních principů a mechanismů využívaných pro zajištění kvality služeb. V této části jsou uvedeny aplikace QoS, mezi které jsou zařazeny Best Effort, IntServ a DiffServ. Každý z těchto přístupů ke QoS je podrobně představen včetně potřebných doplňujících informací.

V souvislosti s modelem integrovaných služeb nelze opomenout ani protokol RSVP, který slouží pro rezervaci cesty a tím zajišťuje prioritní komunikaci. V této části jsou dále teoreticky popsány i správy front či algoritmus tocken bucket, které využívá model diferencovaných služeb.

Teoretickou část uzavírá využití QoS nad MPLS.

Praktická část této bakalářské práce vyžaduje dopřednou přípravu pro sběr a následnou analýzu dat. Data jsou získána od firem, jejichž správci počítačové sítě byli ochotni zodpovědět anonymní a velmi snadný dotazník. Anonymita zde byla použita kvůli zachování vnitrofiremních informací. Díky anonymitě se však můžeme pouze domnívat, jaké obory firem QoS využívají.

Tato část zpracovává přehlednou formou získané informace, na jejichž základě je postaven model topologie. Modelová topologie byla následně po mnoha konzultacích a revizích zprovozněna v rámci univerzitní laboratoře.

Je důležité mít na paměti, že práce je zaměřena na využití QoS ve firemní síti, nikoliv na konfiguraci firemní sítě. Jsou zde tedy potlačeny konfigurace VLAN či autorizačních a autentifikačních mechanismů.

Praktické část je zaměřena na přehlednou ukázku kvality přenesených dat v případě využití mechanismů QoS a bez nich. Výsledky měření jednotlivých konfigurací jsou graficky zobrazeny, aby bylo možné snadno ověřit rozdíly v kvalitě služeb při aplikaci QoS.

1 ZAJIŠTĚNÍ KVALITY SLUŽEB

1.1 NUTNOST ZAJIŠŤOVÁNÍ KVALITY SLUŽEB V POČÍTAČOVÉ SÍTI

Termín kvalita služeb v počítačové síti může mít velké množství výkladů. Tuto skutečnost z části podporují i marketingové akce poskytovatelů internetového připojení. Internetoví poskytovatelé kvalitu služeb zneužívají k vyjádření skutečnosti, že právě jejich služby patří mezi nejlepší. Mnoho lidí si proto pod tímto pojmem představí pouze garantovanou rychlost připojení či funkčnost jedné vybrané služby. Pro správné pochopení a význam QoS je však nutné podívat se do problematiky kvality služeb a jejich zajišťování více do hloubky.

Jak již bylo zmíněno v předchozí části textu, nepředstavuje zajištění kvality pouhou garanci rychlosti. Ve skutečnosti jde o zajištění potřebné šířky pásma a minimalizování zpoždění pro služby, které pracují v reálném čase. U takových služeb by i minimální zpoždění mohlo mít vliv na kvalitu výstupu. Mezi služby ovlivňované mírou zpoždění a kvalitou přenosu řadíme hlasovou komunikaci (VoIP) a videokonference.

Podle jedné z definic [1] lze QoS definovat jako schopnost sítě poskytovat lepší či speciální služby vybraným uživatelům a aplikacím na úkor ostatních. A to nezávisle na používaných technologiích, mezi které se řadí ATM, Frame Relay, Ethernet či sítě založené na protokolu 802.1

Administrátoři tak získávají efektivní nástroj, s jehož pomocí mohou ovlivňovat výkon sítě. Tento výkon je ovlivněn:

- řazením paketů do front,
- prioritizací komunikace,
- garancí maximálního zpoždění,
- rozptylem zpoždění,
- šířkou pásma.

Díky výše uvedeným je možné navrhnout systém předcházející zahlcení a zajišťující plynulou komunikaci po síti.

1.2 Vývoj QoS

V počátcích, před zavedením konvergovaných sítí, bylo zvykem, že administrátoři kladli důraz především na zajištění konektivity v rámci sítě. Z toho vyplývá, že jednotlivé komunikace využívající dnes sdílené přenosové médium, byly striktně odděleny. Síť nebyla vytížena rovnoměrně, ale zatížení přicházelo v rozdílných intervalech, kdy docházelo k nárazovým tokům dat [2].

V této době byl využíván jednoduchý systém založený na FIFO, tedy kdo dřív přijde, bude dříve obsloužen. Data, jenž přicházela na rozhraní, se snažila zabrat největší množství pásma a tím si zajistit co nejefektivnější přenos. Kvalita služeb a množství přiděleného pásma tak přímo závisela na připojených uživatelích, kteří v dané chvíli využívali síťové služby.

Protokoly, které byly využívány v tomto období, byly navrženy tak, aby se dokázaly s nárazovými toky dat vyrovnat. Pokud tedy odeslaný e-mail přišel za více než pár sekund, nebylo zpoždění nijak znatelné. V případě, že se komunikace protáhla na několik minut, jednalo se o nepříjemnou překážku, ovšem v žádném případě nemohl tento fakt výrazně ovlivnit samotnou komunikaci.

Díky oddělení prvků v síti společně s oddělenými přenosovými médii, byla zajištěna potřebná funkčnost. Zvuk, video i data putovaly oddělenými sítěmi, které byly k tomuto účelu navrženy.

S dalším vývojem docházelo k postupné konvergenci sítě [3], kdy hlasová komunikace, video i data začaly využívat sdílené síťové prostředky. Spojení rozdílných služeb s rozdílnými požadavky často vedlo ke vzniku řady problémů.

Jako příklad lze uvést porovnání paketů hlasové komunikace a přenosu dat. Pakety v rámci hlasové komunikace jsou sice typicky velmi malé, avšak sebemenší zpoždění může vést k přeskakování hlasu, nesrozumitelnosti sdělení a v nejhorším případě k celkovému přerušení komunikace. Zpoždění a případné výpadky paketů mají pouze minimální toleranci, pokud chceme zachovat kvalitu a srozumitelnost hlasu. Naopak pakety, přenášející data, bývají obvykle mnohem větší a tím zabírají značnou kapacitu přenosového pásma. Na rozdíl od hlasové komunikace však dokáží snést jistou míru zpoždění i výpadky paketů, které mohou být znovu přeposlány.

Z výše uvedeného je patrné, že video i zvuk jsou velmi choulostivé na včasné doručení do cílového zařízení. Není zde prostor pro zpoždění ani výpadky, jelikož se tyto faktory nepříznivě

projeví na výsledné kvalitě přenosu. Z tohoto důvodu je nadmíru důležité najít mechanismus, který umožní rozlišení obsahu jednotlivých rámců a vybrané komunikaci umožní přednostní obsloužení. Následující text shrnuje dopady neadekvátně nastavené sítě na různé typy komunikace. [1]

Zvuk

- výpadky v komunikaci,
- ozvěna,
- nesrozumitelnost komunikace,
- ukončení komunikace.

Video

- problémy obdobné se zvukem,
- desynchronizace zvuku a videa,
- zpomalení a s tím spojená nesrozumitelnost a desynchronizace

1.3 PARAMETRY PRO KONFIGURACI QOS

Nyní nám vyvstává otázka, podle jakých parametrů lze posuzovat výkon dané sítě. Je totiž velmi obtížné optimalizovat něco, co se nedá změřit. V aplikacích QoS tomu tak naštěstí není.

Dále jsou rozebrány klíčové prvky, na kterých je postaveno zajišťování kvality služeb v konvergovaných sítích.

1.3.1 Šířka pásma

Šířka pásma je jeden z důležitých parametrů, který ovlivňuje rychlost celé sítě. Základní jednotkou je *b/s*. Šířku pásma pro QoS určujeme z end-to-end spojení. Šířka pásma, kterou při komunikaci disponujeme, se rovná šířce pásma nejpomalejší linky, která se v cestě nachází. Důležitý je také fakt, že čím více datových toků na lince běží, tím se šířka pásma úměrně zmenšuje.

$$Bandwidth_{max} = \min(bandwidth_1, bandwidth_2, \ldots + bandwidth_n)$$

1.3.2 Zpoždění

Je definováno dle [1] jako konečné množství času, které potřebuje paket k dosáhnutí cílové bodu potom co byl odeslán. Mějme na paměti, že každý přechod přes síťové zařízení zvyšuje zpoždění. Zpoždění je nevyhnutelné a tak se můžeme snažit pouze o jeho minimalizaci.

Zpoždění typů zpoždění je několik[1]:

- **Zpoždění při zpracování** představuje typ zpoždění, které nastává při zpracování paketu směrovačem. Svou roli v tomto procesu hraje rychlost procesoru, architektura směrovače a jeho konfigurace.
- **Zpoždění ve frontách** lze popsat jako čas, po který pakety čekají ve výstupních frontách procesoru. Zde záleží především na počtu paketů ve frontě, šířce pásma a způsobu, jakým jsou pakety ve frontě zpracovány.
- **Serializační zpoždění** je časový úsek, který trvá vložení dat na fyzické přenosové médium.
- **Zpoždění při propagaci** je čas, který pakety cestují v síti, obvykle je závislý typu přenosového média a jeho rychlosti.

1.3.3 Rozptyl zpoždění (Jitter)

Jak název napovídá, jedná se o [11] rozdíl v end-to-end zpoždění mezi jednotlivými pakety. To znamená, že pokud jeden paket potřebuje pro přenos 110 ms a druhý 135 ms je rozptyl zpoždění 25 ms. Rozptyl bývá způsoben nekonstantním zpožděním při serializaci paketů či rozdílnou délkou front na jednotlivých směrovačích.

1.3.4 Ztrátovost

Podle **Chyba! Nenalezen zdroj odkazů.** lze definovat ztrátovost jako relativní míru počtu aketů, které nebyly doručeny ve srovnání s celkovým počtem odeslaných paketů. Ztrátovost lze obvykle brát jako měřítko dostupnosti sítě. Ztráty paketů nejčastěji nastávají v případě, že je buffer na odchozím rozhraní síťového zařízení již plný, a tak jsou nové příchozí pakety zahazovány. Mohou nastat i méně obvyklé varianty jako zahazování paketů na vstupním rozhraní, přetížení procesoru směrovače nebo nesprávná konfigurace směrování.

1.3.5 Minimální požadavky na komunikaci

Pro přenos hlasu a videokomunikace je důležité, dodržet maximální povolené hodnoty výše zmíněných parametrů. Zatímco u zvuku a videa jsou maximální hodnoty relativně přesně

stanovené, datové přenosy nemají striktní omezení. Na rozdíl od paketů, které přenášejí zvuk a video jsou však mnohem větší a tak potřebujeme dostatečnou šířku pásma a vyrovnávací paměti pro efektivní přenos. Nároky jednotlivých komunikací popisují následující tabulky **Chyba! Nenalezen zdroj odkazů.** – uvedené informace platí pouze pro jednosměrnou omunikaci.

Tabulka 1 Nároky na hlasovou komunikaci

NÁROKY NA HLASOVOU KOMUNIKACI	
Zpoždění	≤ 150 ms
Rozptyl	≤ 30 ms
Ztrátovost	≤ 1 %
17 – 106 kbps garantované šířky pásma pro hovor	
150 bps šířky pásma pro řízení provozu	

Tabulka 2 Nároky na videokonference

NÁROKY NA VIDEOKONFERENCE	
Zpoždění	= 150 ms
Rozptyl	= 30 ms
Ztrátovost	= 1 %
Garantovaná šířka pásma	≥ stream + 20 % (384 kbs stream vyžaduje 460 kbps šířky pásma)

K tomu, abychom mohli obsluhovat aplikace, které mají takto rozdílné nároky, je zapotřebí komunikaci přicházející na směrovač, nebo jiné zařízení podporující QoS, rozdělit do jednotlivých tříd. Z toho důvodu je nezbytná identifikace jednotlivých prvků síťového provozu a zjištění požadavků firmy na kvalitu služeb.

Poté co máme třídy hotovy, aplikujeme na ně pravidla, podle kterých je bude směrovací zařízení zpracovávat.

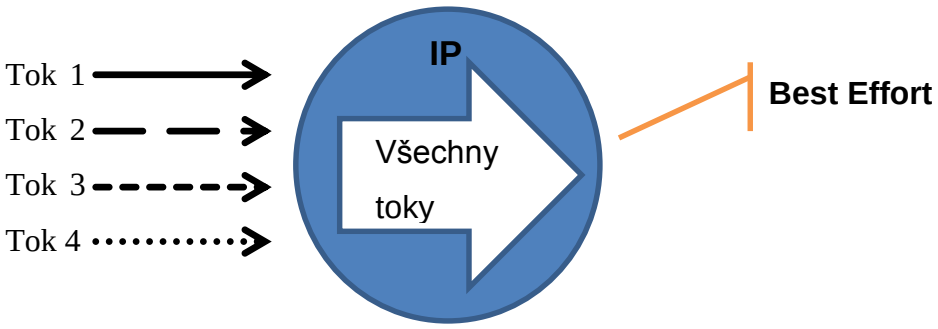
1.4 METODY PŘÍSTUPU KE QOS

Ke kvalitě služeb lze přistupovat několika způsoby, které budou podrobně rozebrány v následující části:

- Best-Effort
- IntServ
- DiffServ

1.5 BEST-EFFORT

Jednoduše lze říci, že pokud není aplikován QoS, jedná se o model Best-Effort. Všechny pakety se zpracovávají naprosto stejně. Na tomto principu je založena i síť Internet. Pokud tedy nepotřebujeme zaručovat kvalitu pro vybrané služby, je model Best-Effort nejlepším řešením.



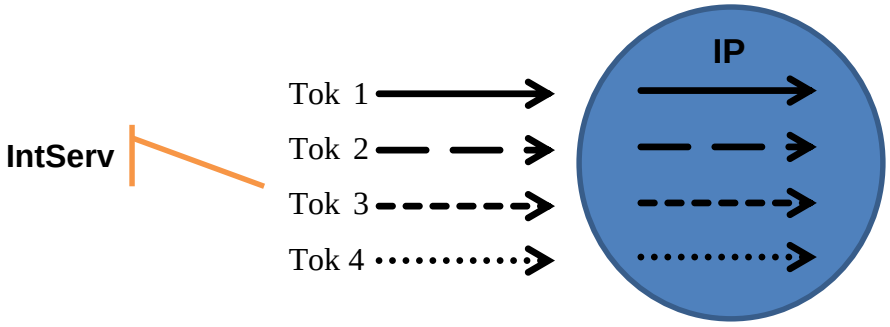
Obrázek 1 Model Best Effort

1.6 INTSERV

Integrated Service model [7] nabízí uživatelům sítě garanci služeb, což je hlavní výhodou této metody. Celý model je postaven na možnosti end-to-end rezervace prostředků, které zajistí minimální nutnou šířku pásma, zpoždění, jitter i ztrátovost pro daný datový tok. Jedná se o první komplexní aplikaci end-to-end QoS.

Každý datový tok v síti musí jednoznačně definovat, o jakou službu se jedná a jaké klade na síť požadavky. Hraniční směrovače pak poskytují řízení přístupu neboli admission control. Dle [7] je řízení přístupu rozhodovací algoritmus, který používá daný směrovač pro definování, zda

jsou v síti dostatečné prostředky. Aktuální směrovač sdělí všem směrovačům spadajícím do cesty paketu způsob, jakým bude datový tok rozeznán a zpracován. Samotná data jsou odesílána až poté, co síť potvrdí rezervaci. Rezervovanou šířku pásma pak nemůže po danou dobu využívat žádná jiná služba.



Obrázek 2 Model IntServ

K rezervaci potřebných prostředků se používá Resource Reservation Protocol (RSVP), který bude rozebrán v následující části této kapitoly. Nad jednotlivými frontami potom pracuje plánovač paketů. Ten se podle [7] stará o odesílání proudů paketů, přičemž využívá fronty s roztříděnými pakety a další mechanismy jako jsou časovače.

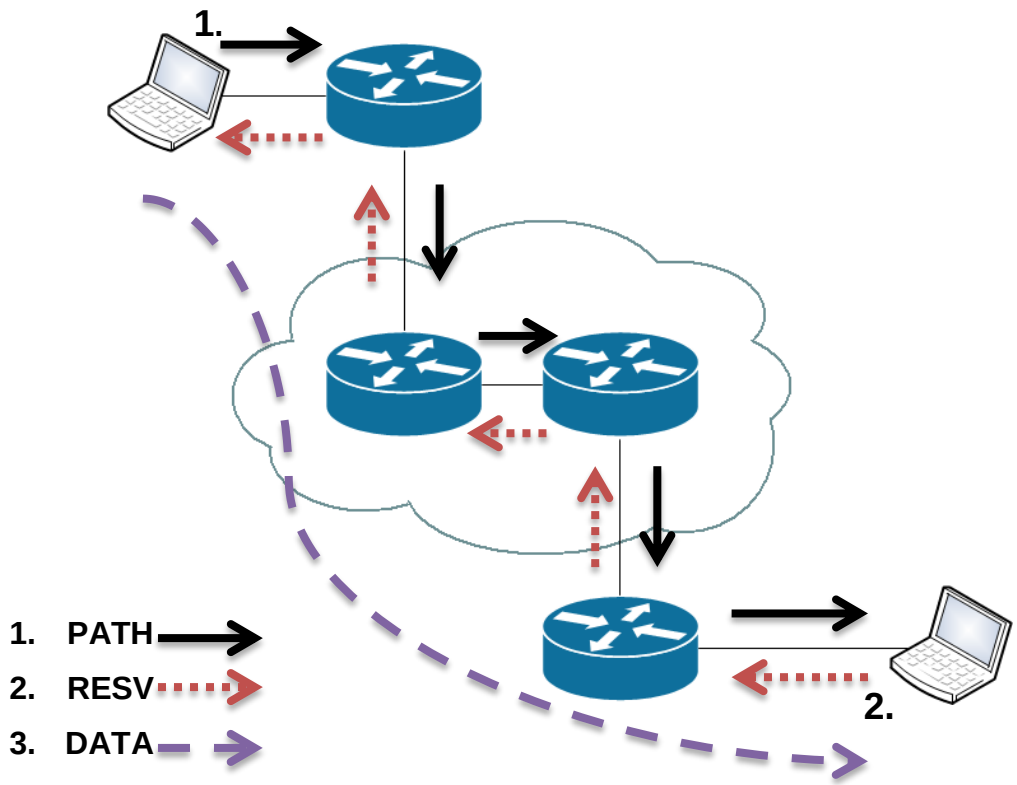
1.6.1 RSVP

Podle RFC 2205 [8] je RSVP rezervační protokol, navržený pro využití v IntServ. Protokol využívají jak koncové uzly, pro vyžádání specifické kvality služeb, tak i směrovače pro rozeslání tohoto požadavku všem směrovačům, přes které bude komunikace uskutečněna. Je vhodné zmínit, že výběr cesty již není v režii RSVP, ale na směrovacích protokolech, respektive statickém směrování. Další důležitou vlastností RSVP je fakt, že tento protokol je simplexový. To znamená, že rezervace prostředků je prováděna vždy pouze jednosměrně.

Pro komunikaci definuje RSVP několik typů zpráv, které jsou podrobně rozebrány v RFC 2205. Pro nás jsou důležité především dva typy, a to **zpráva PATH**, kterou odesílá host a **zpráva RESV**, sloužící jako odpověď typ zprávy.

Princip lze shrnout následovně [5]. Host, který vyžaduje pro své služby speciální zacházení, odešle PATH příjemci dat. Destinace v síti na tuto zprávu odpoví pomocí RESV, kterou potvrzuje přidělení síťových prvků. Zpráva RESV je odeslána po stejné cestě, jakou definuje

zpráva PATH. RESV zpráva při své cestě zajišťuje rezervaci prostředků. Výše popsaný způsob popisuje obrázek 3.



Obrázek 3 RSVP

Nevýhodou modelu IntServ je jeho vysoká náročnost na dostupné prostředky [1]. Již samotná rezervace pomocí RSVP vyžaduje velkou režii. QoS musí být aplikován na celé síti, a tudíž může nastat značné omezení ostatních služeb. Pokud je síť rozsáhlá a komunikace s vyšší prioritou probíhá často, jsou veškeré prostředky zabrány prioritizovanou komunikací a velkou režií RSVP.

Je důležité si uvědomit, že i když datový tok nevyužije všechny rezervované prostředky, nemohou být až do doby uvolnění použity a tím dochází k plýtvání dostupné šířky pásma. Dalším problémem je, že například při videokonferenci s více zdroji. V takovém případě totiž každý zdroj vyžaduje vlastní datový tok, který potřebuje být obsloužen.

1.7 DIFFSERV

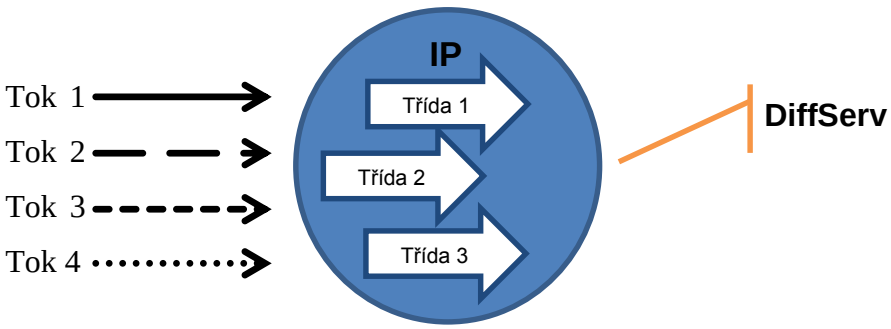
K vývoji dalšího mechanismu pro zajišťování kvality služeb přispěl především rapidní rozvoj Internetu. Čím více uživatelů, bylo připojeno k síti, začalo být jasné, že současné metody již

nejsou dostačující. Proto bylo potřeba navržení škálovatelné architektury, která dokáže držet tempo s růstem sítě a přibývajícími uživateli.

Podle [9] představuje DiffServ neboli Differentiated Services model pro aplikaci QoS, navržený tak, aby předcházel limitacím, které mají modely Best-Effort a IntServ. To ovšem neznamená, že DiffServ je v současnosti jediná používaná metoda. Pokud máme relativně malou síť a potřebujeme prioritizovat vybranou komunikaci, je stále nejlepší volbou IntServ.

Zatímco IntServ má klasifikaci a přeposílací politiky staticky stanovené, DiffServ využívá signalizaci hop-by-hop. Díky tomu je často DiffServ označován jako tzv. „Soft QoS“ [1], jelikož pro služby nejsou přesně vyhraněné hranice a nesnaží si zabrat potřebné pásmo jen pro sebe. Architektura tohoto modelu je [10] postavena na hraničních uzlech v doméně DiffServ, které obsahují instrukce pro přeposílání paketů, algoritmy pro klasifikaci komunikace a funkce pro řízení provozu.

Mezi tyto funkce patří značkování (marking), shaping a policing [5]. Celý mechanismus pak funguje na nastavených pravidlech hop-by-hop. To znamená, že každý uzel v síti, má vlastní sadu politik, podle kterých nakládá s pakety nezávisle na ostatních zařízeních v síti. Tím pádem nemůžeme předem garantovat doručení, jak je tomu u systému IntServ, popsaném v předchozí kapitole.



Obrázek 4 Model DiffServ

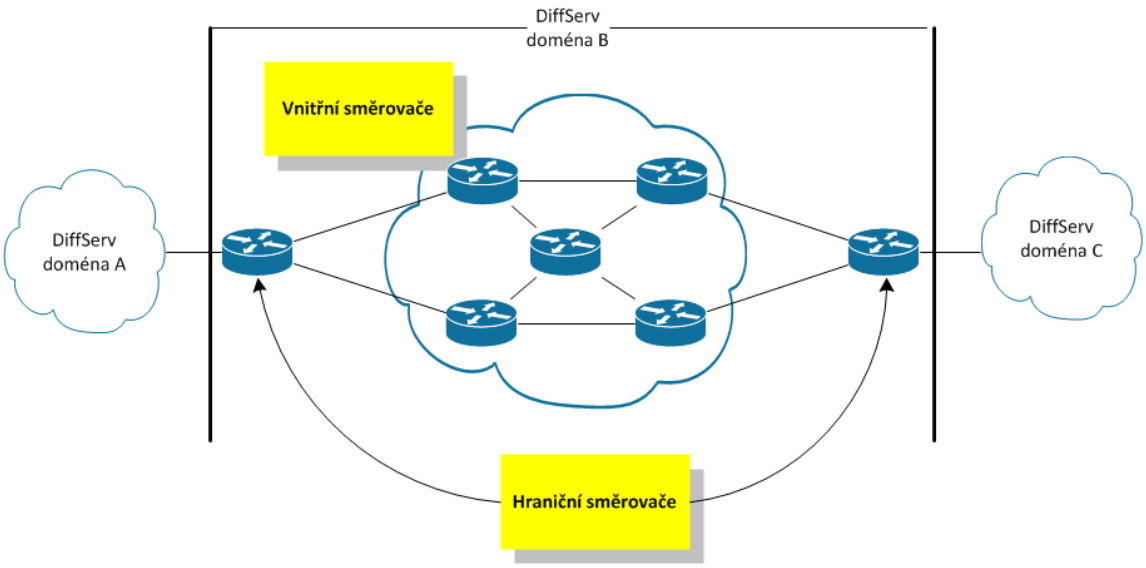
1.7.1 Differentiated Service Domain

Již několikrát byla zmíněna DiffServ doména. Tu si lze představit jako skupinu směrovačů, které můžeme dále rozdělit na hraniční a vnitřní.

- **Vnitřní směrovače** se starají o přeposílání paketů uvnitř domény, nemají specifická nastavení pro přeposílání paketů

- **Hraniční směrovače** (někdy je lze nalézt pod označením vstupně/výstupní) se starají o třídění příchozích a odchozích paketů. Tyto směrovače jsou na pomezí dvou domén, a tudíž pracují jako vstupní směrovač pro jednu doménu a výstupní v rámci domény druhé.

Grafické znázornění domény DiffServ představuje následující obrázek.



Obrázek 5 Ukázka domény DiffServ

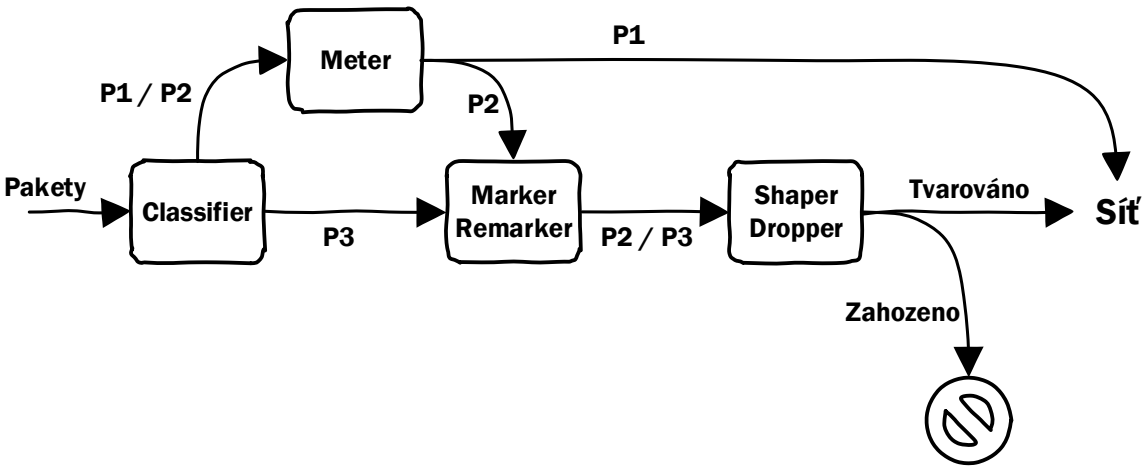
Jak již bylo zmíněno, síťová komunikace je klasifikována, tedy rozdělována do předem definovaných tříd. K tomu abychom mohli jednotlivé pakety v datovém toku rozlišit, [2] jsou identifikovány pomocí DSCP [12] (Differentiated Services Code Point) nebo značkovacím bitem v IP hlavičce.

Hodnoty DSCP posléze slouží jako označení paketů, podle kterého směrovač pozná, jak má s daným paketem zacházet. DSCP nahrazuje v hlavičce paketu IP-precendence. DSCP na rozdíl od IP-precedence používá místo tří bitů šest. S každou hodnotou DSCP je svázáno Per-Hop Behavior (PHB). Všechny pakety se stejnou značkou DSCP označujeme jako Behavior Aggregate, zkráceně BA. Na každou BA se aplikují vždy stejná pravidla pro zpracování, tedy stejné PHB.

1.7.2 Klasifikace a značkování paketů

Základní princip fungování modelu DiffServ lze popsat jednoduchým schématem. Celé schéma lze rozdělit do dvou funkčních kategorií, kterými jsou třídění a úprava provozu. Třídění provozu, jak již název napovídá, slouží ke značkování paketů a úprava provozu následně na základě

značek DSCP dále zpracovává síťovou komunikaci dle nastavených pravidel. Zmíněný mechanismus je uveden na obrázku 6.



Obrázek 6 Mechanismus zpracování paketů DiffServ

Mechanismus pro úpravu provozu obsahuje následující funkční bloky:

Classifier (Klasifikátor, třídič)

DiffServ tento prvek využívá pro identifikaci paketů, podle které jsou následně zařazovány do určité třídy. Pakety mohou být rozlišovány pomocí mnoha kritérií, mezi které patří:

- značka DSCP,
- IP precedence,
- zdrojová adresa,
- cílová adresa,
- číslo UDP/TCP portu.

Marker (Značkovač)

Marker [10] slouží pro přeznačkování paketů. Přeznačkováním myslíme změnu hodnoty DSCP, čímž se paket zařazuje do konkrétní třídy provozu. Podle hodnoty DSCP, kterou nastaví marker, je paketu přidělen způsob zacházení PHB. Tím můžeme definovat několik úrovní QoS pro rozdílnou komunikaci.

Meter

Provádí měření parametrů síťového provozu, vybraného klasifikátorem a tyto parametry dále porovnává s datovými profily. Podle daných pravidel lze posléze rozhodnout, zda paket spadá do rámce profilu či nikoliv. Pakety spadající do rámce profilu jsou vpuštěny dál do sítě, nespadající pakety mohou být dále zpracovány značkovačem, tvarovačem nebo zahazovačem.

Meter je běžně implementován pomocí algoritmu Token Bucket. Princip si lze představit jako kbelík (bucket) dané velikosti, do kterého se přidávají žetony (tokens) zadanou rychlostí. Pokud je kbelík plný, žetony se zahazují. Pokud přijde paket, je z kbelíku odebrán počet žetonů, které odpovídají jeho velikosti. Pokud je k dispozici dostatečný počet žetonů, je paket odeslán a žetony odebrány. V opačném případě je paket pozdržen, v krajním případě zahozen.

Remarker (přeznačovač)

Zajišťuje přeznačování paketů, které nevyhovují kritériím pro přenos. Většinou se pakety přeznačují hodnotou DSCP spadající do třídy s vyšší prioritou zahození.

Dropper (zahazovač)

Pakety, které by mohly přesáhnout dostupnou šířku pásma, jsou zahazovány nebo přeznačkovány. Zahazování paketů může být realizováno na vstupním i výstupním zařízení.

Shaper (tvarovač)

Slouží k úpravě provozu, kterou provádí pomocí zpožďování paketů. Příchozí pakety se řadí do fronty, ze které jsou pak odebírány a posílány dále. Pracuje nejčastěji také na algoritmu Token Bucket, ale k němu se ještě přidávají algoritmy pro využití fronty.

1.7.3 Plánované odesílání paketů

Poté, co pakety přijdou na rozhraní směrovacího zařízení, je nutné je dále zpracovat. Proto, abychom mohli určit, který z paketů má být zpracován jako další, je nutné zajistit plánované odesílání paketů. Plánování je řešeno pomocí front a jejich správy. Jelikož plánování paketů není standardizováno, výrobci k němu mohou přistupovat několika způsoby. Podle [QoS in Packet Network] lze plánování paketů nejlépe popsat jako srdce QoS mechanismu, které může sloužit jako měřítko kvality a zásadně ovlivňuje kvalitu služeb. Rozlišujeme následující typy front [5]:

- **FIFO** (First In First Out) je nejjednodušším řešením. Paket, který přijde na rozhraní jako první, je první zpracován. Jedná se o metodu, která nám neumožňuje ovlivňovat výslednou kvalitu, jelikož zde nedochází k žádnému prioritnímu zpracování.
- **PQ** (Priority Queuing) na rozdíl od FIFO umožňuje větší množství front členěných podle priority od *1* do *N*. Princip spočívá v tom, že pakety zařazené v nižší frontě mohou být odeslány až potom, co jsou všechny vyšší fronty prázdné. Jedná se tedy o vylepšený model FIFO, který je velmi jednoduchý na implementaci, ovšem přináší značné nevýhody a omezení. V prioritních frontách se musí vyskytovat pouze menšinové služby, jinak nemusí dojít k obsloužení paketů, které čekají v nižších frontách.
- **FQ** (Fair Queuing), často známá jako Round Robin, má definováno N front, přičemž má každá přidělenu propustnost *1/N*. Tyto fronty jsou cyklicky zpracovány a prázdné fronty jsou přeskakovány. Při zpracování je vždy z fronty odeslán jeden paket. Tím dochází k obsloužení všech front. Z tohoto faktu vyvstává i hlavní nevýhoda. Všechny fronty totiž nemusí mít pakety o stejné velikosti a rozdílné služby mají rozdílné nároky na propustnost. Prioritní komunikace tak může být znevýhodněna.
- **WRR** (Weighted Round Robin) řeší problém s malou propustností tak, že paketům přiděluje šířku pásma podle jejich potřeb. Vstupní datové toky jsou rozděleny do N tříd a každé třídě je přidělená určitá propustnost. Váhy jsou odvozovány od požadavků jednotlivých tříd a jejich součet musí být *100%*. Zůstává zde však stále nevýhoda s velikostí jednotlivých paketů.
- **WFQ** (Weighted Fair Queuing) řeší nedostatky s propustností velikostí paketů. Stejně jako u WRR jsou pakety rozděleny do N tříd a každé je přidělena propustnost podle jejích požadavků. Opět zde platí, že součet musí dát 100%. Hlavní rozdíl oproti předchozím případům tkví v tom, že se neodesílá jeden paket, ale cyklicky jsou procházeny fronty a odebírány jednotlivé bity. Poté, co je paket z bitů složen, je následně odeslán. Díky tomu nedochází k nechtěnému upřednostňování objemných paketů. Tento systém je již značně komplikovaný na výpočetní čas i implementaci. Přesto však přináší nejlepší výsledky, a proto je v technologiích DiffServ nejčastěji používán.
- **CBWFQ** (Class-Based Weighted Fair Queuing) je z velké části podobný WRR, pakety jsou řazeny do několika front. Pásmo je přiděleno jednotlivým frontám na základě jejich váhy, která je definována na základě jejich požadavků. Narozdíl od WRR nejsou fronty obsluhovány odesíláním jednotlivých paketů, ale pomocí plánování jak je tomu u WFQ.

- **LLQ** (Low Latency Queuing) je algoritmus vyvinutý společností Cisco. Funkčnost je postavena na CBWFQ, kterému je přidána prioritní fronta, která slouží především pro přenos hlasové komunikace a videokomunikace. Díky tomu lze vybrané komunikaci snížit zpoždění a jitter.

1.7.4 Aktivní správa front

Aby při komunikaci nedošlo k zahlcení směrovače, potřebujeme mechanismy, které se postarají o aktivní správu front. Fronty mají pevně stanovenou velikost, kterou nesmí překročit. K tomuto problému lze přistupovat několika metodami – aktivní či pasivní správou front.

Pokud nemáme na směrovači mechanismus pro aktivní správu front je implicitně využit Tail-drop. Tato pasivní metoda automaticky zahazuje pakety, pokud pro ně již ve frontě není místo. Jedná se o nejjednodušší řešení, které s sebou však přináší problémy. Při zahození TCP paketu dostane při synchronizaci odesílající host negativní acknowledgement (NAK). To je pokyn pro znovu odeslání paketů a snížení rychlosti linky. Při tail-dropu TCP paketů, dochází k ovlivnění všech TCP komunikací, jejichž pakety byly odhozeny. Tím dochází k simultánnímu zpomalení všech paketů, které vede k tomu, že se pakety vrátí na zařízení v přibližně stejnou dobu, čímž může dojít k opětovnému zahlcení a tail dropu.

Problémy pomáhá řešit aktivní správa front, která se snaží možnému zahlcení předcházet. Nesnaží se jej však v případě nastání řešit. Rozlišujeme základní algoritmy pro zprávu front [1][5]:

- **Random Early Detection (RED)** je algoritmus předčasné detekce s náhodným zahazováním. RED se snaží predikovat blížící se zahlcení. Algoritmus funguje na základě sledování zaplněnosti fronty. Jakmile zaplněnost překročí stanovenou hranici, začne se s náhodným odhazováním paketů. Intenzita odhazování se stupňuje s úrovní zaplnění fronty. Nevýhodou však je, že RED je efektivní při použití na TCP komunikaci, kdy dochází ke zpomalování toku. Při aplikaci na UDP pakety, jsou sice pakety zahozeny, avšak jejich tok se nezpomaluje.
- **Weighted Random Early Detection (WRED)** je jedná se o vylepšený algoritmus RED. WRED umožňuje definovat více odhazovacích profilů, přičemž všechny profily mohou být aplikovány nad jednou frontou. Díky tomu můžeme dosáhnout různé pravděpodobnosti odhození paketů v rámci jedné fronty. Profily mohou být nastaveny

tak, že každý si „hlídá“ pouze jemu přidělené pakety a ty pak zahazuje. Je důležité zmínit, že ani tento mechanismus se nedokáže vyrovnat s datagramy UDP.

Je důležité si uvědomit, že využití správy front na komunikaci, která využívá výhradně UDP pakety, postrádá význam. Při zahazování TCP paketů, se rychlost toku zpomaluje, zatímco u paketů UDP tomu tak není. Kontinuálním zahazováním bychom pouze narušili konzistenci dat a datový tok by se nezměnil. Docházelo by pouze ke zbytečnému plýtvání síťovými prostředky.

1.7.5 Omezování a tvarování provozu

Omezování a tvarování provozu patří mezi další metody, kterými lze přispět k nastavení a zajištění optimální kvality služeb. Jedná se o nástroje, které slouží ke správě šířky pásma, potažmo rychlosti, jakou jsou pakety odesílány. Účelem těchto nástrojů je omezení šířky pásma pro daný provoz. Při omezování nastavíme maximální možnou šířku, kterou nemůže daná komunikace překročit. Obě dvě metody využívají pro odesílání paketů algortimus Token Bucket (či jeho obdobu Dual Token Bucket), který již byl zmíněn v souvislosti s klasifikací a značkováním provozu. Každá metoda však ke své práci přistupuje odlišně.

- **Omezování provozu (Traffic Policing)** využívá samotný algoritmus Token Bucket, kdy přicházející pakety odebírají žetony z pomyslného kbelíku. Pokud již nejsou k dispozici žetony, je to znamení, že bychom překročili maximální šířku pásma. V takovém případě jsou pakety automaticky zahazovány.
- **Tvarování provozu (Traffic Shaping)** využívá kromě algoritmu Token Bucket některou z front (nejčastěji CBWFQ). Pakety se nejdříve řadí do front. Pokud jsou v kbelíku žetony, pakety jsou z front odebírány a dále zpracovány. Výhodou je, že pokud v kbelíku dojdou žetony, nemusí to znamenat okamžité zahazování komunikace. K odhazování paketů dochází až v případě zaplnění celé fronty.

1.8 PER-HOP BEHAVIOR

Per-Hop Behavior neboli PHB je další prvek, který se úzce váže s QoS, především s modelem diferencovaných služeb. PHB lze [10] popsat jako chování jednotlivých prvků sítě při zpracování a přeposílání paketů. V základu rozlišujeme čtyři standardní PHB:

- **Default PHB** je základní nastavení, které využívá Best Effort model. Používá se i v případě, že na rozhraní přijde paket, jehož DSCP není spojeno s jiným PHB. Doporučená hodnota DSCP pro pakety dle [12] je *000000*.
- **Class-Selector PHB** je navrženo pro udržení zpětné kompatibility s IP-precedence. Využívá téměř stejné přeposílací chování, jaké používá IP-precedence založená na klasifikaci a přeposílání. Doporučená hodnota DSCP dle [12] je *xxx000*, kde *x* značí číslo 1 nebo 0. Například hodnota DSCP 110000 znamená IP-precedence 110.
- **Expedited Forwarding PHB** představuje klíčové chování pro služby, u kterých vyžadujeme nízkou ztrátovost, zpoždění a jitter. Toto PHB využívají aplikace jako VoIP či video. Doporučené DSCP dle [12] je *101110*.
- **Assured Forwarding PHB** je chování vymezené pro pakety, u kterých vyžadujeme záruku doručení. Assured Forwarding PHB lze dále rozdělit na 4 třídy AF1 – AF4. Každá třída má přidělenou velikost bufferu a šířku pásma. Kromě toho má přidělené i tři úrovně přednostního zahazování. Rozdíly mezi třídami jsou nejčastěji dány propustností. Nejdříve se vždy zahazují pakety z nižších tříd. Doporučené označení DSCP podle [12] je *001010 – 100110*.

1.9 MPLS – MULTIPROTOCOL LABEL SWITCHING

MPLS je další alternativou pro zajištění bezproblémového a rychlého přenosu, přičemž využívá upravený systém směrování. Často je MPLS zmiňován [5] jako protokol 2,5 vrstvy či jako hybridní protokol. Při běžném přenosu datového toku v síti je zkoumána hlavička paketu a na základě získaných informací je zjištěna cesta ve směrovací tabulce. Následně je paket odeslán přes daný port. Na každém směrovači tak dochází k opětovné kontrole, hledání cesty a přeposílání. MPLS přistupuje k přeposílání paketů jinou cestou. MPLS [13] využívá vlastního návěstí a značek, které se dají přirovnat k poštovním směrovacím číslům, díky kterém je mnohem lehčí a rychlejší určit cílovou destinaci doručení než vyhledáváním dle adresy.

Technologie MPLS pracuje v rámci referenčního modelu ISO/OSI mezi linkovou a síťovou vrstvou, díky čemuž jí mohou využívat nejrůznější technologie, mezi které se řadí Ethernet, ATM, Frame Relay nebo PPP.

Vzhledem k možnosti implementace na nejrůznějších technologiích i své rychlosti je využíván ve firemním prostředí při realizaci VPN. Mluvíme tak o MPLS VPN, která je vytvořena na

síťové vrstvě a je založena na peer modelu. Díky tomu je mnohem pružnější, bezpečnější a nabízí snadnou realizaci i správu.

Pro směrování se využívá MPLS návěstí, které obsahuje [5][13]:

- **Label** představuje návěstí, podle kterého probíhá přepínání paketů.
- **EXP** (Experimental) je pole pro experimentální použití, nejčastěji využíváno právě při QoS.
- **S** (Bottom Stack) je informační bit, udávající zda rámec nese více MPLS informací.
- **TTL** (Time To Live), který představuje dobu „života“ paketu.

Komunikace pomocí MPLS probíhá vždy pouze v uzavřené virtuální skupině, která je označována jako MPLS doména. Funkce směrovacích zařízení v doméně závisí na jejich umístění. Hraniční směrovače **LER** [5] (Label Edge Router) slouží pro přidělování či odebírání MPLS návěstí paketům, které přicházejí či opouštějí doménu. Vnitřní směrovače **LSR** [5] (Label Switched Router) pak slouží pro přepínání provozu po předem definované cestě. Když paket vstupuje do MPLS domény, LER jej na základě IP adresy přiřadí do jedné z několika tříd FEC (Forwarding Equivalence Class). Podle třídy je následně paketu přiřazeno návěstí, které definuje cestu pro LSR.

Právě úprava tříd a FEC a definování různých cest může být jednou cestou, jak lze ovlivnit kvalitu služeb. Je třeba si však uvědomit, že samotné MPLS nedefinuje nové mechanismy pro QoS. V rámci MPLS je nejčastěji využívána upravená architektura DiffServ.

2 VÝSLEDKY DOTAZNÍKŮ

V rámci splnění cíle mé bakalářské práce, tedy osvětlení principu zajištění kvality služeb ve firemním prostředí, byl vytvořen dotazník, jenž byl rozeslán do několika firem. Na základě výsledů bude v následující části vytvořen model topologie a předvedena ukázková konfigurace QoS.

V této konfiguraci by měla být pokryta co největší množina požadavků, jenž byly uvedeny dotázanými firmami. Je důležité mít na mysli, že každá firma používá rozdílné vybavení a zdroje. Tudíž mohou být odpovědi značně rozdílné. Větší firmy často používají ve své firemní síti směrovače (routery), zatímco menší společnosti mají sítě založené na přepínačích (switche).

2.1 OTÁZKY

Dotazník byl vytvořen pomocí Google Docs a byl rozeslán vybraným firmám. Hlavní výhodou takto vytvořeného dotazníku je jednoduchá tvorba, rozšiřitelnost a zaznamenávání výsledků do cloudového uložiště v přehledné formě.

Otázky byly cíleně voleny tak, aby bylo možné provést následnou analýzu požadavků na kvalitu služeb sítě. Jednotlivé otázky z dotazníku lze nalézt v příloze A. Při tvorbě dotazníku byl kladen důraz na otázky, které dokáže zodpovědět kdokoliv, kdo má na starosti technické vybavení a má zároveň základní povědomí o fungování firmy.

Mezi informace, které byly hlavním cílem dotazníku, patří:

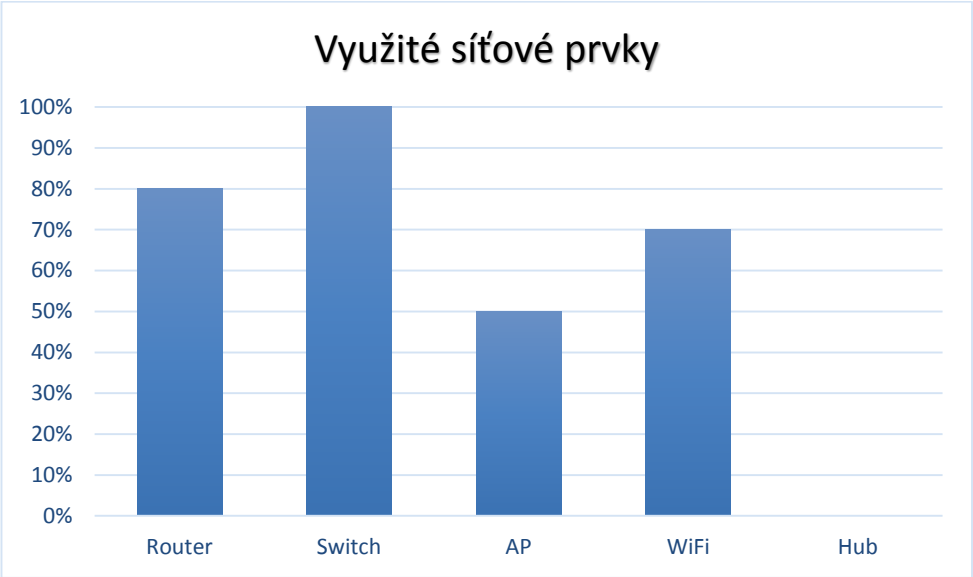
- využívané síťové služby,
- nástroje pro komunikaci,
- používaná síťová zařízení.

2.2 ANALÝZA ODPOVĚDÍ

Následující sekce přibližuje souhrn odpovědi dotázaných společností. Sesbíraný vzorek dat je relativně malý, a proto nelze jasně vyvozovat závěry ohledně globálního využití QoS. Pro účely této bakalářské práce se však jedná o vzorek dostačující.

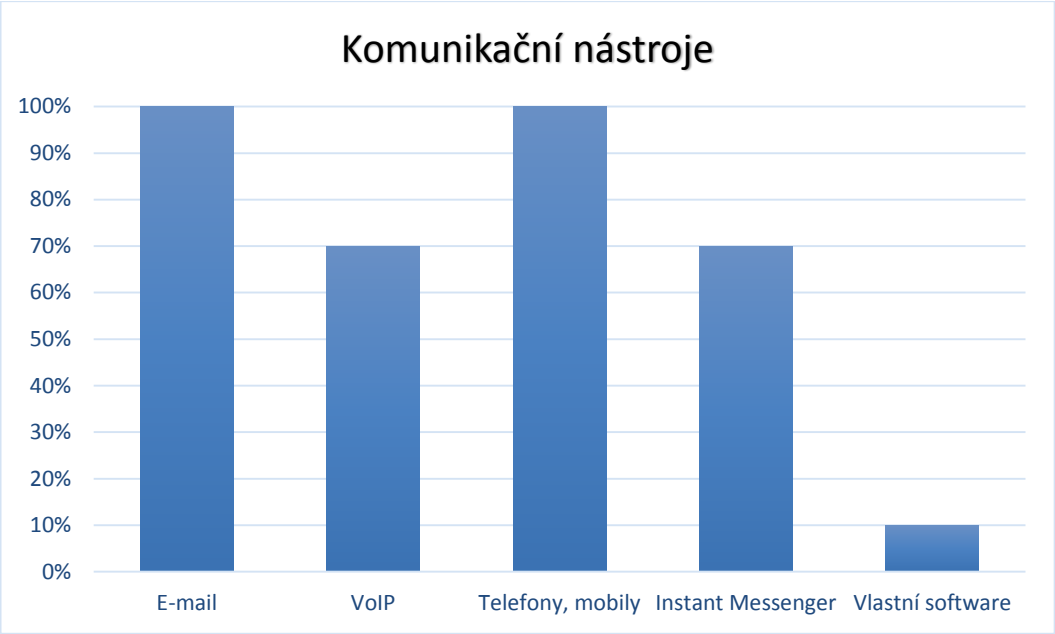
Prvním zkoumaným prvkem bylo využití síťových prvků. Každý síťový prvek nabízí různé možnosti konfigurace a především slouží k rozdílným účelům. Konfigurace QoS se provádí především na směrovačích, které jsou spojovacími uzly rozsáhlé sítě.

Z výsledků vyplynulo, že většina firem využívá celou škálu dostupných síťových prostředků. Nejširší využití mají switche a routery, následované WiFi přístupovými body.



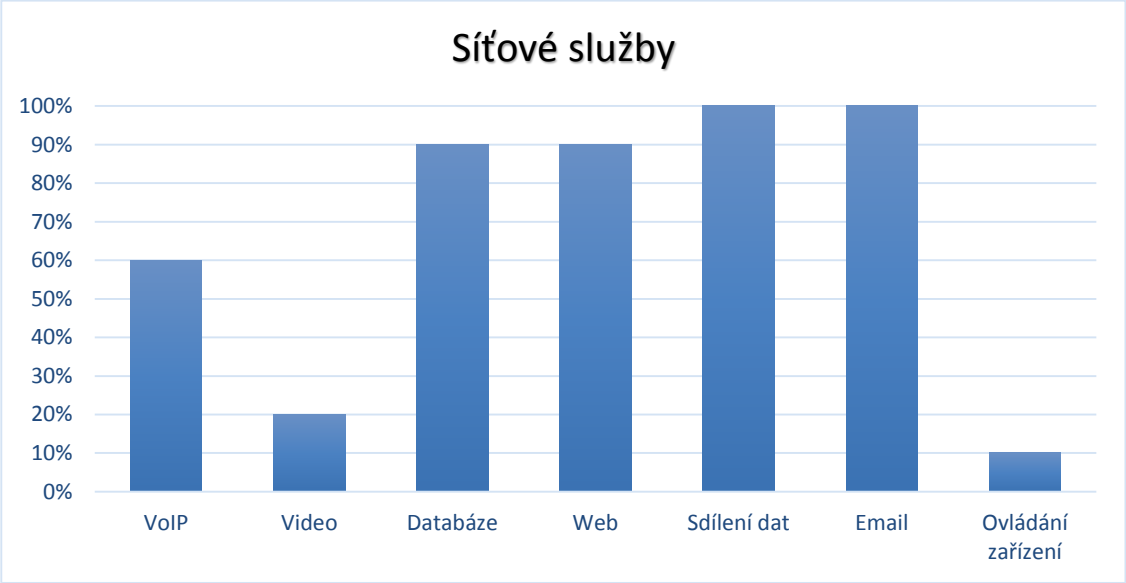
Graf 1 Využívané síťové prvky

Kromě používaných zařízení pro nás byla z pohledu kvality služeb zajímavá i firemní komunikace. Ve světě současného obchodu se žádná společnost neobejde bez perfektně fungující komunikace, ať už se jedná o vnitrofiremní komunikaci nebo komunikaci se zákazníky. Není překvapující, že v komunikaci si drží první příčku zavedená komunikační zařízení, jako jsou mobilní telefony a e-mail. Zajímavé je také poměrně vysoké procento společností využívajících VoIP.



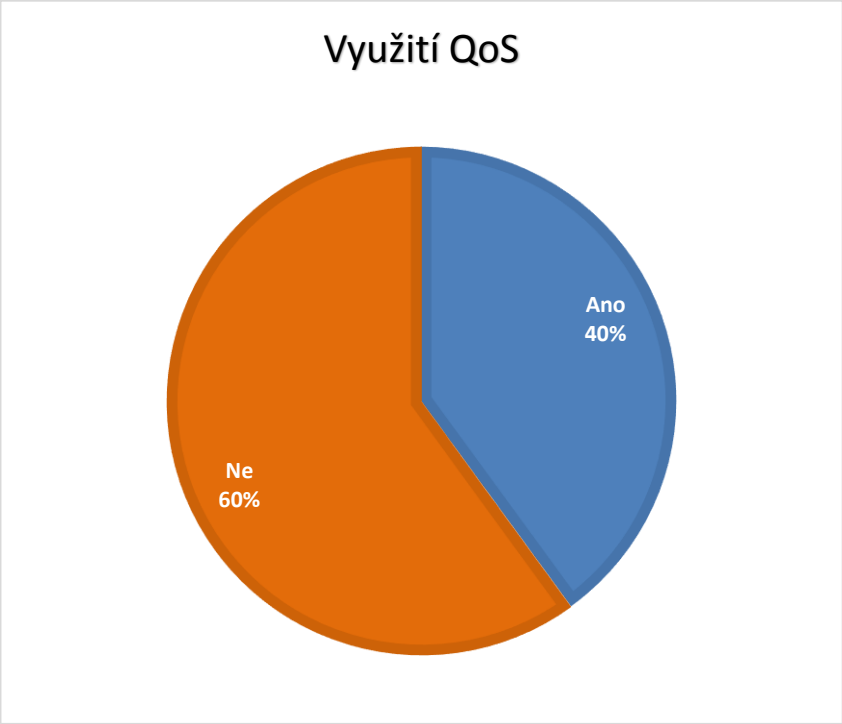
Graf 2 Využívané komunikační nástroje

Dalším prvkem pro bezproblémový chod společnosti jsou využívané síťové služby. Proto byl dotazník směřován i na ně.



Graf 3 Využívané síťové služby

Na závěr byla položena jednoduchá otázka. Používáte ve své firemní síti QoS? Značná část firem na tuto otázku odpověděla kladně. Jedná se především o firmy, které využívají široké spektrum síťových služeb a mezi jejich komunikační prostředky patří VoIP či video přenosy.



Graf 4 Využití QoS v oslovených firmách

2.3 ZHODNOCENÍ

Z výsledků dotazníků a osobní komunikace s některými správci sítě, vyšel poměrně očekávaný závěr. Většina malých a středních firem má firemní síť realizovanou především pomocí přepínačů neboli switchů. Nejčastěji se setkáváme s topologií hvězda či méně rozvětvený strom.

Pro obecnou představu si můžeme představit topologii, která obsahuje centrální router či core switch, přes který proudí veškerá komunikace a na něj jsou napojeny další směrovače, které propojují všechny části sítě. Z toho vyplývá, že router či core switch musí zvládat obsluhu veškerých síťových požadavků směřující především do okolí firemní sítě. Kvůli velkému zatížení je riziko odhození některých paketů.

U větších firem a korporací lze najít všechny dostupné síťové prvky. Nalezneme zde častější využití směrovačů než v předchozím případě. Využití směrovačů umožňuje rychlejší a efektivnější komunikaci v rozsáhlé síti. U velkých firem se lze často setkat i s implementovanými mechanismy QoS. Je totiž velmi důležité zajistit bezproblémovou

komunikaci se zákazníky, helpdesk i vnitrofiremní komunikaci. Za tímto účelem je nejefektivnějším a nejlevnější způsobem využití VoIP telefonie. Kromě efektivnější komunikace a nasazení QoS umožňují směrovače další funkci, kterou přepínače postrádají. Je to možnost tvorby VPN, které je pro mnoho společností nepostradatelná. Ať již kvůli dceřiným společnostem, které využívají centrální firemní zdroje, nebo kvůli detašovaným pracovištím. Důležité je si uvědomit, že i přes VPN lze využít určité prvky zajištění kvality služeb.

3 MODEL SÍTĚ A APLIKACE QOS

Na základě dotazníků bylo zjištěno, že většina firem má stávající síť založenu převážně na přepínačích a směrovačích, které se starají především o odesílání dat z firemní sítě. LAN sítě jsou většinou velmi rychlé, a tudíž nepotřebují zásahy ze stran QoS. Zajišťování kvality služeb přichází na řadu až na hranicích sítě. LAN sítě pracují s rychlostmi nejčastěji 100 Mbit/s – 1 Gbit/s. Páteřní sítě jsou pak ještě o řád rychlejší, tedy dosahují rychlostí až 10 Gbit/s. Problém s rychlostí však nastává při propojování jednotlivých poboček či připojování lokální sítě k Internetu. Zde se nejčastěji nachází linka s omezenou rychlostí, např. 10 Mbit/s. Konfiguraci QoS tedy nejčastěji provádíme na směrovači či L3 přepínači, který propojuje naši LAN síť s další sítí. Pro efektivnější nastavení lze využít obou prvků, tedy L3 přepínače a směrovače. Přístupový switch slouží pro rozdělování a klasifikaci síťového provozu, tak aby na směrovači docházelo k lepšímu a rychlejšímu zpracování tohoto provozu.

Díky rozličným datovým tokům a velkým nárokům na firemní síť je ideálním řešením pro zajištění kvality služeb mechanismus diferencovaných služeb. V rozlehlé síti s několika směrovači a různými rychlostmi linek umožňuje DiffServ vytvoření několika domén, značkování a přeznačkování paketů a zvládá aktivní správu front. Oproti staršímu mechanismu integrovaných služeb sice nemá záruky doručení, avšak nehrozí u něj riziko „vyhladovění“ určité komunikace a zabrání celé šířky pásma pouze prioritním provozem. Další výhodou je lepší využití DiffServ v rozsáhlých sítích s tendencí dalšího růstu. Mechanismus diferencovaných služeb nám pomáhá zajistit, že při správné konfiguraci zůstanou síťové prostředky dostupné všem uživatelům a typům provozu. Mezi další vlastnosti diferencovaných služeb patří také jejich škálovatelnost. V případě, že do sítě bude potřeba přidat další zařízení, není nutná opětovná konfigurace ostatních síťových prvků.

Každý prvek v síti může spadat do jiné domény a může mít jinak nastavenou prioritu pro síťový provoz. To značně usnadňuje konfiguraci, pokud se o zařízení nestará pouze jeden správce. Není nutné dodržovat stejné nastavení pro komunikaci, a proto se v každé doméně mohou prvky k vybraného síťového provozu chovat jinak.

3.1 HARDWAROVÉ VYBAVENÍ

Topologie a názorná konfigurace bude prováděna s pomocí směrovačů z řady Cisco 2800 Series Integrated Services Routers s operačním systémem Cisco IOS 15.1. Vzhled tohoto směrovače zobrazuje obrázek 7. Každý směrovač je vybaven minimálně dvěma sériovými porty

s rychlostí až 8 Mbit/s. Dále každý směrovač disponuje dvěma Fast Ethernetovými a jedním Gigabit Ethernetovým portem pro připojení počítače či celé LAN sítě.

Z důvodu přehlednosti budou při konfiguraci využity pouze počítače, které budou generovat síťovou komunikaci. V praxi by na fast ethernetovém či gigabit ethernetovém portu byla přes core switch napojená celá firemní LAN síť.

Obrázek 7 Cisco 2800 Series Integrated Services Router

3.2 POUŽITÝ SOFTWARE

Pro konfiguraci a ověřování získaných výsledků je potřeba kromě Cisco IOS i další software, jenž nám umožní generování a následné ověřování komunikace.

Za tímto účelem je využit profesionální program IxChariot [14] od společnosti Ixia. Tento software slouží pro ověřování výkonu sítě při zatížení. Mezi hlavní výhody řadíme velké množství integrovaných skriptů, které je možné dle potřeby upravovat v jednoduchém editoru. Tyto skripty slouží pro generování komunikace mezi koncovými uzly, na kterých je IxChariot nainstalován. Primární výhodou IxChariot jsou mimo jiné i grafické výstupy, které je možné zobrazovat v reálném čase. Díky tomu nám software umožňuje získat ucelenou představu o výkonu sítě.

Dalším využívaným softwarem je Wireshark [15], jenž je multiplatformní a zároveň nabízí uživatelům přívětivé uživatelské rozhraní. Pomocí Wireshark je možné provést hloubkovou analýzu komunikace, jenže může probíhat v online i offline režimu.

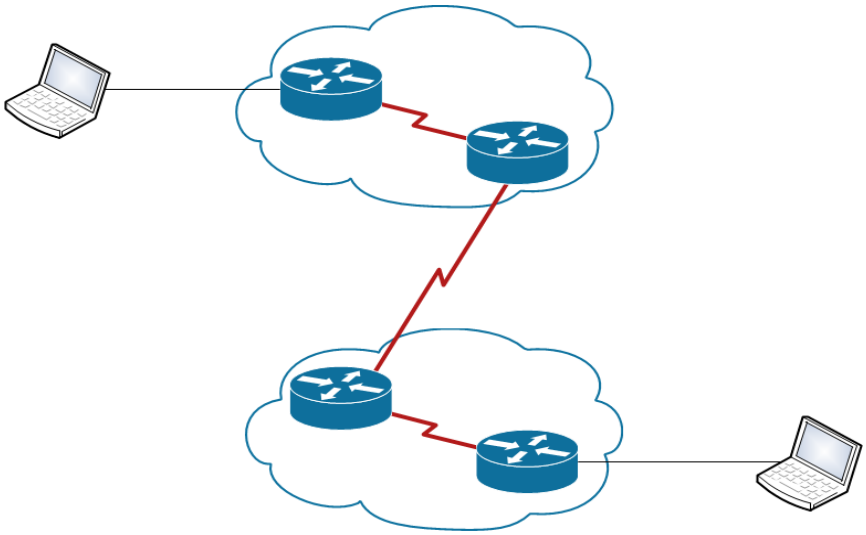
4 APLIKACE QOS POMOCÍ SMĚROVAČŮ

Pro předvedení zajištění kvality služeb byla zvolena aplikace metody diferencovaných služeb pomocí směrovačů. Využitím směrovačů se snažíme zajistit bezproblémový provoz v rámci rozsáhlé síti. Směrovače jsou většinou propojeny pomocí sériových linek, které mají oproti fast ethernetu značně omezenou rychlost.

Abychom sníženou šířku pásma a přenosovou rychlost vynahradili, potřebujeme zajistit klasifikaci paketů a následné přednostní zpracování přenosu dat, která jsou náchylná na výpadky a zpoždění.

Cílem práce je předvedení maxima možností, jenž nám DiffServ nabízí. Z toho důvodu bude ukázková konfigurace a následná měření provedena na topologii s více DiffServ doménami. Mezi jednotlivými doménami je možnost přeznačkování paketů, díky čemuž mohou mít nastavenu jinou prioritu v každé doméně. Toto je výhodou především v případě, že rozsáhlou síť spravuje více správců, či jsou značné rozdíly mezi rychlostí linek v jednotlivých částech sítě.

Naše síť, na které bude konfigurace předváděna, je zjednodušená firemní síť. Toto zjednodušení vychází z menšího množství dostupných síťových prvků a zároveň tato jednoduchost bude předpokladem pro snazší orientaci při konfiguraci a popisu.



Obrázek 8 Zjednodušená firemní síť

Na základě dotazníků nám vyplynulo, že mezi často využívané služby patří především VoIP komunikace, přístupy k databázovým údajům, email a v některých případech i videokonference. Simulovaný model je navržen jako zjednodušená síť, která by mohla být využita například

v odvětví pojišťovnictví. V tomto odvětví je důležitá především komunikace na pracovišti i s klienty, kterou může nejefektivněji zajistit právě VoIP. Pro vnitřní komunikaci a školení lze využít kromě VoIP i streamované video či videokonference. K tomuto účelu Cisco nabízí WebEx, který je používán ve firmách u nás i v zahraničí. WebEx je software pro webové konference s možností sdílení souborů, prezentací, integrovanými VoIP a video službami.

I přesto, že minimum společností v dotazníku vyplnilo, využívání video přenosů, bude v konfiguraci video zahrnuto. Přenos hlasu a videa v reálném čase patří mezi základní prvky pro aplikaci QoS.

Samozřejmě je možné využití zajištění kvality služeb i pro datové přenosy, avšak v tomto případě není rozdíl tak patrn. Mimo jiné je důležité, že při přenosu dat musí být brán ohled i na další prvky, které se na komunikaci podílejí. To znamená, že pokud provedeme databázový dotaz, je cesta sítí pouze jeden z faktorů rychlosti. Významnou roli zde hraje i samotná rychlost databázového serveru, jeho zatížení a složitost (komplexnost) databázového dotazu.

4.1 PŘÍPRAVA PRO APLIKACI QOS

Před samotnou konfigurací QoS je nutné označit komunikaci, která má být upřednostňována. Již bylo zmíněno, že pro označení způsobu, jakým má být paket zpracován, je použita hodnota PHB (Per-Hop Behavior). PHB má několik tříd, z nichž některé lze rozdělit do dalších podtříd. Bližší informace k Per-Hop Behavior byly probrány v kapitole [1.8].

PHB může být nastaveno pomocí dvou základních způsobů. Velmi často označení nabízí přímo aplikace, kterou při komunikaci používáme. Například zmiňovaný Cisco WebEx Communications nabízí automatické označení VoIP pomocí hodnoty *DSCP* 46, v označení PHB *EF*, a videa pomocí hodnoty *DSCP 34*, v označení PHB *AF41*. Tyto hodnoty patří mezi uznávané standardy. Hodnoty DSCP může správce sítě využívat dle svého uvážení, jelikož zařazení do určité třídy ještě neznamená zpracování paketu. Je ovšem vhodné využívat doporučené hodnoty DSCP pro vybraný provoz. Některé prvky mají již automaticky nakonfigurované přednostní obsluhování aplikací dle DSCP a kromě toho, jednotné značení usnadňuje komunikaci při správě rozsáhlé sítě.

Další možností je využití access listů neboli ACL. S pomocí ACL můžeme vybírat pakety na základě zdrojové a cílové IP adresy, portu i používaném protokolu. Samozřejmě může být využita případná kombinace více nebo všech zmíněných atributů. Na základě access listů je

možné tvořit třídy provozu nebo je rovnou využívat pro aplikaci QoS. Nabízejí se nám tedy dvě možnosti:

- Konfigurace QoS pomocí ACL,
- Vytvoření tříd provozu na základě ACL

4.1.1 Konfigurace pomocí ACL

Při konfigurace postavené na ACL dochází k vytvoření tříd, se kterými se pracuje na výstupním rozhraní. Na základě tříd je prováděna identifikace komunikace, přidělení vyhrazeného pásma a způsobu zpracování. Při této metodě se nepoužívá vstupní třída pro přeznačkování komunikace. Nevýhodou je však nutnost vytvoření ACL na všech hraničních prvcích, na nichž má docházet k označování a úpravě komunikace. To může vést k množství chyb a vyšším nárokům na konfiguraci.

Konfigurace class-map:

```
R1(config)#class-map Vystup
R1(config-cmap)#match access-group vystupniACL
```

Konfigurace policy-map:

```
R1(config)#policy-map Politika
R1(config-pmap)#class-map Vystup
R1(config-pmap-c)#bandwidth percent 15
```

Napojení na rozhraní:

```
R1(config)#interface Serial0/0/0
R1(config-int)#service-policy output Politika
```

4.1.2 Vytvoření tříd provozu

Druhou a pravděpodobně výhodnější variantou je vytvoření tříd, kterým je následně na vstupním rozhraní přidělena hodnota DSCP. V rámci prioritizace, tvarování a omezování komunikace na výstupním rozhraní se již pracuje se třídami a politikami, které jsou definovány pomocí DSCP. Při využití doporučených hodnost DSCP je konfigurace napříč síti mnohem snadnější a méně náchylná k vytvoření chyb.

Konfigurace class-map:

```
R1(config)#class-map Vystup
R1(config-cmap)#match access-group vystupniACL
```

Konfigurace policy-map:

```
R1(config)#policy-map PreznaceniNaDSCP
R1(config-pmap)#class Vstup
R1(config-pmap-c)#set dscp af41
```

Napojení na rozhraní:

```
R1(config)#interface Serial0/0/0
R1(config-int)# policy-service input PreznaceniNaDSCP
```

Přeznačování paketů se uskutečňuje především na vstupním portu směrovače. Je teoreticky možné využít výstupní port, ale ten je primárně určen pro aplikaci metodiky QoS. Je to vcelku logické, paket musí projít nejprve zpracováním, které zajišťuje směrovač. Každý směrovač má svou paměť a procesor, s jejichž pomocí se stará o provádění výpočtů. Paměť pak slouží pro udržování front.

Poté co již máme je přeznačování hotovo, můžeme být provedena samotná konfigurace QoS. K dispozici máme veškeré výše popsané prvky, tedy můžeme nastavit velikost fronty pro odhazování, shaping, policing, přednostní přidělení pásma aplikacím. Základem je opět vytvoření class-map. Na jejich základě se vytvoří policy-map, tedy mapa politik, které ovlivňují zpracování paketů. Tato policy-map je aplikována na výstupním rozhraní směrovače. Ve zjednodušené ukázkové konfiguraci je předvedeno vytvoření class-map s názvem *Vystup*, do které spadají všechny pakety s hodnotou *DSCP AF31*. Tedy pakety, které jsou označeny jako mission critical (rozumějme pakety důležitých aplikací) a nejsou zařazeny do tříd pro video či hlasovou komunikaci.

Vytvoření class-map pro výstup:

```
R1(config)#class-map match-all Vystup
R1(config-cmap)#match dscp af31
```

V dalším kroku je vytvořena policy-map, která definuje chování směrovače. V naše případě říkáme směrovači, že si přejeme vyhradit 15 procent z šířky pásma pro tuto komunikaci a vyžadujeme zpracování pomocí CBWFQ, což zajišťuje příkaz `bandwidth`.

Vytvoření policy-map:

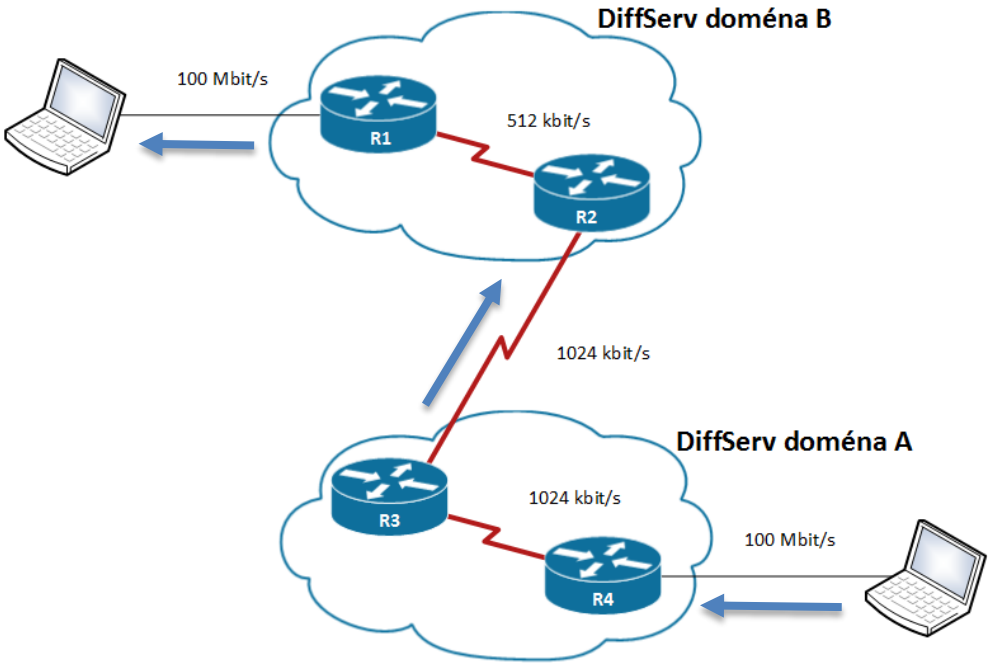
```
R1(config)#policy-map AplikacePravidelQoS
R1(config-pmap)#class Vystup
R1(config-pmap-c)#bandwidth percent 15
```

Napojení na výstupní rozhraní směrovače:

```
R1(config)#interface serial0/0/1
R1(config-if)#policy-service output AplikacePravidelQoS
```

4.2 Scénář pro aplikaci QoS

Pro aplikaci QoS byla zvolena topologie se třemi základními šířkami pásma, a to 1024 kbit/s, 512 kbit/s a 100 Mbit/s. Různé rychlosti představují skutečnost, že se síť skládá z několika částí a tak i k zajišťování kvality služeb je potřeba přistupovat v každé části rozdílným způsobem. Z výše uvedených parametrů topologie vyplývá, že nejlepší volbou pro aplikaci QoS v rámci této sítě je metoda DiffServ.



Obrázek 9 Ukázková topologie pro konfiguraci

Počítače jsou připojeny ke směrovačům pomocí fast ethernetových linek s výchozí rychlostí 100 Mbit/s. Mezi směrovači v doméně A a zároveň mezi doménami A a B jsou linky s šířkou pásma 1024 kbit/s. V doméně B se pak nachází nejpomalejší linka v síti s šířkou pásma pouhých 512 kbit/s. To je polovina předchozí šířky pásma, a proto bude tato linka také nejvíce ovlivňovat výslednou kvalitu služeb.

Směr, kterým bude komunikace směrována, zobrazují šipky na obrázku 9. Důležitou roli v naší konfiguraci hrají hraniční směrovače jednotlivých domén. Jelikož jsou v každé doméně pouze dva směrovače, jsou oba hraniční. Pro námi vytyčený zvolený směr jsou však důležité pouze hraniční směrovače R4 a R2. Komunikace do domény vstupuje touto cestou a tak bude nutné zajistit přeznačení hodnot DSCP na vstupním rozhraní a aplikaci metodiky QoS na výstupním.

V datové komunikaci budou generovány čtyři datové proudy, a to VoIP, video, databázové dotazy a FTP.

Pro hlasovou komunikaci byl zvolen kodek G.711u s rychlostí 64 kbit/s, což je nejvyšší kvalita jakou nám simulační program IxChariot umožňuje. Kodek G.711u [16] patří mezi nejjednodušší a nejrozšířenější standard schválený ITU (International Telecommunication Union) používaný v telekomunikacích. Kodek využívá bezztrátové logaritmické komprese a poskytuje nejvyšší kvalitu zvuku.

Pro video byl zvolen kodek MPEG-2 s rychlostí přenosu 400 kbit/s, kde byla nižší rychlost zvolena kvůli nízké kapacitě linky mezi směrovačem R1 a R2. Tato linka dosahuje pouhých 512 kbit/s. Kodek MPEG-2 [17] je ztrátový komprimační datový formát, který slouží pro snížení datového toku, a tak se ideálně hodí pro využití v počítačové síti. S rychlostí 400 kbit/s se sice nejedná o nejkvalitnější video přenos, avšak pro tento případ je hodnota zcela dostačující. Video komunikace je generována pomocí předpřipraveného skriptu na jedné stanici a zachycována a zpracována na stanici druhé.

FTP komunikace a přístup k databázi jsou další dvě formy komunikace, které jsou ve firemním prostředí naprosto běžné a budou nám vytvářet další provoz, který může ovlivňovat výslednou komunikaci. Na přístupu k databázi bude kromě toho aplikován policing a přeznačování hodnoty paketů při přechodu mezi doménami.

4.2.1 Základní konfigurace

Pro námi vytvořenou síť jsme zvolili jako směrovací protokol OSPF. Pro tuto volbu existuje několik důvodů. Hlavním důvodem je, že OSPF zohledňuje na rozdíl od ostatních směrovacích protokolů stav linky a vytváří si v paměti směrovače kompletní mapu topologie celé sítě. Nad touto mapou pak používá výpočty pro nalezení nejvhodnější cesty. Metrikou je cost, neboli cena linky, která je vypočítána z šířky pásma. Čím nižší je hodnota, tím bude cesta preferovanější. Díky tomu se OSPF ideálně hodí pro aplikace QoS. Výpočet ceny linky popisuje následující vzorec:

$$cost = \frac{100000000}{bandwidth\ [bps]}$$

Mezi další výhody patří kompatibilita s MPLS, které je ve firemních sítích hojně využíváno či fakt, že se jedná otevřený standard IETF a je tak možné jej používat na všech zařízeních.

Ne každá společnost disponuje vybavením Cisco, což je zapříčiněno především vyšší pořizovací cenou síťových prvků.

Dalším důležitým krokem je nastavení šířky pásma na rozhraních směrovačů. Tyto hodnoty nejenže používá směrovací protokol OSPF, ale také mohou být používány pro výpočty v rámci QoS. Konfigurace na směrovači je pak vcelku triviální:

```
R1#configure terminal
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#clock rate 512000
R1(config-if)#bandwidth 512
```

Za povšimnutí stojí příkazy `clock rate` a `bandwidth`. Příkaz `clock rate` se využívá při spojení pomocí sériových linek, kdy jeden konec je vždy označen jako DTE (Data Terminal Equipment), a druhý jako DCE (Data Communications Equipment). Clock rate se nastavuje na zakončení DCE a udává rychlost linky v *bit/s*.

Příkaz `bandwidth` pak slouží pouze pro účely směrovacích protokolů a aplikaci QoS. Tímto způsobem sdělujeme, s jako hodnotou mají směrovače při svých výpočtech pracovat. Bandwith neboli šířka pásma se pak udává v *kbit/s*.

Síť s touto základní konfigurací je dostačující pro naměření hodnot bez aplikace mechanismů QoS.

4.3 APLIKACE A VÝSLEDKY BEZ VYUŽITÍ QOS

První měření proběhlo bez potřeby přeznačování paketů. Tudíž byla komunikace vysílána s nulovou hodnotou DSCP. Bylo zjištěno, že již při pouhém počátečním označení paketů nenulovou hodnotou DSCP se směrovač pokoušel o přidělení vyšších priorit takto označené komunikaci. Díky tomu by byly výsledky velmi zavádějící.

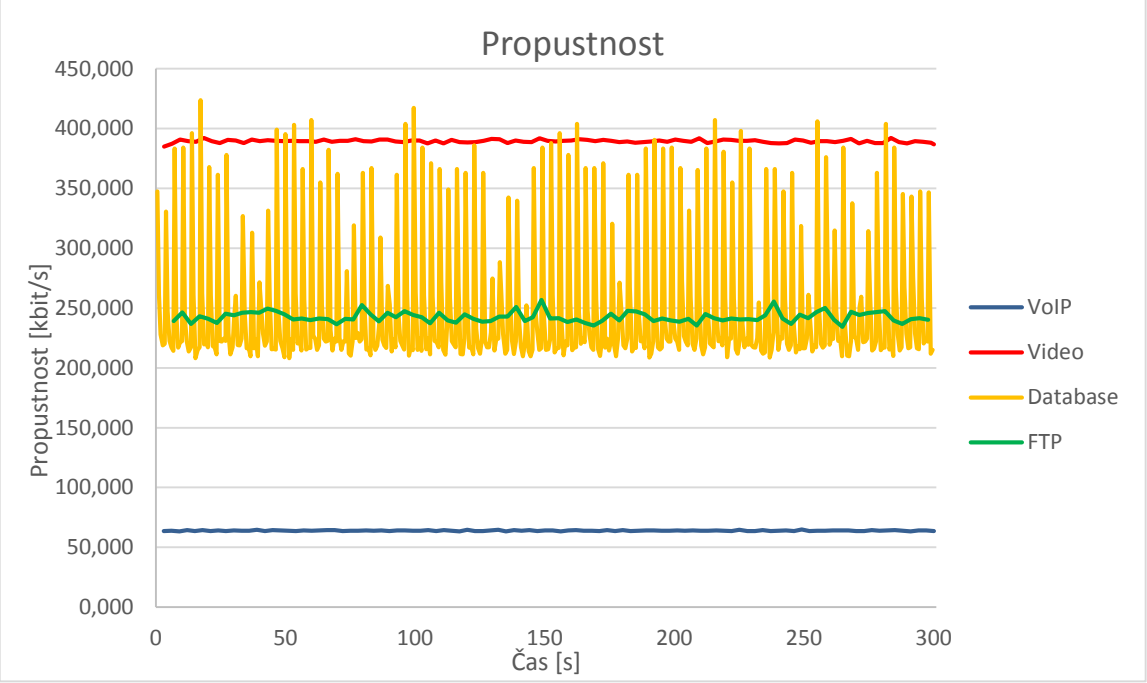
Abychom si budoucí aplikaci QoS usnadnili, využili jsme pro komunikaci předem definované porty. V opačném případě bychom museli pracovat s rozsahem přidělených portů. V tomto případě, by se některé z nich mohly krýt.

Program IxChariot nabízí celou řadu možných parametrů ke změření. Zaměřili jsme se však na ty nejdůležitější, které nám mohou přinést užitečné informace o výkonu sítě z pohledu kvality služeb.

4.3.1 Propustnost

Mezi první měřené hodnoty patří propustnost, která vyjadřuje množství přenesených dat za jednotku času. Nejčastěji se uvádí v *bit/s*, *kbit/s* či *Mbit/s* podle rychlosti linky. Je důležité si uvědomit, že v naší testovací topologii má nejpomalejší linka dostupnou šířku pásma pouhých 512 kbit/s. Proto nelze očekávat hodnoty propustnosti nad touto hranicí.

Na grafu je jasně vidět, že aplikace se snaží zabrat maximum pásma, které mají k dispozici. Z grafu je také patrné, že všechny toky kromě databázových dotazů vyžadují konstantní šířku pásma. Databázové dotazy jsou nárazové a krátké, což se projevuje i na kolísání hodnot. Je patrné, že nejvyšší šířku pásma pro své potřeby si zabírá video, které pracuje na protokolu UDP, a tudíž nedochází k žádnému zpomalování případnými ztrátami paketů. VoIP se drží na poměrně nízkých hodnotách, to je však zapříčiněno tím, že vyžaduje pouze něco málo přes 60 kbit/s.



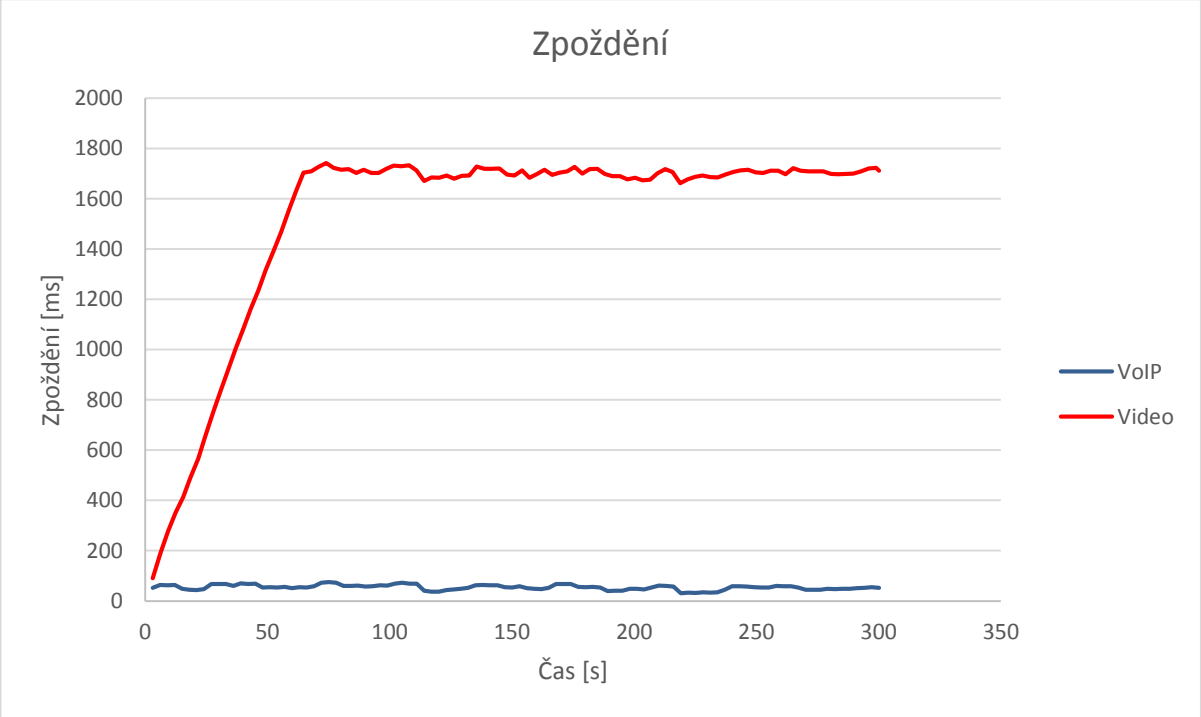
Graf 5 Propustnost bez využití QoS

Další sledované prvky se zaměřují pouze na provoz, který je na aplikaci kvality služeb z velké míry závislý. Proto se v dalších grafech bude objevovat především hlasová komunikace a video.

4.3.2 Zpoždění

Další sledovaná hodnota je zpoždění, které je velmi důležité pro porozumění komunikace. Velké prodlevy v komunikaci jsou nepřípustné a mohou celý proces značné komplikovat. Při velkém zpoždění paketů se jednotlivé strany mohou překrývat v přenosu a znemožnit tím plynulý průběh komunikace. Zpoždění je uváděno v hodnotách *ms* a je vhodné připomenout, že v ideálním případě by hodnota neměla přesáhnout 150 ms. A to jak u hlasové komunikace, tak u videa.

Z následujícího grafu je patrné, že pokud nejsou využity mechanismy QoS dochází především u videa ke značnému zpoždění, které se po ustálení drží v průměru na hodnotě 1702 ms. To je o 1035% více, než jsou doporučené hodnoty. V takovémto případě, nejen že by došlo k narušení plynulosti, ale při této ztrátovosti by byla video komunikace nepoužitelná.



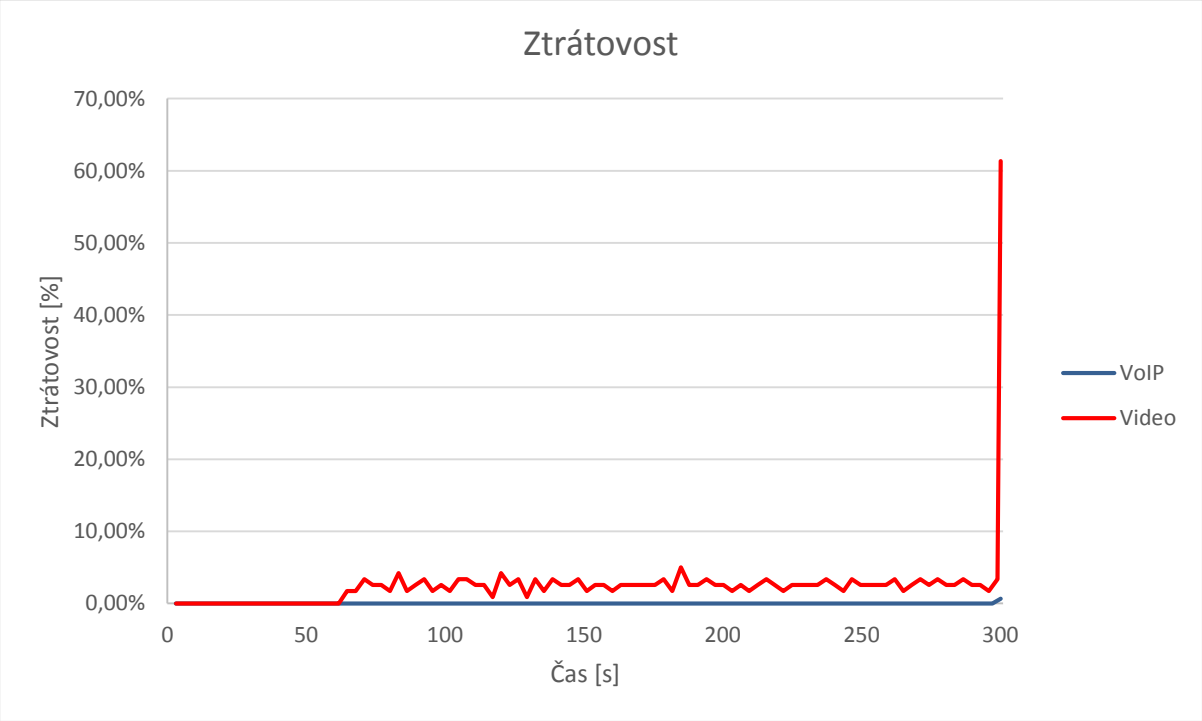
Graf 6 Zpoždění bez využití QoS

4.3.3 Ztrátovost

Dalším ze zohledňovaných parametrů je ztrátovost. Tato hodnota udává, kolik procent dat, bylo při přenosu v aktuálním čase ztraceno. Zde je vhodné připomenout, že ztrátovost videa i zvuku by se v ideálním případě měla pohybovat pod hodnotou 1 %. Na následující grafu je poměrně jasně patrné, že v první části měření byla ztrátovost nulová. Později u videa vystoupala na průměrnou hodnotu 2,61 %. Tato hodnota není ideální. Pokud by však komunikace závisela

pouze na této hodnotě, bylo by video pravděpodobně ještě použitelné. Je nutné si však uvědomit, že sledovaná ztrátovost je přímo spojená s narůstající hodnotou zpoždění, které bylo zobrazeno v předchozím grafu.

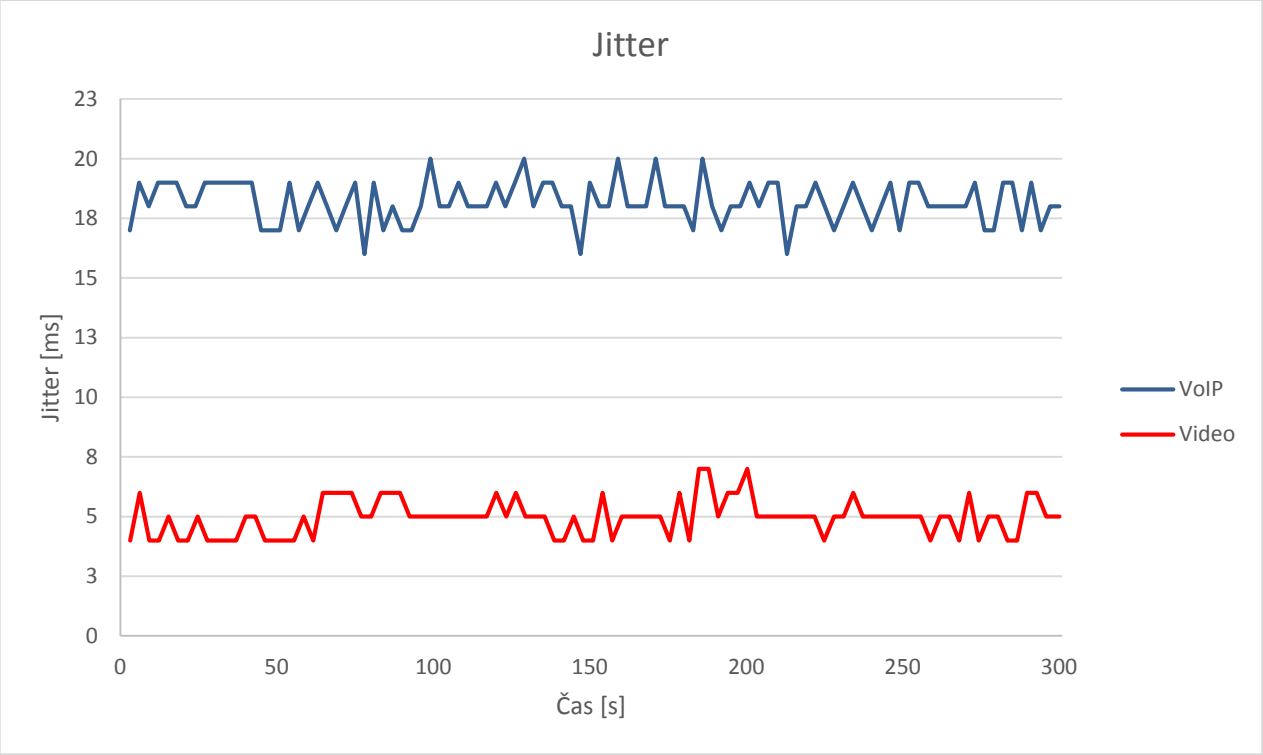
Konečný prudký vzestup ztrátovosti nebereme v úvahu, jelikož se pravděpodobně jedná o následek ukončování veškeré komunikace a zvýšené režie programu IxChariot. V průběhu měření byla data jinak vesměs konstantní. Ztrátovost videa se pohybovala přibližně kolem 2,5 % a ztrátovost hlasové komunikace byla nulová.



Graf 7 Ztrátovost bez využití QoS

4.3.4 Rozptyl zpoždění, jitter

Mezi hodnoty, které nám umožňují určit kvalitu hlasové komunikace i videa, se řadí také rozptyl zpoždění neboli jitter. Rozptyl zpoždení by měl být v ideálním případě konstantní a neměl by přesáhnout 25 ms. Následující graf zobrazuje rozptyl zpoždění bez využití QoS. Díky malému množství směrovačů v topologii jitter nepřekračuje limity pro bezproblémovou komunikaci.

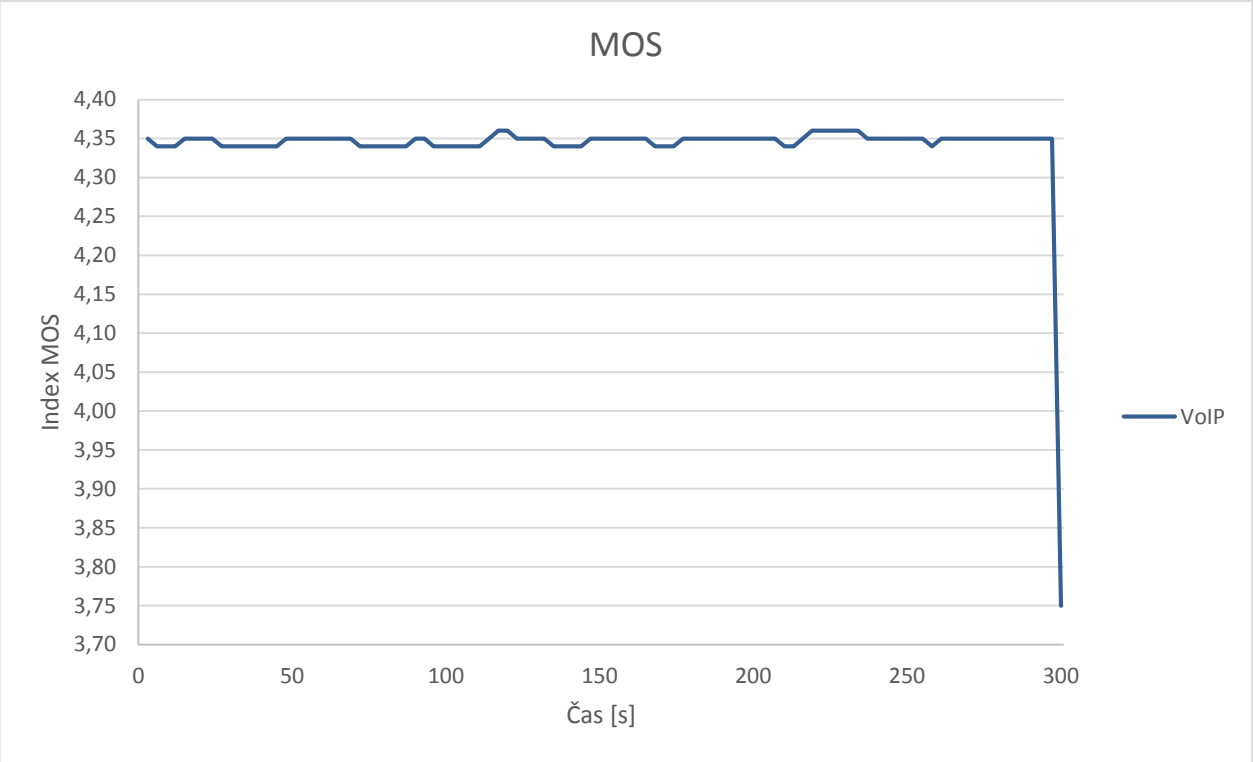


Graf 8 Jitter bez využití QoS

4.3.5 MOS, Meaning Opinion Score

MOS [18] je test, který se po dlouhou dobu využíval v telefonních sítích pro určení kvality přenosu. Později se přeneslo využití MOS i na přenos hlasu po datové síti. MOS je udáván v rozpětí hodnot 1 – 5.

Z následujícího grafu je patrné, že se hodnota MOS po celou dobu drží ve velmi dobrých hodnotách, což odpovídá i zbylému průběhu hlasové komunikace. I bez využití QoS byla šířka pásma a výkon sítě dostačující pro kvalitní přenos hlasu. Opět zanedbáváme konečnou fázi, kterou pravděpodobně způsobila vysoká režie měřícího programu. Po celou dobu měření zůstaly hodnoty téměř neměnné a případné odchylky byly minimální.



Graf 9 MOS bez využití QoS

4.3.6 Závěr měření bez QoS

Při měření byly využity čtyři druhy komunikace, kde pro každou byl definován jeden datový tok. I přesto jsme si ověřili, že při využití videa, jehož datový tok byl nakonfigurován na hodnotu blížící se dostupné šířce pásma, došlo ke značnému ovlivnění komunikace. Samotná hlasová komunikace se díky jednomu datovému toku a nízkým nárokům i na takovéto síti obešla bez problémů. Mezní hodnoty zpoždění, rozptylu zpoždění ani ztrátovosti nebyly překročeny. Kromě toho nám test MOS potvrdil vysokou kvalitu VoIP.

Video na této síti velmi citelně přesáhlo mezní hodnoty pro zpoždění, a tudíž by byla komunikace nepoužitelná. Mezi další překročené hodnoty patří i ztrátovost, která má však v porovnání se zpožděním pouze minimální účinek na výslednou kvalitu.

4.4 APLIKACE METODIKY QOS

Při aplikaci QoS bylo využito označování komunikace pomocí hodnot DSCP. V běžné praxi programy jako WebEx nabízejí automatické značkování paketů na doporučené hodnoty DSCP. Tuto funkci má ve své nabídce i simulační program IxChariot.

Bohužel při praktickém pokusu bylo zjištěno, že i při nastavení hodnot DSCP v programu není komunikace řádně označena. K tomuto problému mohlo dojít použitím operačního systému Windows 8.1, na kterém byl test prováděn nebo mohl problém nastat přímo ve skriptech, které program používá pro generování komunikace.

Abychom tento problém vyřešili, byly jednotlivé skripty upraveny tak, aby byla komunikace odesílána na pouze námi vybrané porty. To značně ulehčilo přípravu ACL, poslouží jako základ pro přeznačování paketů. Pro databázové dotazy byl využit skript simulující komunikaci s MS SQL databází. MS SQL databázový server přijímá dotazy na port 1433 a z tohoto portu je i odesílá. Pro video a VoIP jsme si pak zvolili vlastní porty. Ve skutečnosti totiž video i VoIP pracují na velkém rozsahu portů, z nichž některé se překrývají. To vše navíc závisí na typu použité aplikace. Proto byl jako komunikační port pro video zvolen port 16392 a pro VoIP port 16384. S definovanými porty již není problém navrhnout funkční ACL.

```
R4(config)#ip access-list extended Database
R4(config-ext-nacl)# permit tcp any host 192.168.1.2 eq 1433
R4(config-ext-nacl)# permit tcp host 192.168.1.2 eq 1433 any
R4(config-ext-nacl)# exit
R4(config)#ip access-list extended video
R4(config-ext-nacl)# permit udp any any eq 16392
R4(config-ext-nacl)# exit
R4(config)#ip access-list extended voip
R4(config-ext-nacl)# permit udp any any eq 16384
```

Pokud již máme potřebné ACL nakonfigurované, můžeme přejít k samotnému označování paketů na vstupním rozhraním směrovače. K tomu bylo zapotřebí zajistit pro ACL třídní mapy (class-map). Ty následně slouží pro vytvoření mapy politik, která umožňuje vlastní přeznačování.

```
R4(config)#class-map match-all VoIP_in
R4(config-cmap)# match access-group name voip
R4(config-cmap)# exit
R4(config)#class-map match-all Video_in
R4(config-cmap)# match access-group name video
R4(config-cmap)# exit
R4(config)#class-map match-all Data_in
R4(config-cmap)# match access-group name Database
R4(config-cmap)# exit
```

Napojení na vstupní rozhraní pro přeznačkování paketů:

```
R4(config)#interface FastEthernet 0/0
R4(config-int)#service-policy input REMARK
```

V tomto bodě je přeznačování nastaveno. Veškeré pakety, které vstupují do sítě přes rozhraní FastEthernet 0/0 jsou prozkoumány a pokud odpovídají vytvořeným ACL, jsou přeznačkovány na dané hodnoty DSCP.

Hodnoty jsou odvozené od PHB:

- EF, jenž je doporučená hodnota pro VoIP,
- AF41 představující doporučenou hodnotu pro video komunikaci,
- AF31, což je doporučená hodnota pro důležitou komunikaci, tzv. mission critical.

Následně může být aplikováno zajištění QoS na výstupním rozhraní, kde již můžeme pracovat se správou front, prioritizací, přidělováním šířka pásma a omezováním komunikace. Tedy hlavními nástroji, díky kterým je možné zajistit kvalitu služeb.

Pro konfiguraci na zařízení je opět nutné vytvořit mapy, kterým se budou následně přiřazovat pravidla chování.

Vytvoření class-map:

```
R4(config)#class-map match-all VoIP
R4(config-cmap)#match dscp ef
R4(config-cmap)#exit
R4(config)#class-map match-all Video
R4(config-cmap)#match dscp af41
R4(config-cmap)#exit
```

Následné vytvoření policy-map:

```
R4(config)#policy-map POLICY
R4(config-pmap)#class VoIP
R4(config-pmap-c)#priority percent 9
R4(config-pmap-c)#exit
R4(config-pmap)#class Video
R4(config-pmap-c)#priority percent 41
R4(config-pmap-c)#exit
R4(config-pmap)#class class-default
R4(config-pmap-c)#fair-queue
R4(config-pmap-c)#queue-limit 15
R4(config-pmap-c)#random-detect
```

Při tvorbě této policy-map byl vynechán databázový provoz, jelikož šířka pásma je dostačující pro obsloužení celé komunikace. Konfigurace databázového přenosu bude uvedena v další části při přeznačování paketů na hraničním směrovači DiffServ domény B, což je směrovač R2. Pro pochopení bude výše uvedená konfigurace rozebrána.

Třída VoIP má pomocí příkazu `priority` vyhrazenu minimální šířku pásma 9 %. Pokud dojde k zahlcení sítě je třída automaticky omezována tak, aby tuto hodnotu nepřekračovala. Zpracování paketů je prováděno pomocí LLQ. Stejným způsobem je zpracováno i video, pouze je pro něj vyhrazena minimální šířka pásma 41 %.

Komunikace, která nespadá ani do jedné z výše uvedených tříd, je zpracována pomocí výchozí třídy class-default. Pro tuto třídu je pomocí příkazu `fair-queue` nastavena fronta WFQ, která rozděluje pásmo spravedlivě mezi jednotlivé datové toky. Délka fronty je omezena na 15 paketů pomocí příkazu `queue-limit`. Nastaveno je také včasné zahazování pomocí WRED, které zajišťuje příkaz `random-detect`.

Nastavenou mapu politik je opět nutné aplikovat na rozhraní směrovače, avšak nyní na rozhraní odchozí.

```
R4(config)#interface Serial 0/0/0
R4(config-int)#service-policy output POLICY
```

Ve druhé doméně disponujeme pouze poloviční dostupnou šířkou pásma. Proto je nutné upravit stávající komunikaci na potřebné limity, abychom zajistili co nejefektivnější přenos. Tuto úpravu má na starosti vstupní směrovač domény B, který je v modelové topologii označen jako R2.

Na vstupním rozhraní směrovače dochází k přeznačení databázové komunikace z DSCP *AF31* na *AF21*, jenž je určena pro transakční data.

```
R4(config)#class-map Data_in
R4(config-cmap)#match dscp af31
R4(config-cmap)#exit
R4(config)#policy-map REMARK
R4(config-pmap)#class Data_in
R4(config-pmap-c)#set dscp af21
R4(config-pmap-c)#exit
R4(config-pmap)#exit
R4(config)#interface Serial0/0/0
R4(config-int)#service-policy input REMARK
```

Nastavení tříd provozu je obdobné jako na směrovači R4, a proto nebude tato konfigurace znovu uváděna a přejdeme rovnou k úpravám mapy politik.

```
R4(config)#policy-map POLICY
R4(config-pmap)#class VoIP
R4(config-pmap-c)#priority percent 15
R4(config-pmap-c)#exit
R4(config-pmap)#class Video
R4(config-pmap-c)#priority percent 45
R4(config-pmap-c)# police 390000 conform-action transmit
R4(config-pmap-c)#exit
R4(config-pmap)#class Data_out
R4(config-pmap-c)# police 260000 conform-action transmit
R4(config-pmap-c)#exit
R4(config-pmap)#class class-default
R4(config-pmap-c)#fair-queue
R4(config-pmap-c)#queue-limit 15
R4(config-pmap-c)#random-detect
```

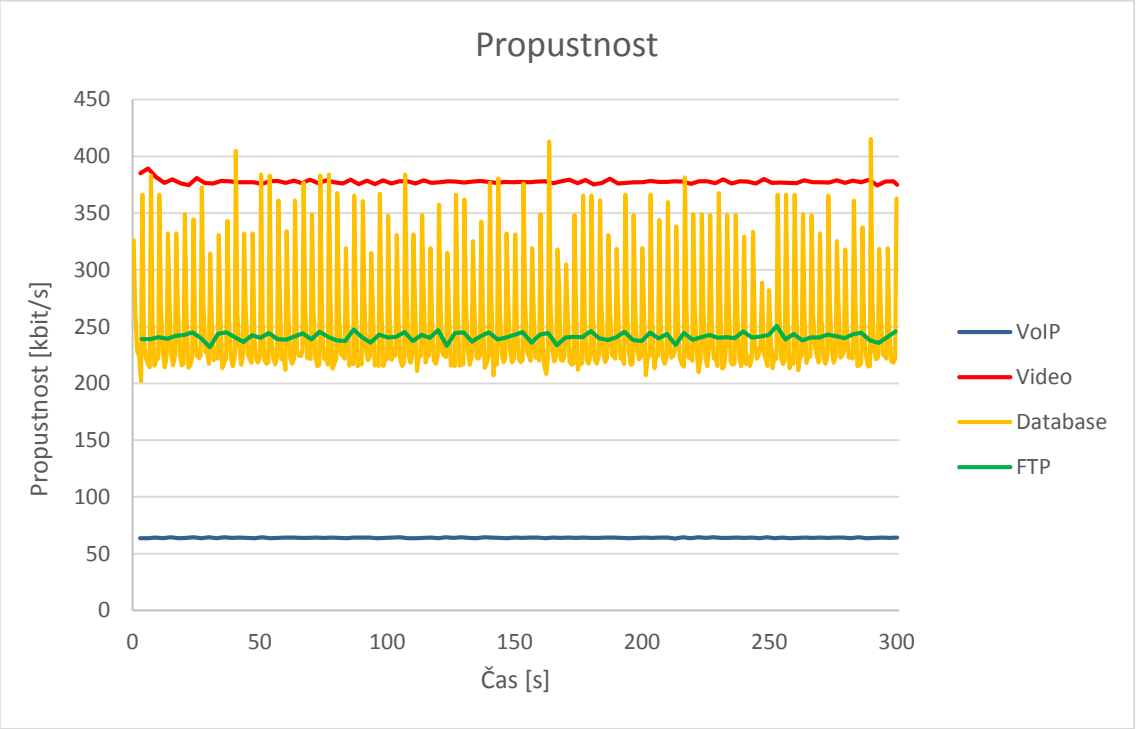
Konfigurace je velmi podobná jako na směrovači R4, pouze jsou upraveny hodnoty. Přibyla nám zde třída Data_out a také zde nastavujeme omezování provozu pomocí příkazu `police`. U videa jsme si vyhradili minimální šířku pásma 45 procent, přičemž když z jakéhokoliv důvodu dojde k překročení přenosové rychlosti 390000 b/s budou pakety odhazovány. To samé platí i pro třídu Data_out, která nám obsluhuje databázový přenos. Zde je hodnota odhazování nastavena na 260000 b/s.

4.5 VÝSLEDKY S VYUŽITÍM QOS

Nyní můžeme opět přejít k měření, grafickému vyjádření výsledků a jejich porovnání. Scénář je stejný jako u aplikace bez využití QoS.

4.5.1 Propustnost

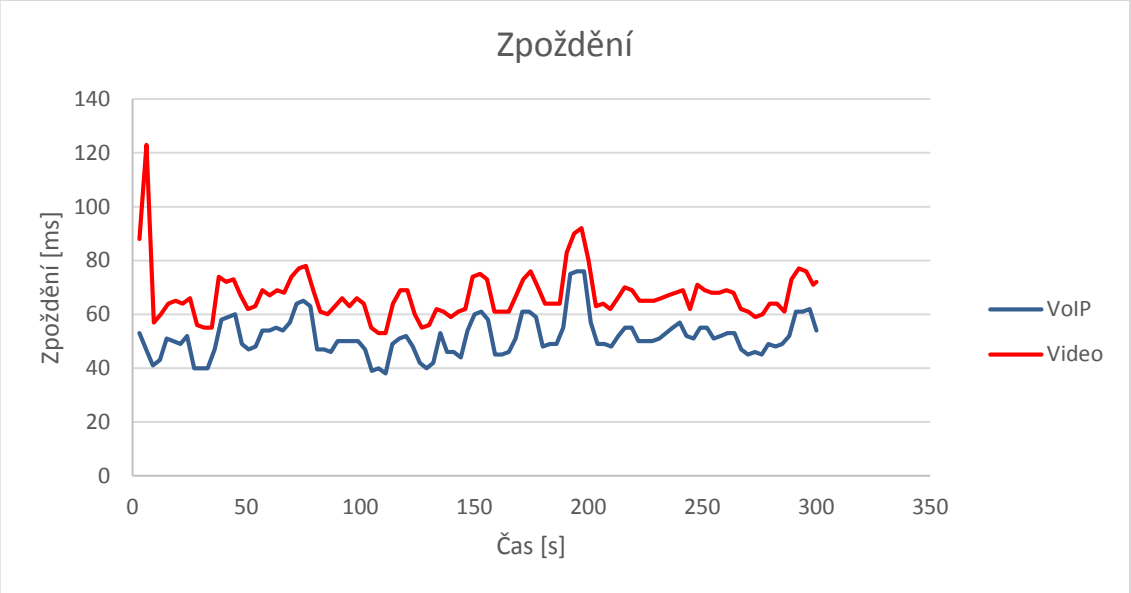
Co se týče propustnosti, zůstaly hodnoty na přibližně stejné úrovni jako bez aplikace QoS. Jediný rozdíl nastává ve video komunikaci, kde stálý datový tok překračoval námi stanovenou hodnotu 390 kbit/s, a proto je snížen na tuto hranici.



Graf 10 Propustnost s využitím QoS

4.5.2 Zpoždění

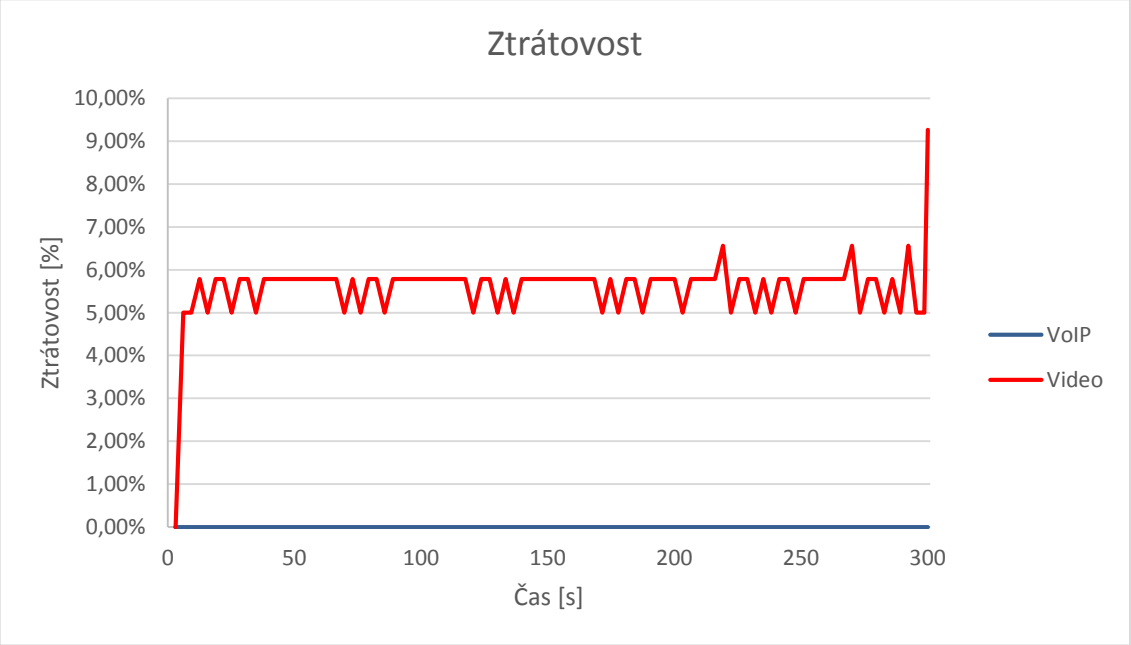
U zpoždění lze pozorovat opravdu znatelné zlepšení. Z původních hodnot, který přesahovaly 1700 ms, se nyní videokomunikace pohybuju v ustálených hodnotách v průměru na 66 ms. To je více než 2000% zlepšení. Zpoždění videa se díky tomu dostává pod hranici 150 ms, která je hraniční pro bezproblémovou video komunikaci. VoIP doznalo také zlepšení, průměrné hodnoty jsou o 2 ms nižší, což však lze považovat za odchylku v měření.



Graf 11 Zpoždění při využití QoS

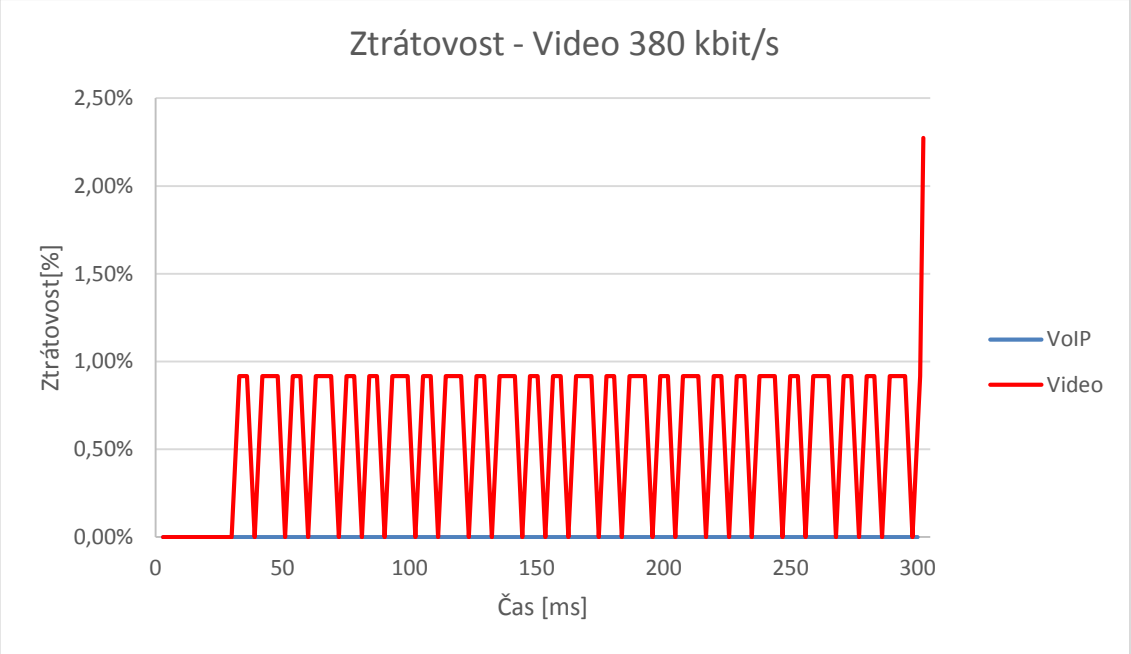
Ztrátovost

Hodnoty ztrátovosti jsou v tomto měření vyšší, než bez využití QoS. Je tomu díky zahazování při překročení hraničních hodnot datového toku na 390 kb/s. Jelikož samotný datový tok má 400 kb/s a dodatečnou režii, bylo zvýšení ztrátovosti očekávané. Bohužel při nastavení vyšší hranice pro omezování provozu jsme již zaznamenali značný nárůst zpoždění. Ztrátovost v tomto testu narostla přibližně o 3,5 %, což je pro zajištění bezproblémové video komunikace nedostatečné.



Graf 12 Ztrátovost při využití QoS

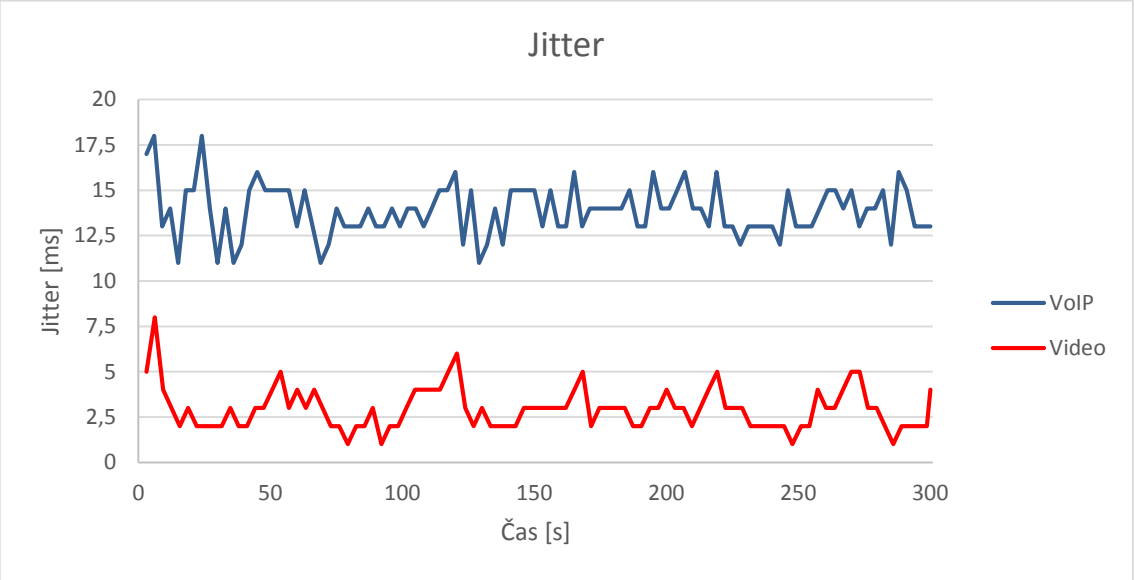
Řešením tohoto problému by se pro nás nacházelo ve snížení kvality videa. Již při snížení datového toku a poměrně zanedbatelných 20 kbit/s, tedy ze 400 na 380 kbit/s se maximální hodnoty ztrátovosti dostávají pod hranici 1 %, která je hraniční pro bezproblémový video přenos. Konečnou fázi opět z našeho měření vynecháváme, jelikož je pravděpodobně spojená s vysokou režií simulačního programu.



Graf 13 Ztrátovost při využití QoS, video 380 kbit/s

4.5.3 Rozptyl zpoždění, jitter

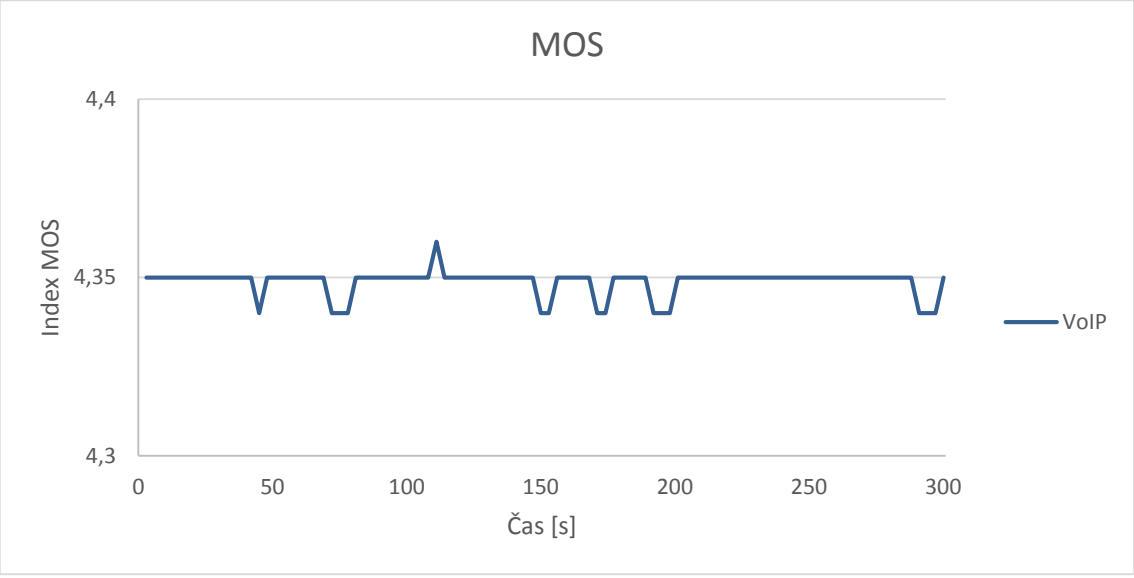
Z následujícího grafu je patrné, že došlo i ke zlepšení hodnot u rozptylu zpoždění a to u obou sledovaných položek. Vyšší rozdíl v tomto směru zaujímá video kdy průměrná se průměrná hodnota snížila z 5 na 2,9 ms.



Graf 14 Jitter při využití QoS

4.5.4 MOS, Meaning Opinion Score

Poslední sledovanou hodnotou je MOS, která určuje kvalitu výsledného hlasového přenosu. Po konfiguraci QoS se hodnota mnohem více ustálila a projevovala pouze drobné odchylky. Hodnota MOS se ustálila na 4,35, což znamená vysokou kvalitu přenosu.



Graf 15 MOS při využití QoS

ZÁVĚR

Cílem bakalářské práce bylo teoretické představení a následná konfigurace mechanismů zajištění kvality služeb (QoS) v rámci firemního prostředí.

Pro splnění cílů této bakalářské práce bylo nutné nejprve vytvořit cílený dotazník zaměřený na zjištění potřebných informací týkajících se využití mechanismů QoS, používanými technickými prostředky a zároveň dispozicemi firem pro využívání nejrůznějších moderních komunikačních prostředků, například videokonferencí či internetové telefonie. Tento dotazník byl zkonzultován s IT odborníky a po provedení revize otázek odeslán do skupiny firem. Na základě odpovědí bylo patrné, že zhruba polovina oslovených firem využívá mechanismy QoS: Bohužel byl dotazník vyplňován anonymně, a tudíž nelze určit, zda jsou mechanismy QoS využívány ve větším měřítku v rámci IT firem, či firem zaměřených na pojišťovnictví nebo ve zdravotnictví. Zvolená cílová skupina tohoto dotazníku byla volena tak, aby pokryla co možná největší škálu firem, vyskytujících se v Pardubickém kraji.

První, teoretická část této bakalářské práce byla zaměřena na obecné představení technologií QoS, zejména pak na základní principy tohoto mechanismu. Mezi primární aplikace QoS jsou zařazeny Best Effort, IntServ či nejmodernější DiffServ. Všechny tyto metodiky přístupu byly v této části podrobně popsány a zároveň zde byla uvedena i nadstavba v podobě doplňujících informací pro pochopení jednotlivých principů.

V souvislosti s modelem integrovaných služeb byl představen také protokol RSVP, jenž slouží pro rezervaci cesty pro prioritní komunikaci. Zároveň zde byly zmíněny i informace o správě front a také algoritmus token bucket, jenž jsou důležitou součástí popisu diferencovaných služeb.

Teoretická část byla uzavřena využitím QoS nad MPLS, což je v dnešní době využíváno širokým spektrem firem. Tato část pojednávala o upraveném modelu DiffServ, avšak po konzultaci s vedoucím bakalářské práce, bylo rozhodnuto, že tato kombinace nebude v této bakalářské práci dále rozvíjena.

V druhé části bakalářské práce byl nejprve stručně představen výsledek přijatých dotazníků od oslovených firem a zároveň popsána topologie, na níž byla následně provedena konfigurace QoS.

Konfigurace byla vysvětlena v rámci této praktické části bakalářské práce.

V rámci praktické části byla provedena dvě měření s totožnými vstupními toky pro ověření funkčnosti QoS. Datové toky byly generovány pomocí profesionálního analytického programu, který zároveň umožňoval přehlednou formu záznamu výstupů. Na základě získaných výsledků byly následně zpracovány přehledné grafické výstupy, které věrně vystihují rozdíly před a po aplikaci mechanismů pro zajištění kvality služeb. Jednotlivými měřeními byla ověřena funkčnost a význam QoS v datových sítích. Rozdíly v kvalitě služeb byly z grafů a průměrných hodnot zřejmé.

Na tomto místě je nutné podotknout, že konfigurace QoS mohla být v laboratorním prostředí relativně snadno vyladěna. Pokud by se jednalo o aplikaci QoS v reálném firemním prostředí, předcházelo by konfiguraci velké množství měření a také komplexní analýza síťového provozu. Bylo by nutné zjistit objem odeslaných dat a nároky na síťové prvky při běžném i nárazovém zatížení sítě. Na základě získaných dat by bylo teprve možné přemýšlet o způsobu konfigurace síťových prvků.

LITERATURA

[1] SZIGETI, Tim a Christina HATTINGH. *End-to-end QoS network design*. Indianapolis: Cisco Press, 2005, 734 s. ISBN 15-870-5176-1.

[2] WALLACE, Kevin. *Implementing Cisco unified communications voice over IP and QoS (Cvoice) foundation learning guide*. 4th ed. Indianapolis, IN: Cisco Press, c2011, xxxii, 696 p. ISBN 15-872-0419-3.

[3] FOWLER, Thomas B. Convergence in the Information Technology and Telecommunications World: Separating Reality From Hype. *Convergence in the Information Technology and Telecommunications World: Separating Reality From Hype*. 2003.

[4] ODOM, Wendell a Michael J CAVANAUGH. *Cisco QOS exam certification guide: CCVP self-study*. 2nd ed. Indianapolis: Cisco Press, c2005, xxxiv, 730 s. ISBN 15-872-0124-0.

[5] PARK, Kun I. *QOS in packet networks*. New York: Springer Science Business Media, c2005, xii, 243 p. ISBN 03-872-3389-X.

[6] ODOM, Wendell. *CCIE routing and switching certification guide*. 4th ed. Indianapolis: Cisco Press, c2010, xlv, 1016 s. ISBN 978-1-58705-980-3.

[7] BRADEN, Bob, David CLARK a SHENKER. RFC 1633. *Integrated Services in the Internet Architecture: an Overview*. IETF, 1994. Dostupné z: http://www.ietf.org/rfc/rfc1633.txt

[8] BRADEN, Bob et al. RFC 2205. *Resource ReSerVation Protocol (RSVP)*. IETF, 1997. Dostupné z: http://www.ietf.org/rfc/rfc2205

[9] DURAND, Benoit. *Administering Cisco QoS for IP networks*. Editor Michael E Flannagan. Rockland, Mass.: Syngress Publishing, Inc., c2001, xxiv, 536p. ISBN 1928994210.

[10] BLAKE, Steven et al. RFC 2475. *An Architecture for Differentiated Services*. IETF, 1998. Dostupné z: http://www.ietf.org/rfc/rfc2475

[11] DEMICHELIS a CHIMENTO. RFC 3393. *IP Packet Delay Variation Metric for IP Performance Metrics*. IETF, 2002. Dostupné z: http://www.ietf.org/rfc/rfc3393

[12] NICHOLS et al. RFC 2474. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. IETF, 1998. Dostupné z: http://www.ietf.org/rfc/rfc2474

[13] ROSEN, Eric C., VISWANATHAN a CALLON. RFC 3031. *Multiprotocol Label Switching Architecture*. IETF, 2001. Dostupné z: http://www.ietf.org/rfc/rfc3031

[14] IXIA. *IxChariot* [software]. 2014 [cit. 2014-04-20]. Dostupný z: http://www.ixiacom.com/products/ixchariot/

[15] WIRESHARK FOUNDATION. *Wireshark* [software]. 2014 [cit. 2014-04-20]. Dostupný z: http://www.wireshark.org/ Požadavky na systém: 32bitový x86 nebo 64bitový AMD64/x86-64 procesor, operační systém Windows XP Home, XP Pro, XP Tablet PC, XP Media Center, Server 2003, Vista, Home Server, Server 2008, Server 2008 R2, Home Server 2011, 7, Server 2012, volné místo na disku 75 MB, operační paměť 128 MB

[16] ITU-T. *G.711*. 1988. Dostupné z: https://www.itu.int/rec/T-REC-G.711-198811-I/en

[17] ISO/IEC 13818-2. *Generic coding of moving pictures and associated audio information*. International Organization for Standardization. Dostupné z: http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=61152

[18] ITU-T P.800.1. *Mean Opinion Score (MOS) terminology*. ITU-T, 2006. Dostupné z: http://www.itu.int/rec/T-REC-P.800.1-200607-I/en

PŘÍLOHA A – DOTAZNÍK

Jaké prostředky využíváte pro firemní komunikaci?

- ☐ E-mail
- ☐ Telefony, mobily
- ☐ VoIP telefonie
- ☐ Skype či jiný Instant Messenger
- ☐ Vlastní software pro komunikaci
- ☐ Jiné

Jaké síťové služby jsou pro vaši firmu důležité?

- ☐ VoIP
- ☐ Videokomunikace, videokonference
- ☐ Připojení k databázi
- ☐ Připojení k webu
- ☐ Sdílení dat
- ☐ E-mail
- ☐ Vzdálené ovládání zařízení
- ☐ Jiné

Na jakých prvcích je postavena firemní síť?

- ☐ Routery
- ☐ Switche
- ☐ Access Point (AP)
- ☐ WiFi routery, WiFi AP

☐ Hub

☐ Jiné

Využíváte ve firemní síti zajišťování kvality služeb - QoS?

○ Ano

○ Ne

Disponuje Vaše společnost vybavení pro videokonference?

○ Ano

○ Ne

PŘÍLOHA B – NASTAVENÍ ADRESACE

Zařízení	Rozhraní	IP adresa	Maska podsítě	Výchozí brána
PC1	ehternet	192.168.1.2	255.255.255.0	192.168.1.1
R1	fa0/0	192.168.1.1	255.255.255.0	---
	se0/0/0	10.0.0.1	255.255.255.252	---
R2	se0/0/0	10.0.0.2	255.255.255.252	---
	se0/0/1	10.0.1.1	255.255.255.252	---
R3	se0/0/0	10.0.2.1	255.255.255.252	---
	se0/0/1	10.0.1.2	255.255.255.252	---
R4	se0/0/0	10.0.2.2	255.255.255.252	---
	fa0/0	192.168.2.1	255.255.255.0	---
PC2	ehternet	192.168.2.2	255.255.255.0	192.168.2.1