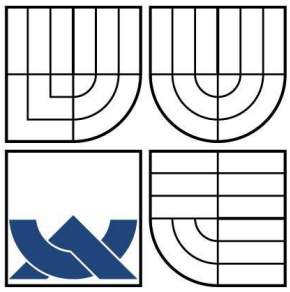
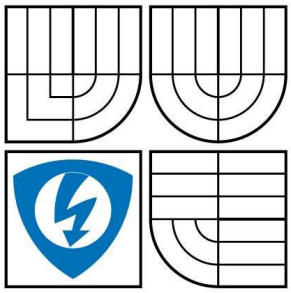


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKACNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

TECHNOLOGIE PRO ZAJIŠTĚNÍ KVALITY SLUŽEB V IP SÍTÍCH A JEJICH VZÁJEMNÁ SPOLUPRÁCE

TECHNOLOGIES FOR QUALITY OF SERVICE ASSURANCE IN IP NETWORKS AND THEIR MUTUAL COOPERATION

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — VÁCLAV OUJEZSKÝ
AUTHOR

VEDOUCÍ PRÁCE — ING. JIŘÍ HOŠEK
SUPERVISOR

BRNO 2009

Abstrakt

Tato bakalářská práce se zabývá souhrnným popisem jednotlivých způsobů a technologií k zajištění kvality služeb v IP sítích. Je zejména orientována na architektury IntServ a DiffServ a jejich možné způsoby vzájemné spolupráce. V praktické části je proveden test uvedených architektur a jejich vlastností v síťovém emulačním programu GNS3.

Abstract

This barchelor thesis deals with complex description of technologies and particular ways providing quality services in IP networks. It is especially oriented on architecture of IntServ and DiffServ and their possible ways of mutual cooperation. In practical part, the testing of architectures mentioned is made and their characteristics in network emulator program GNS3.

Klíčová slova

IP, QoS, IntServ, DiffServ, RSVP, GNS3, Cisco

Key word

IP, QoS, IntServ, DiffServ, RSVP, GNS3, Cisco

Bibliografická citace mé práce:

OUJEZSKÝ, V. Technologie pro zajištění kvality služeb v IP sítích a jejich vzájemná spolupráce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 68 s. Vedoucí bakalářské práce Ing. Jiří Hošek.

Prohlášení

Prohlašuji, že svoji bakalářskou práci na téma „Technologie pro zajištění kvality služeb v IP sítích a jejich vzájemná spolupráce“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

V Brně dne .... podpis autora

Děkuji vedoucímu práce, panu Ing. Hoškovi za jeho trpělivost a podporu. Dále také své rodině za její tolerantní přístup.

V Brně dne .... podpis autora

OBSAH

ÚVOD

V dnešní době je životně důležité a to zejména pro obchodní zákazníky, aby se veškerý síťový provoz dostal tam, kam má a i tehdy, kdy má. S neustálou poptávkou po dostupné šířce pásma a s příchodem nových technologií a zařízení musí být nějakým způsobem zaručen kompromis mezi cenou, rychlostí a potřebami jednotlivých technologií využívajících připojení k internetu. V praxi to znamená odeslat zaručeným způsobem data, která jsou důležitější. Ve firmě, která provozuje telefonní centrum bude jistě důležitější zajistit bezproblémový provoz VoIP aplikací. Nižší prioritu zde bude mít například přenos běžných uživatelských dat.

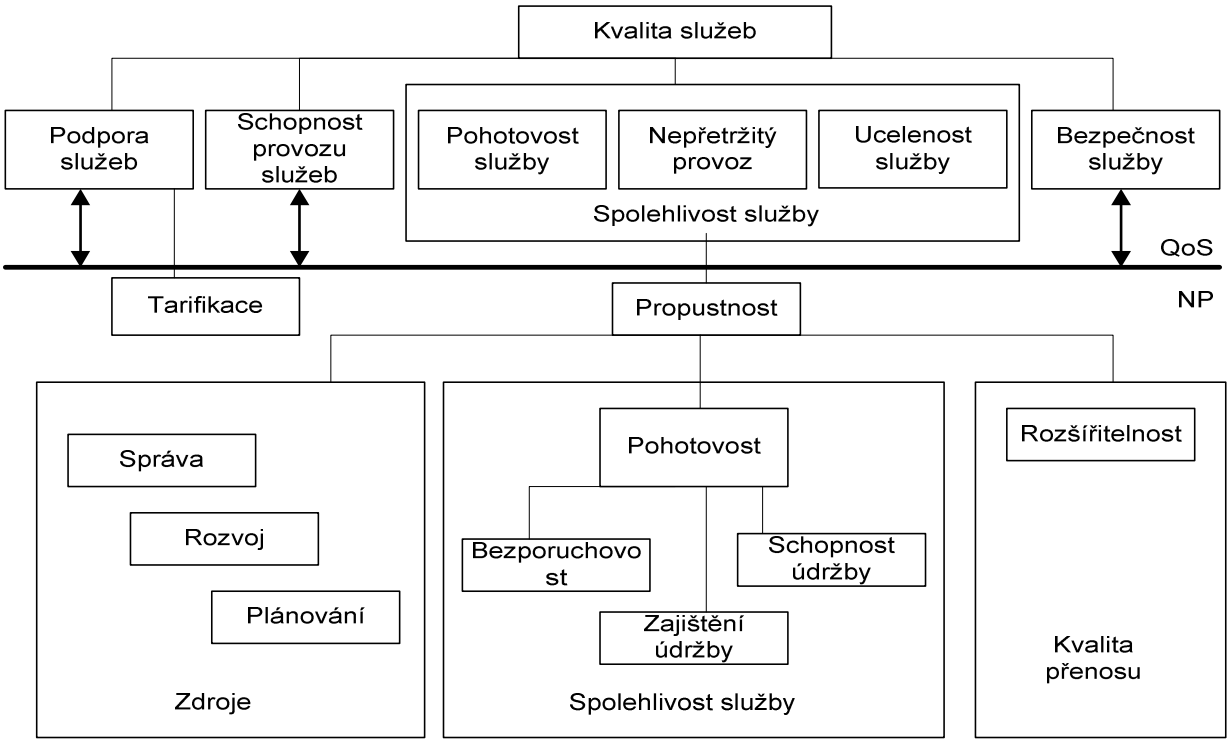
To vše je možné zajistit implementací technologie zásad nazvané QoS. Při zavedení těchto zásad jsou přiřazeny jednotlivým typům síťového provozu různé priority zpracování a různé způsoby zpracování. V následujících kapitolách budou popsány mechanizmy pro zajištění QoS a dále definovány jejich modely a možnosti vzájemné spolupráce. Mechanizmy pro zajištění kvality služeb v IP sítích, které jsou uvedené v této práci, jsou základním kamenem pro QoS. Do QoS se dále řadí i nástroje k zajištění bezpečnosti v IP sítích.

1 DEFINICE KVALITY SLUŽEB Z HLEDISKA PŘENOSU DAT A JEHO ZÁKLADNÍ PRINCIPY

V IP sítích je implementace kvality služeb obtížnější než v sítích ATM či Frame Relay. A to hned z několika důvodů. Dostupná šířka pásma je zde konečná a s požadavky se nemění. Jakýmkoliv způsobem se bude aplikovat kvalita služeb, každý bit v přenosovém pásmu půjde na vrub ostatních. Bez nástrojů autentizace uživatelů a záznamů pro účely zpoplatnění služeb a kontroly, nemohou být mechanizmy kvality služeb efektivní.

Doporučení ITU-T E800 [4] všeobecně rozlišuje kvalitu služeb na dva základní pojmy viz. Obrázek 1.1

- Kvalita služby QoS – zajímá se o popis vlastností sítě z pohledu uživatele. Ke kvalitě služby slouží řada aspektů vztažených k výkonnosti služby a bezpečnosti.
- Výkonnost sítě NP – zajímá se o popis vlastností sítě z pohledu poskytovatele. A to z důvodu plánování sítě a vývoje. Neboli jde o technickou stránku QoS.



Obrázek 1.1. Koncepce kvality služeb podle ITU-T E.800

1.1 ZÁKLADNÍ PARAMETRY DEFINUJÍCÍ KVALITU SLUŽEB QOS

Kvalitu služeb, nebo i kvalitu datového přenosu jako takového, definuje sada parametrů popisující komunikační relaci. Pokud má dojít k implementaci QoS, musí se vyjádřit požadavky konkrétními metrikami. V paketových sítích je základním požadavkem doba doručení paketů. Proto jsou metriky pro IP sítě převážně vztaženy ke službám či aplikacím, které jsou označovány jako REAL-TIME, neboli aplikace v reálném čase.

Do základních metrik „REAL-TIME“ patří [7]:

- **Komunikační zpoždění**

Komunikační zpoždění reprezentuje celkový čas potřebný k přenesení paketů ze zdroje do cíle. Rozlišuje se zde několik typů zpoždění:

- ✓ procesní zpoždění - obecně zpoždění na zařízeních v síti ze vstupu na výstup
- ✓ paketizační (linkové) zpoždění - zpoždění čekáním paketů ve frontách
- ✓ kompresní zpoždění nebo i zpoždění kódováním - příprava paketů na přenos
- ✓ rámcové zpoždění – zpracování řeči do rámců.

Při zpoždění cca 150ms je již doba prodlevy postřehnutelná. Vyšší odezvy zpoždění již silně ovlivňují všechny aspekty spojení.

- **Jitter**

Propustnost a zatížení sítě se v čase mění, proto nemůžeme přesně určit hodnotu zpoždění. Tento jev se nazývá „jitter“. Zdrojové zařízení vysílá tzv. datagramy a to v pravidelných časových intervalech. A právě hodnota jitteru zachycuje velikost změny času příchozích datagramů v cílovém zařízení, které také pracuje v časových intervalech. Dochází zde k rozkolísání časových intervalů, nebo nestabilitě zdroje těchto intervalů. V ideálním případě by byla velikost jitteru nulová. Pokud dojde některý z datagramů příliš pozdě, je vyřazen a nahrazen následujícím datagramem.

K potlačení časové variability a ztrátě datagramů může být využit „Jitter Buffer“, který je vložen mezi síťovou vrstvu a VoIP aplikaci. „Jitter Buffer“ uschová datagramy, které přišly v nesprávném pořadí. Poté datagramy zpracuje a pošle je aplikacím již ve správném pořadí.

- **Šířka pásma**

Měřítkem je objem dat, které je schopna přenosová cesta přenést za určitý čas v bitech za sekundu. To platí pro digitální přenos. V analogovém přenosu se měří analogová šířka pásma v Hz.

- **Ztráta paketů**

Ztráta paketů vzniká z důvodu zahlcení, přetížení kapacity prvků sítě. Ty nestačí odbavovat příchozí pakety a jejich fronty přetečou. Důsledkem je zahození paketů.
Spolehlivost je definována v ITU-T.350 jako IPER a IPLR.

- **Pravděpodobnost blokování**

Jedná se především o metriku danou pro spojově orientované paketové sítě. Pravděpodobnost blokování je zde definována základními matematickými modely jakými jsou Erlang B (systém se ztrátami) a Erlang C (systém beze ztrát). Jedná se o vyjádření hodnocení QoS v trunkových systémech se sdílením kanálů.

- **Subjektivní a objektivní testování**

Vnímání kvality služby ze strany uživatele se vyjadřuje v hodnotách MOS. Využívá subjektivní metody, objektivní testování a výpočetní metody tzv. Model E. Podle příslušného ITU-T (ITU-T P.862 , ITU-T G.107) [4]

- **Kvantovací šum**

Kvantovací šum se váže na vzorkovací a kvantovací procesy ve zdrojovém kodování. Rozdíl kvantovací chyby v rekonstruovaném analogovém signálu zavádí kvantovací šum, který snižuje danou kvalitu služby.

2 ÚROVNĚ SLUŽEB QOS V IP SÍTÍCH

Proto, aby bylo možné definovat jednotlivé služby QoS v IP a jejich metriky, musí být určeno, jaká aplikace a kdo těchto služeb bude využívat. Jedním z hlavních faktorů na definici QoS jsou požadavky síťových aplikací

Aplikace jsou podle požadavků rozděleny na [1]. :

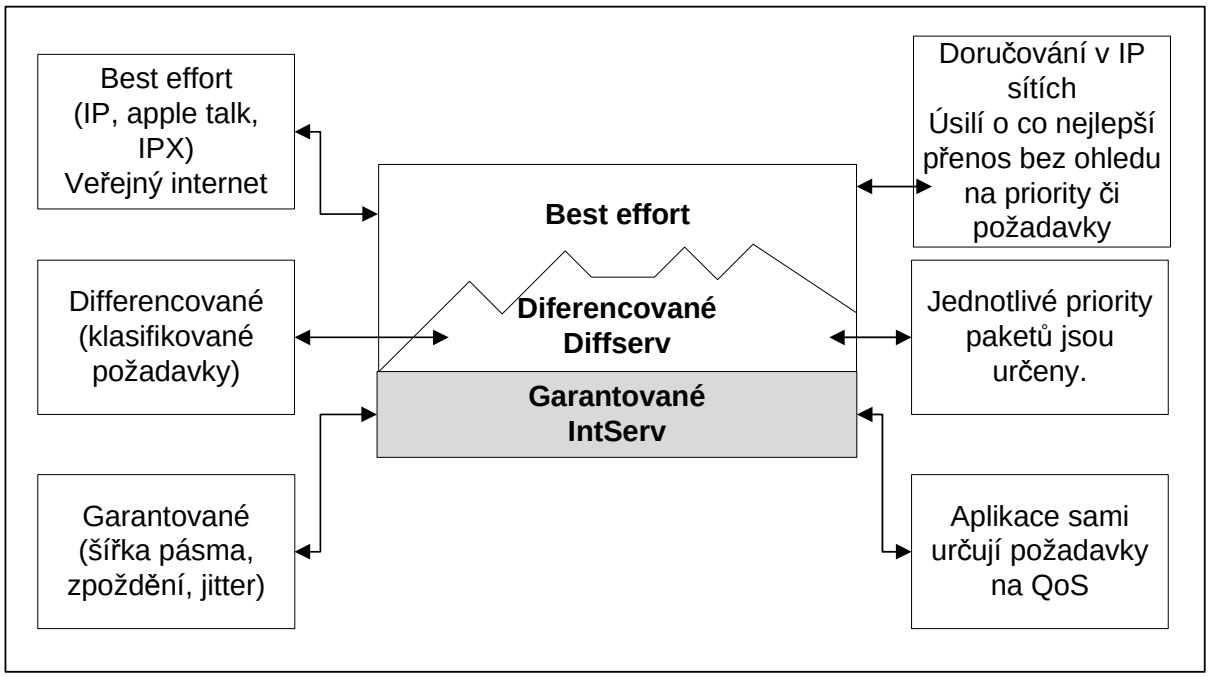
- *Přenos souborů* – náročné na pásmo, ne však na zpoždění.
- *Bussines aplikace* – požadavek na dostupnost a minimální zpoždění.
- *Multimediální aplikace* - audio video streaming, nemají vysoké nároky na jitter.
- *Webové aplikace* – HTTP protokol využívající TCP, tedy spolehlivý přenos. Zde záleží, jaké webové aplikace budou využity. Nejde jednoznačně určit požadavky.
- *Groupware aplikace* – např. Exchange. Většinou obdoba souborového přenosu, pokud nebereme v potaz real-time přenos videa.
- *Aplikace v reálném čase* – Videokonference, VoIP – náchylné na časovou invariabilitu, jitter, dostupnou šířku pásma.

Od QoS v IP síti je očekáváno především zlepšení kvality služeb a předvídatelnosti sítě. To může být zajištěno především těmito vlastnostmi:

- Vyhrazením šířky pásma
- Snížením výskytu ztrát
- Řízením proti zahlcení sítě
- Nastavením priorit
- Zlepšením provozu sítě

Dále je prováděno rozdělení QoS podle typu poskytnuté služby [2], jak je zobrazeno viz. Obrázek 2.1

- Služby Best effort (s maximálním úsilím o přenos)
- Integrované služby
- Garantované služby



Obrázek 2.1. QoS podle typu poskytované služby [1]

Služba typu „Best effort“ je provozována většinou v dnešním veřejném internetu. Tento typ služby je známý také pod pojmem „lack QoS“ neboli „bez podpory QoS“. Jedná se o základní spojení, bez garancí služeb. Nejlépe jej charakterizuje plánování front FIFO .
Diferencované služby využívají nejvíce modelu služeb DiffServ . Zde dochází ke klasifikaci jednotlivých síťových přenosů a používá se zde nástrojů QoS, jako je například WFQ, WRED.

Garantované služby zvané také „hard QoS“ tzv. „absolutně“ rezervují požadavky určitého síťového provozu po celou dobu jeho trvání. Zde se využívá nástrojů QoS, jako je RSVP, řízení přístupu a služeb typu IntServ.

2.1 QOS METRIKY V IP SÍTÍCH

Pro úspěšnou implementaci QoS v IP sítích podle předchozích definicí jsou určeny metriky specielně pro tyto sítě. Definované jsou v doporučení ITU-T (I.380,Y.1540, Y.1541) Těmito metrikami jsou :

- Zpoždění přenosu paketů IPTD - IP packet transfer delay
- Poměr chybovosti paketů IPER - IP packet error ratio

- Poměr strátovosti paketů IPLR - IP packet loss ratio
- Propustnost paketů IPPT - IP Packet Troughput
- Poměr zaměněných paketů SIPPR - Spurious IP packet rate
- Nedostupnost IP služeb v procentech PIU - Percent IP Service Unavailability
- Nedostupnost IP služeb v procentech PIA - Percent IP Service Availability

ITU-T I.380 shrnuje kritéria do tzv. výkonnostní matice viz. Tabulka 2.1

Tabulka 2.1. : Výkonnostní matice dle ITU-T 350 pro IP sítě.

Fáze / Kritérium	Rychlost	Přesnost	Spolehlivost
Spojení	Přístupové zpoždění	Poměr nesprávného přístupu	Poměr nezdařeného přístupu
Přenos informace	Přenosové zpoždění / výkon	Poměr chyb	Poměr ztráty dat
Ukončení spojení	Zpoždění ukončení spojení	Poměr nevydařeného Spojení	
	Dostupnost služby	nebo její nedostupnost	

A dále je v ITU-T [4] Y.1541 definováno šest tříd QoS průměrných horních hodnot výkonnostních parametrů, které je nutné dodržet pro požadovanou kvalitu služby v IP sítích viz. Tabulka 2.2 . Písmeno N v tabulce označuje nepovinný parametr.

Tabulka 2.2.: Třídy QoS podle ITU-T.Y.1541 pro IP sítě

Výkonnostní parametr	Třídy QoS					
	Třída 1	Třída 2	Třída 3	Třída 4	Třída 5	Třída 6
IPTD	100ms	400ms	100ms	400ms	1s	N
IPDV	50ms	50ms	N	N	N	N
IPLR	$1 \cdot 10^{-3}$					N
IPER	$1 \cdot 10^{-4}$					N

3 MODELY PRO ZAJIŠTĚNÍ KVALITY SLUŽEB V IP SÍTÍCH A JEJICH NÁSTROJE

V IP sítích existují různé typy úrovní QoS. Z toho plyne, že existují i jejich modely a nástroje, jakými je dosaženo jednotlivých úrovní [3].

Definované modely pracujících na síťové vrstvě IP sítí jsou následující:

- Best Effort
- Architektura IntServ – Integrované služby: Metoda rezervace síťových prostředků.
- Architektura DiffServ – Diferencované služby: Metoda priority paketů.
- MPLS – přepínání paketů podle návěstí
- SBM – správa přenosové kapacity v podsítích

Detailněji budou dále rozebrány architektura IntServ, architektura DiffServ a jejich vzájemná spolupráce.

3.1 BEST EFFORT

V sítích typu Best Effort aplikace zasílají data, bez jakýchkoliv politik a síťová zařízení se snaží o jejich přenos s co největším úsilím. Zajisté se nejedná o QoS jako takové. Služeb typu Best Effort využívají například FTP, HTTP nebo P2P sítě. V základě byl na tomto principu založen veškerý provoz v IP sítích.

V současných veřejných sítích je podle průzkumů tato služba využívána z 60 % celkového síťového provozu. S postupujícím časem bude nutné nahrazovat „Best-effort“ sítě za sítě podporující QoS. Z důvodu proti zahlcení sítě, zvýšení kvality služeb a účtování.

3.2 INTSERV – INTEGROVANÉ SLUŽBY

Tento model byl definován v RFC1633 [4] v roce 1994 a je prvním z modelů, který měl zajistit v IP sítích požadavky na QoS. Pracuje zejména ve 3. vrstvě modelu OSI a je tedy použitelný zejména na páteřních prvcích sítě. V případě IntServ, oznamuje požadavky na přenos dat a požadavků QoS aplikace síti. K zajištění IntServ se mohou použít různé protokoly. V současnosti jsou zpracovávány protokoly RSVP, COPS od firmy CISCO [1] a dále například YESSIR [8], který nahrazuje protokol RSVP.

Integrované služby rozdělují aplikace do kategorií:[1]

- *Elastické aplikace* - bez požadavku na doručování, zpoždění, kapacitu spoje , sem patří například aplikace využívající SMTP, HTTP protokolu.
- *Real Time Tolerant aplikace* (RTT) – s požadavky na snížení maximálního zpoždění.
- *Real Time Intolerant aplikace* (RTI) – požadavek na minimální zpoždění a jitter, Sem patří například videokonferenční přenosy.

IntServ referenční základní model viz. Obrázek 3.1 obsahuje :[13]

- Kontrola a řízení přístupu (Admision Control)
- Rezervační protokol
- Klasifikátor (Packet Clasifier)
- Plánovač paketů (Packet Scheduler)

3.3 ŘÍZENÍ PŘÍSTUPU (ADMISSION CONTROL)

Aplikace oznámí síti své požadavky a síť své prostředky, jako je šířka pásma a vyrovnávací paměť, poskytne nebo zamítne. Bez takového řízení přístupu by model IntServ byl pouhou službou typu „Best-Effort“. Pokud dojde k zamítnutí žádosti, aplikace rozhodne, zda požádá o méně náročnější zajištění QoS.

3.3.1 REZERVAČNÍ PROTOKOLY

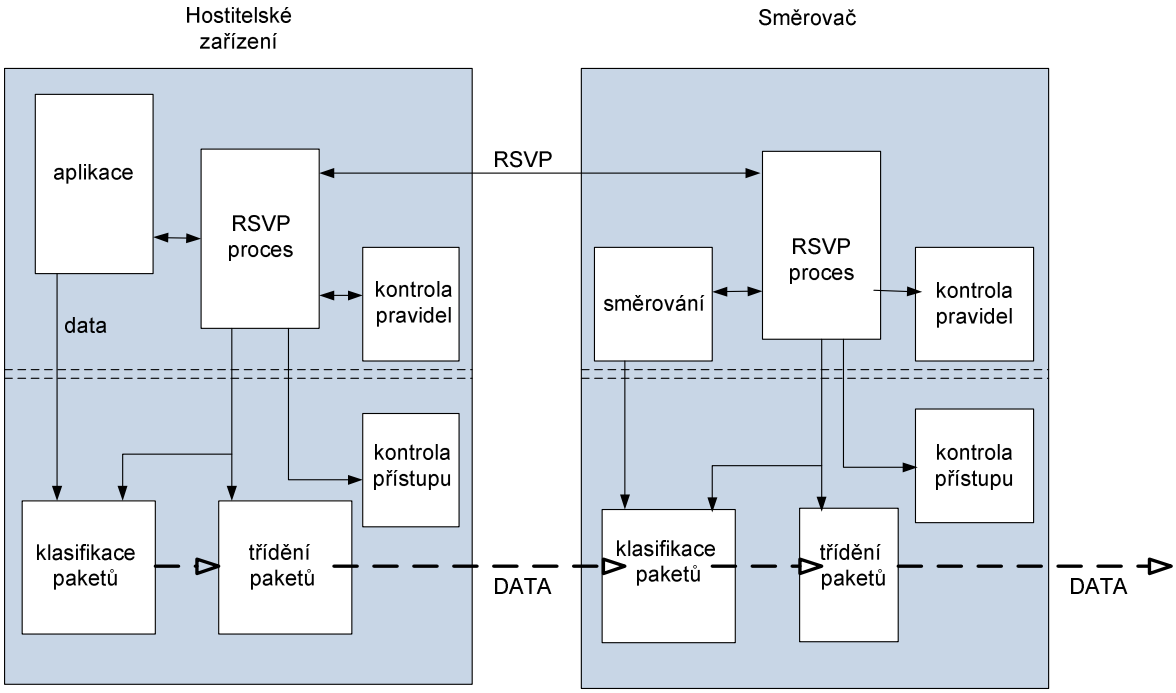
Pokud je požadavek přijat, síť musí informovat všechny síťové komponenty, pře které bude sestaven přenos. K tomu slouží rezervační protokoly. Nejznámějším rezervačním protokolem je RSVP. Rezervovaná spojení jsou mnohem složitější oproti zavádění priority šířky pásma. Rezervační schémata se musejí dostat ke všem směrovačům na cestě a před zahájením rezervací musí být i definována samotná cesta. Navíc se celá situace komplikuje problémem s měnícími se podmínkami sítě v reálném čase.

3.3.2 KLASIFIKÁTOR (PACKET CLASIFIER)

Třídí pakety jak v hostitelích tak i ve směrovačích do jednotlivých úrovní dohodnutých služeb. Ke každému paketu jsou přidány hodnoty jako je číslo portu, cílová a zdrojová IP adresa. Podle toho je každý paket „namapován“ do určité třídy služeb.

3.3.3 PLÁNOVAČ PAKETŮ (PACKET SCHEDULER)

Řídí odesílání paketů použitím metod front, časovačů a dalších mechanizmů, které odpovídají jednotlivým třídám služeb, do kterých klasifikátor zařadil přicházející pakety. Plánovač paketů musí být zařazen tam, kde jsou pakety řazeny do front.



Obrázek 3.1.: RSVP ve směrovačích a na hostitelských zařízeních dle ITU-T [4].

3.4 RSVP PROTOKOL A VYUŽITÍ V INTSERV

Tato problematika je definována v RFC2205, RFC2210, RFC2211, RFC2212. [4] Protokol RSVP rezervuje definované množství prostředků šířky pásma po celé cestě spojující zdrojové a cílové zařízení. Jedná se o „unicast“ nebo „multicast“ datový přenos. RSVP protokol sám o sobě není směrovací protokol. Jako takový byl sestaven pro spolupráci se směrovacími protokoly.

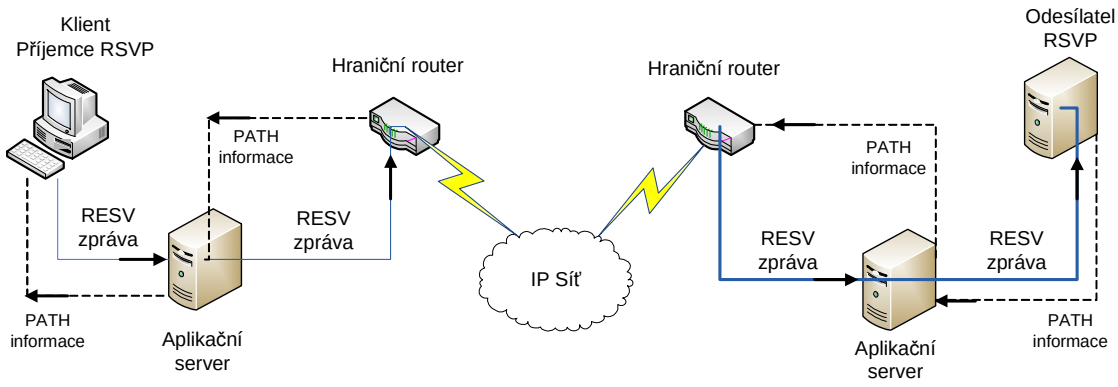
3.5 RSVP ZPRÁVY

Protokol RSVP definuje tyto základní typy zpráv:

- PATH , RESV, PathErr, ResvErr, PathTear, ResvTear, ResvConf.

Nejvýznamnější jsou zprávy PATH a RESV. Spojení a komunikace probíhá tak, že odesílatel zašle po síti zprávu PATH se seznamem zařízení po cestě. Po přijetí zprávy PATH. odešle příjemce zpět odesílateli RSVP po stejné cestě zprávu s požadavkem RESV, s typem požadované rezervace viz. Obrázek 3.2.

Jakmile se dohodnou všechna mezilehlá zařízení na úrovni QoS a nebyla přijata zpráva RESV Error, pošle vysílací hostitel zprávu RESV Confirmation do všech mezilehlých uzlů, které si ji vyžadují a začne komunikační relace. Po ukončení nastoupí explicitní relace a všechny prostředky se uvolní. RSVP je protokol se slabým stavem „soft-state“,, musí tedy informace o rezervacích periodicky obnovovat. Stav rezervace se zaznamenává do mezipaměti v každém síťovém přechodu. Pokud nepřicházejí obnovovací zprávy typu TEAR, vyprší platnost rezervací, nebo na konci přenosu pošle vysílající strana zprávu PATH TEAR a přijímající strana odešle zprávu RESV TEAR a všechny rezervované prostředky se zruší.



Obrázek 3.2.: RSVP rezervace

3.6 RSVP OBJEKTY

V rámci RSVP spojení existují parametry pro ustanovení požadovaných QoS parametrů (třídy objektů), které umožní odesílateli a příjemci RSVP zpráv dohodnout na kvalitě přenosu, typu požadované rezervace. K tomu účelu jsou v RSVP definované jednotlivé třídy objektů [4] :

TSPEC – specifikace požadavků dosažitelné pro datový tok

SENDER_TSPEC – specifikace průměrné a špičkové přenosové rychlosti

RECEIVER_TSPEC – podobně jako SENDER_TSPEC

ERROR_SPEC – chyba specifikace
FLOWSPEC - definuje třídu služby, rezervační typy a specifikaci provozu
FILTER_SPEC – filtr paketů QoS
ADSPEC - informace uzlů, zda mohou poskytnout požadované QoS
SESSION - hodnota o cílové adrese a cestě datového spojení
RSVP_HOP – údaj o síťových uzleh v cestě QoS
STYLE – styl rezervace
SENDER_TEMPLATE – identifikace odesílatele
POLICY_DATA – data předaná ke kontrole modulu „POLICY“
INTEGRITY – verifikace a autentifikace (MD5)
SCOPE – předcházení smyčkám
RESV_CONFIRM – zápis adresy, kam se mají zaslat rezervační potvrzení
TIME_VALUES – časová hodnota obnovování RESV a PATH zpráv

Pokud příjemce obdrží PATH zprávu, rozhodne o přijetí či zamítnutí rezervace. Při přijmutí zprávy vyšle zprávu RESV , která může obsahovat následující objekty:
RSVP_HEADER, RSVP_HOP, FLOWSPEC, FILTER_SPEC, INTEGRITY, SESSION, SCOPE, POLICY, TIME_VALUE, RESV_CONFIRM.

RESV zpráva – v této zprávě jsou uvedeny rezervační typy, které jsou důležité hlavně pro multicastový režim. Následující rezervační typy (žádosti) jsou uvedeny v položce „FlowSpec“:

- *Distinct Reservation* – rezervace šířky pásma zvlášť pro každého odesílajícího hostitele. V multicast vysílání jsou jednotlivá pásma oddělená (Fixed Filter Style).
- *Shared Reservation* – rezervace jedné šířky pásma pro několik odesílajících hostitelů se stejnou skupinovou adresou.
- *Wildcard Filter Type* – přijímající hostitel požaduje rezervaci přenosové kapacity pro všechny zúčastněné odesílající hostitele v daném multicastovém sezení.
- *Shared Explicit Reservation* – přijímací hostitel určuje pevný počet vysílajících hostitelů, jinak jako Wildcard Filter Type.

PATH zpráva - zpráva odesílatele, který chce vytvořit QoS rezervaci obsahuje tyto objekty:
RSVP_HEADER, SENDER_TSPEC, ADSPEC, RSVP_HOP, TIME_VALUE, INTEGRITY,SESSION, POLICY, SENDER_TEMPLATE.

IntServ služba definuje dvě třídy CoS. Ty jsou podle požadované třídy uvedeny v objektu SENDER_TSPEC. Jedná se o službu s řízenou zátěží a o garantovanou službu, které jsou definované podle TOKEN_BUCKET [7] modelu.

3.6.1 SLUŽBA S ŘÍZENOU ZÁTĚŽÍ

- **(Controlled Load Service) CS. IETF RFC 2211**

  Zpoždění paketů je deterministické povahy a má zaručené průměrné zpoždění a zajištění vysokého procenta přenášených dat. Tato služba je určena pro RTT aplikace, které mají vysokou citlivost na přetížení v síti. Tato služba se řídí pomocí hodnoty „Burst Time“, která určuje čas, po který může aplikace generovat data v maximální možné míře a kdy je dodržena kapacita datové cesty a vyrovnávací paměti. Požadované parametry služby jsou zasílány žádostí v objektu TSPEC. Plánovací mechanizmy pro rozlišení, zda vyhovět požadavkům či ne, mohou být libovolné. Například pro VoIP se využívá WFQ s RSVP.

3.6.2 GARANTOVANÁ SLUŽBA

- **(Garanted Service) GS IETF RFC 2212**

  Zde je zaručeno minimálních ztrát paketů a je také definované maximální zpoždění deterministické povahy a zaručená šířka pásma. Tato služba je určena pro RTI aplikace. Zde jsou definovány parametry hodnotou TOCKEN_BUCKET_TSPEC obsaženou v objektu SENDER_TSPEC. Dochází zde ke kontrole zpoždění. Garantovaná služba využívá objekt FLUID BUFFER, který se řídí TOKEN BUCKET modelem. Tím se zabezpečí, že zpoždění, které vzniklo řazením dat do front , bude mít menší hodnotu než celkové zpoždění. Výpočet a uvedené metody jsou v RFC 2210.

3.7 YESSIR

RSVP byl vyvinut pro rezervaci pásma v IP síti. Má ovšem dva závažné problémy. Tím jsou složitost a rozšiřitelnost. Špatnou škálovatelnost a problémy s převodem na hranicích sítě. Spotřebovává velikou šířku pásma a potřebuje veliké množství odkládací paměti. Proto jsou vyvíjeny další protokoly, které by zjednodušili rezervaci prostředků.. Za tímto účelem byl vyvinut i protokol YESSIR.(YeT another Sender Session Internet).[8]

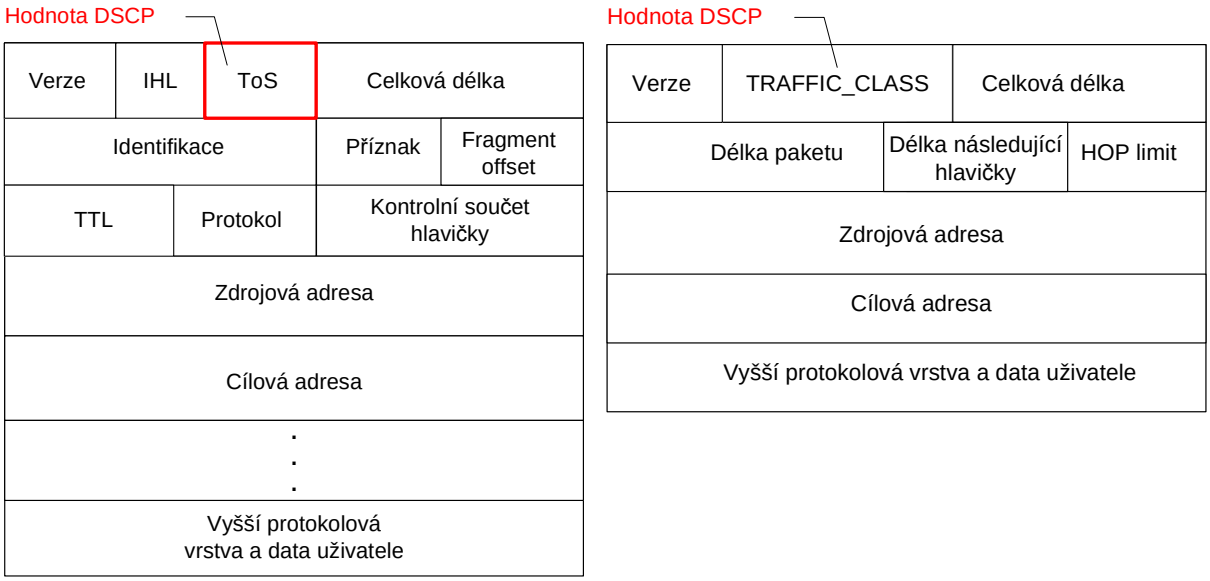
Tento protokol je možné provozovat i ve spolupráci s protokolem RSVP. Nabízí alternativu k rezervací prostředků a využívá RTCP protokolu k zasílání zpráv. Podobně jako RSVP používá k dealokaci zdrojů zprávy RTCP_BAY. Podporuje individuální a sdílený rezervační styl. Tyto rezervace jsou definovány obdobně jako ve WILDCARD_FILTER a SHARED_FILTER v RSVP. Zatímco RSVP je orientovaný na příjemce, YESSIR je orientovaný na odesílatele.

3.8 DIFERENCOVANÉ SLUŽBY DIFFSERV

DiffServ služby jsou definovány v mnoha RFC. Posledním vydáním skupinou IETF byl dokument „ Extensions for Differentiated Services-aware Traffic Engineered LSPs“ v roce 2006. Základ DiffServ služeb byl definován v RFC2475.

V IntServ síti je problém škálovatelnosti. Z tohoto důvodu se v DiffServ síti přesunula veškerá úprava provozu a klasifikace na hraniční směrovače. V tomto typu sítě dochází k dělení jednotlivých služeb podle jejich nároků. Na rozdíl od IntServ sítě, kde o zajištění kvality přenosu dat žádají aplikace, v DiffServ síti jsou požadavky předem definované a aplikace již o zajištění kvality přenosu dat nežádají .

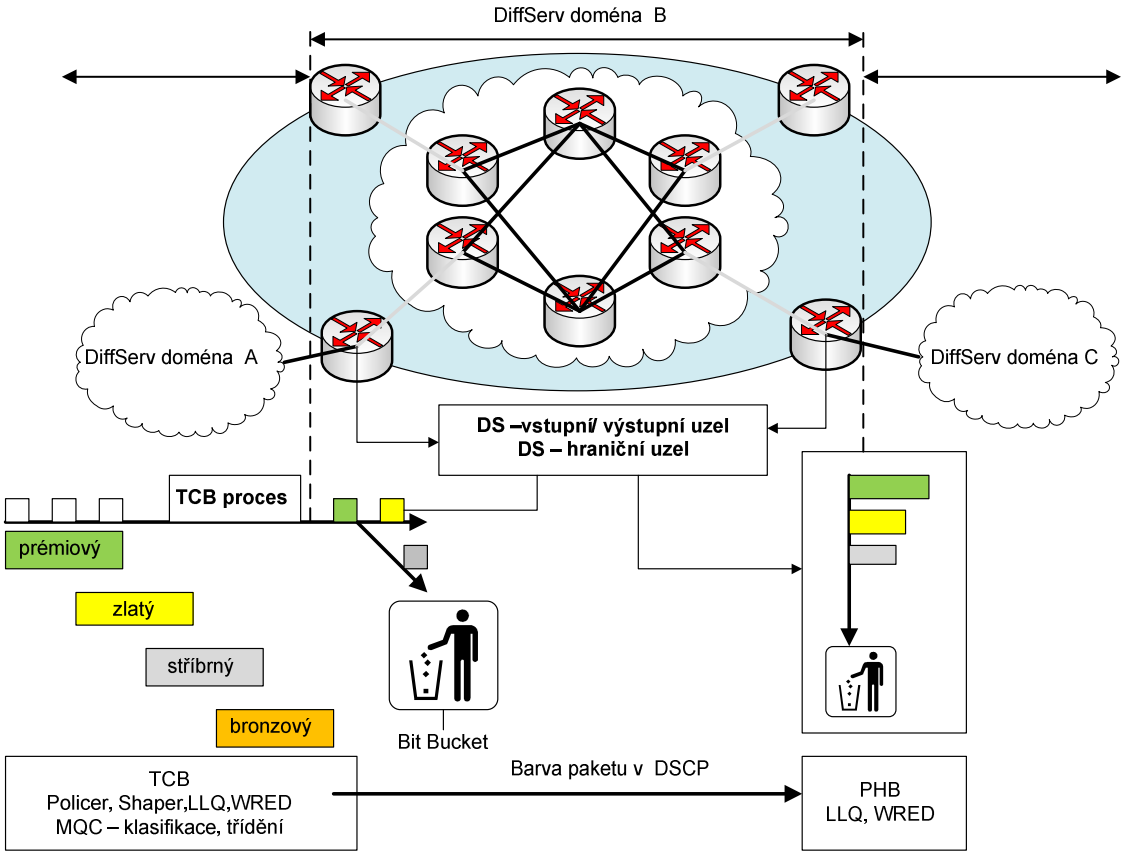
Reprezentované datové toky jsou zde ohodnoceny podle jednotlivých tříd CoS a rozděleny do určitého PHB – Per Hop Behavior (metody pro fronty a forwarding).[9]
K určení do jakého PHB budou data namapována, slouží jak IP precedens, tak DSCP hodnota zapsaná v poli ToS v hlavičce IP paketu ve verzi IPv4, nebo TRAFFIC_CLASS oktet v hlavičce IP paketu verze IPv6 . viz Obrázek 3.3



Obrázek 3.3.: DSCP v IP paketu.

V základním modelu DiffServ sítě se nachází několik DiffServ domén z nutnosti rozdělit síť na menší celky. Souhrnně se nazývají DS celky viz. Obrázek 3.4. Data vstupující do této sítě jsou nejprve klasifikována na okrajovém směrovači (Traffic conditioners) a namapována na příslušné PHB (směrovače v doméně).

V DiffServ síti se vykonává právě jen mapování dat na PHB ve spolupráci s mechanizmy QoS jako je WRED, LLQ atp. podle toho, jaké zařízení máme k dispozici. Poté jsou podle dané značky pakety posílány přes páteřní směrovače, které nevykonávají žádnou další činnost, než přeposílání dat. Na rozhraní DS domén jsou tzv. hraniční směrovače. Ty zajišťují reklasifikaci značek v paketu mezi DS doménami, pokud DS síť, do které data vstupují má jiné nastavení QoS.



Obrázek 3.4. DiffServ doména a její mechanizmy [1].

3.9 DCSP (DIFFSERV CODE POINT)

IETF v pracích RFC neurčuje jakým způsobem bude PHB plnit funkci řazení. Zda se bude mechanizmus řazení front zakládat na hodnotě DSCP, nebo podle hodnoty IP precedens v hlavičce IP paketu. To je ponecháno na dohodě zákazníka a poskytovatele sítě. Tato dohoda je součástí tzv. SLA. Šest nejvyšších platných bitů v DiffServ poli se nazývá DSCP pole. Poslední dva neobsazené bity (CU) v DiffServ poli se prozatím používají uvnitř DS domény pro explicitní oznámení zahlcení sítě.

Následující dva obrázky, viz. Obrázek 3.5 a viz. Obrázek 3.6, zobrazují srovnání ToS Byte definované v RFC791 a Diffserv pole [1].

P2	P1	P0	T2	T1	T0	CU1	CU0

Obrázek 3.5: ToS Byte

IP precedens – tři bity (P2 – P0) – (RFC1122) – hodnota definovaná aplikací nebo směrovačem. Slouží k určení priority jednotlivých dat.
Type of Services - Zpoždění, výkon, spolehlivost atd. – tři bity (T2 – T0)(RFC1349)
CU (Currently unused) – neobsazené dva bity (CU1, CU0)

DiffServ pole

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Obrázek 3.6: DiffServ pole

DSCP – šest bitů (DS5-DS0) (RFC2474)
ECN – dva bity

PHB v každém síťovém uzlu je klasifikováno podle standardního Diffserv pole. Základní hodnota DSCP pole je 000 000. První tři bity jsou zpětně konvertibilní s IP precedens. Pokud se konvertuje z IP precedens do DSCP postup je takovýto, že IP precedens 5 (101) se namapuje do DSCP pole jako 101 000 .

DiffServ aplikuje první tři bity k nastavení priority, stejně jako IP precedens. Ale dalšími třemi bity je schopno služby rozlišit do více tříd. DiffServ reorganizuje a přejmenovává IP precedenc jak je uvedeno viz. Tabulka 3.1

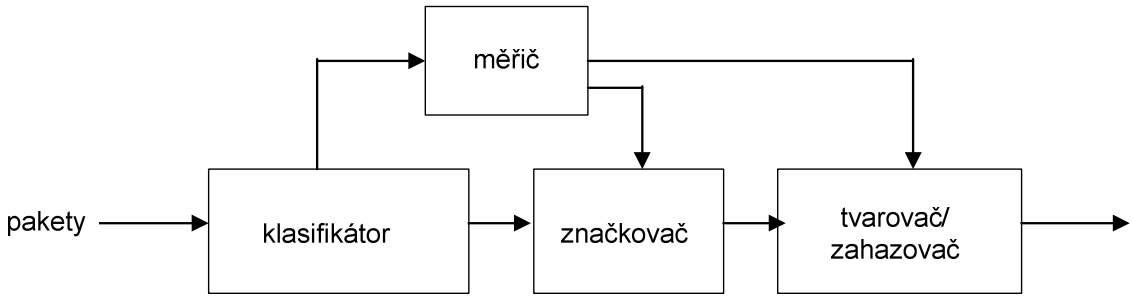
Tabulka 3.1.: IP precedenc/DSCP

Stupeň IP precedenc	Popis dle DSCP
7 Network kontrol	Obsazeno – linkové protokoly , směrovací
6 Internetwork kontrol	Obsazeno pro IP směrovací protokoly
5 Critical	Express forwarding (EF)
4 Flash override	Třída 4
3 Flash	Třída 3
2 Immediate	Třída 2
1 Priority	Třída 1
0 Routine	Best effort

Zařízení rozdělují provoz nejprve podle třídy služby. Zde ne všechna zařízení jsou schopna rozeznávat hodnoty DSCP pole DS2 a DS1 a i když je rozeznají, není zaručeno stejné PHB. To záleží také na tom, jak je každé zařízení v DS síti nakonfigurované.

3.10 REFERENČNÍ MODEL DIFFSERV

Se zvláštním typem paketů v DS doméně musí být nějak zacházeno. K tomu slouží její vnitřní mechanizmus, který mají implementovány směrovače viz. Obrázek 3.7. Jedná se zde o úpravu provozu [11]. Ta je vykonávána na mezních uzlech DS domény. Na vnitřních uzlech je vyžadována podpora zasílání paketů dle hodnoty DSCP.



Obrázek 3.7: Základní model DiffServ pro úpravu provozu:Traffic Conditioner

Traffic conditioners (TC) jsou hraniční směrovače, vykonávající funkci klasifikace paketů, tvarování, značkování, měření. Směrovače v doméně (PHB) provádí alokaci zdrojů, tvarování a zahazování .

3.10.1.1 KLASIFIKÁTOR (CLASSIFIER)

Základní klasifikátory rozdělujeme na MultiField (MF) a Behavior Aggregate (BA). BA třídí pakety na základě hodnoty v DSCP poli. MF třídí pakety podle více polí v paketu a to podle identifikace IP toku, IP precedens, nebo DSCP, MAC, URL, NBAR, TCP/IP parametrů.

3.10.1.2 ZNAČENÍ PAKETŮ (MARKER) V DSCP

Podle značky paketu se definuje zpracování paketů. Na směrovačích jsou pakety označeny podle IP precedens (class selektor), nebo podle hodnoty DSCP pole a QoS skupiny. A to podle toho, jaká konfigurace bude upřednostněna v rámci SLA. Ke zpracování mohou být označeny jako služby Best Effort (BE), Expedited forwarding (EF), Assured Forwarding (AF) či Class Selector (CS)

- EF - (RFC 3246) zajistí minimální odchozí rychlost, garantovanou šířku pásma a hlídá šířku pásma. Nadměrný provoz je zde zahazován. Využívá se zde zahazování paketů typu RED. Určené pro aplikace v reálném čase. (DSCP 46)
- AFxy - (RFC2597) také garantuje šířku pásma, umožní šířku pásma rozšířit pokud jsou volné zdroje. Nehodí se pro aplikace v reálném čase. Využívá se ze také funkce RED. V AF byli definovány čtyři doručovací třídy AF1 až AF4 s 12 podtřídami. Podle dohody SLA (Service Level Agreement) jsou jednotlivé pakety při vstupu kontrolovány a pokud překročí přidělený limit jsou buďto zařazeny do podtřídy nebo zahozeny. X – 4 AF třídy (AF1y – AF4y) Y- 3 preference pravděpodobnosti zahození paketů dané třídy. (DSCP 10/12/14, 18/20/22, 26/28/30, 34/36/38)
- CSx – Class Selector (RFC2474), kde x koresponduje s IP precedens hodnotou 1-7 (DSCP 8, 16, 24, 32, 40, 48, 56)

3.10.1.3 MĚŘENÍ (TRAFFIC METTERING)

Zde se využívá funkcí „traffic rate manageru“, který je obsažen v hraničních směrovačích, kde jsou implementovány funkce tvarování a definice politik. Data, která

jdou od zdroje, se změří a porovnají s uloženým datovým profilem. Profilem jsou zde dohodnuté podmínky mezi zákazníkem a poskytovatelem SLA .Data, která nevyhovují, jsou buďto zahozena, nebo přetvarována či přeznačena (Shapper, Dropper, Remarker).

3.10.1.4 TVAROVÁNÍ PROVOZU A POLITIK (SHAPPING AND POLICY)

Tvarovač odesílá pakety konstantní rychlostí a urovnává provoz. Jsou zde využity metody front jako je FIFO či WFQ pro pakety překračující rychlost. Nevýhodou je, že i pakety označené s vyšší prioritou mohou být zahozeny. Funkce dohlížející na provoz, nepoužívají mezipaměť. Zahazují pakety až při překročení limitů linky. Obojí metody využívají „Token Bucket“ modelu [7].

3.11 ALGORITMY QOS

Tyto algoritmy uvedené viz. Tabulka 3.2, jsou využívané jak samostatně, tak i v interakci s předchozími popsanými metodami QoS. Jsou většinou implementovány na jednotlivých prvcích v síti většinou směrovačích. Společně s modely QoS tvoří neoddělitelnou součást QoS. Některé z těchto algoritmů již byly v předchozím textu zmíněny. Můžeme je rozdělit podle aplikování do jednotlivých skupin. [8]

- Formování paketů – FIFO, Leacky Bucket, Token Bucket
- Alokace zdrojů - Multi-Priority Queing, Fair Queing, Wighted Fair Queing, CBFQ.
- Zahazování paketů (metody zahlcení) - slouží funkce RED, WRED.

Tabulka 3.2.: Definice algoritmů

Leacky Bucket	Řízení rychlosti vstupu paketů do sítě.
Token Bucket	Řízení rychlosti přenosu podle tokenů.
FIFO	Metoda vážení jednou frontou na výstup
FQ	Metoda řízení front
WFQ	Metoda řazení front váženého podle priorit
CBWFQ	Metoda řazení front váženého podle tříd. Váhy v mocninách dvou.
RED	Opatření proti zahlcení sítě předem
WRED	opatření proti zahlcení sítě předem s váhami a prioritami.

4 INTSERV SLUŽBY S VYUŽITÍM DIFFSERV SÍTÍ

Základní myšlenkou spolupráce je zlepšení rozšířitelnosti IntServ služeb za pomoci DiffServ služeb, protože Diffserv sítě je vhodné použít pro rozlehlejší topologie a také jako páteřní sítě. Oproti tomu DiffServ získá použitím RSVP mechanizmy pro kvantitativní využití síťových služeb [9] .

- V DiffServ síti je kontrola přístupu aplikována v relativně statické cestě, obstaráním kontrolních parametrů v síťových uzlech. Použitím RSVP bude schopné DiffServ aplikovat základní kontrolu přístupu, která bude optimalizovat použití zdrojů v síti a RSVP umožní DiffServ použít základní kontrolu přístupu dat .
- DSCP může být nastaven buď v hostiteli, nebo ve směrovači a to přes explicitní mechanismus, jako je RSVP DCLASS. Diffserv bude schopna vykonávat přímou identifikaci a třídění provozu.
- IntServ síťové prvky vykonávají „per-flow“ úpravu datového přenosu. Takovouto úpravou provozu se zvětší schopnost DiffServ sítě poskytnout kvantitativní služby agregačního řízení provozu.

Ve spolupráci obou architektur umožní IntServ architektura uživatelům rezervovat síťové zdroje za použití RSVP zpráv a s využitím DiffServ architektury se vyhne RSVP/IntServ architektura problémům s rozšiřitelností.

RSVP/IntServ – DiffServ spolupráce závisí na DiffServ řízení zdrojů a na tom, jestli DS podporuje RSVP protokol. Toto řízení zásobení zdrojů může být:

- Statické zásobení zdrojů (administrátory)
- Dynamické zásobení zdrojů s využitím protokolů
- Dynamické zásobení zdrojů pomocí jiných nástrojů jako je BB (Bandwidth Broker)

V případě statického zásobení zdroji vyjedná majitel DS statické SLA s uživatelem. U dynamického zásobení zdroji, jsou SLA vyjednány dle požadavků od více uživatelů. K tomuto účelu se využívají mechanizmy jako je BB a jako mezi-doménový komunikační protokol se využívá RSVP nebo SNMP.

Konstrukčně mohou být RSVP/IntServ-DiffServ architektury tvořeny :

- Mapováním IntServ služeb na PHB na hranicích domén. IntServ funguje jako přístupová síť, DiffServ pak jako vnitřní síť.
- DiffServ doména pracuje bez podpory RSVP. Slouží pro IntServ přístupovou síť jen jako přepravce.
- Mapování DiffServ služeb na vhodnou IntServ službu na hranici domén. DiffServ pracuje jako přístupová síť, IntServ pak jako vnitřní síť.
- IntServ doména slouží pro přístupovou DiffServ doménu jako přepravce.

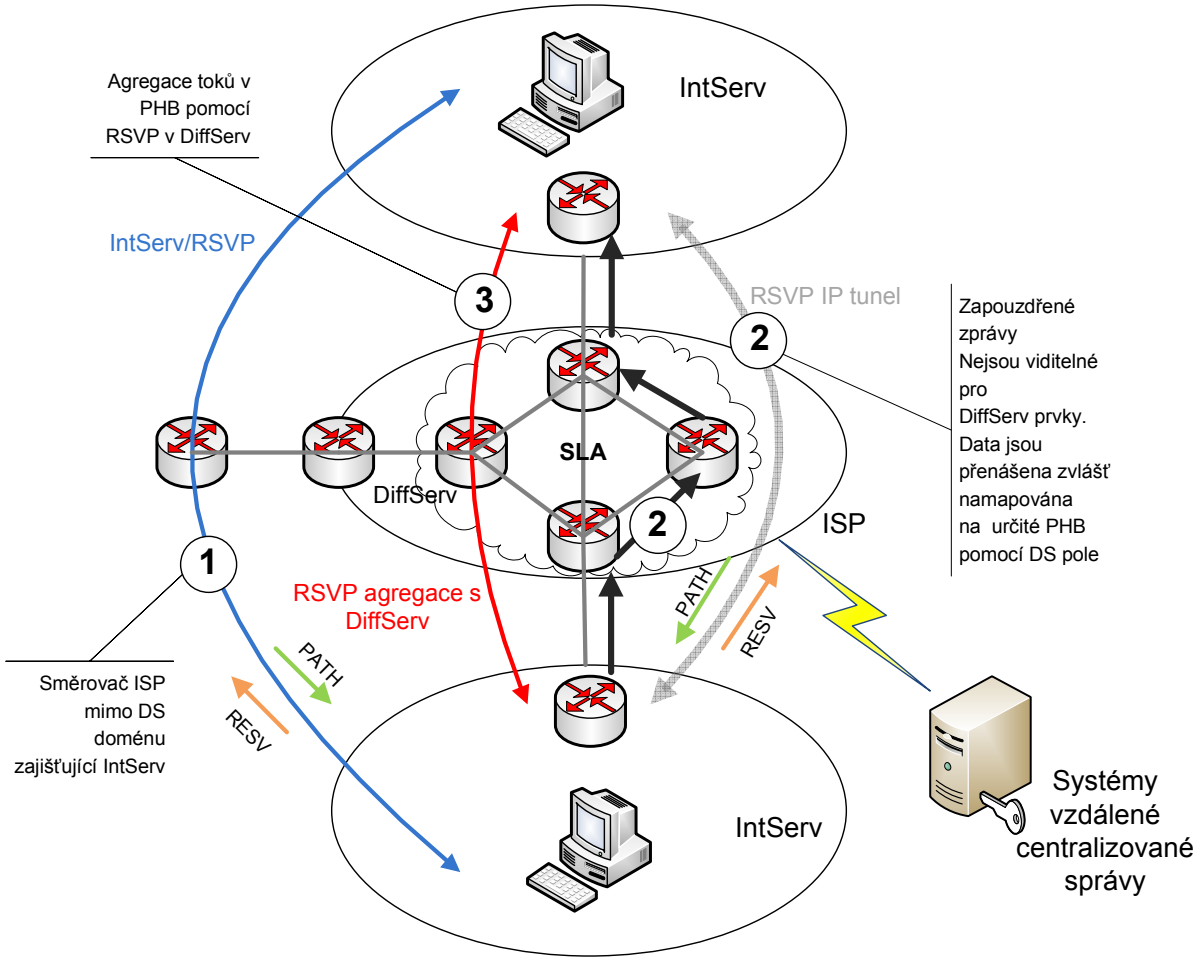
Nejvýhodnější je použití první a druhé varianty. Zde je DiffServ region mezi Intserv sítěmi jako přepravní mezičlánek. Ostatní varianty mají problém s rozšiřitelností, jako je tomu u samotné RSVP/IntServ architektury.

Spolupráce mezi IntServ a DiffServ ve zmíněných variantách je následující viz Obrázek 4.1:

- RSVP/IntServ přes DiffServ (1)
- Agregace RSVP/IntServ stavů
  - ✓ RSVP agregace za využití tunelu (2)
  - ✓ RSVP agregace využívající DiffServ mechanizmů (3)
- Paralerní operace obou architektur

Vše vyžaduje základní požadavky pro splnění správné funkce RSVP/Intserv-DiffServ architektury [8]:

- Aplikace na koncových zařízeních mají podporu QoS a generují RSVP zprávy.
- Přístupová síť je v nejlepším případě založená na IntServ architektuře a generuje RSVP zprávy.
- Je zaručena transparentnost DiffServ architektury vůči IntServ architektuře
- Hraniční směšovače DiffServ architektury jsou RID směrovače.
- DiffServ doména poskytuje minimálně dvě úrovně služeb.
- Vyjednané SLA se zákazníkem je v ideálním případě implementováno staticky administrátorem.



Obrázek 4.1: Možnosti spolupráce IntServ/DiffServ

4.1 POŽADAVKY NA MAPOVÁNÍ SLUŽEB

Pokud je tedy DiffServ doména používána jako přenosové médium, je základní operací správné namapování služeb z IntServ domény na vhodné PHB viz. Tabulka 4.1
Požadavkem tedy bude, aby zaručená služba byla mapována na EF PHB, zatímco služba s řízenou zátěží na AF PHB s různou úrovní, podle toho, jestli je tolerantní vůči zpoždění nebo není.

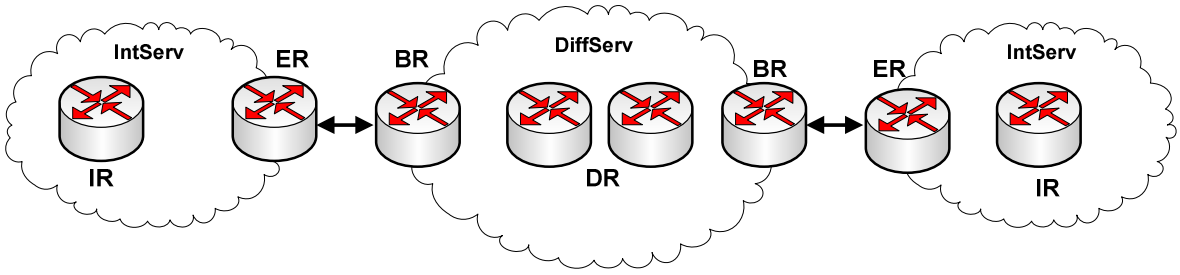
Tabulka 4.1.: Mapování IntServ na PHB

IntServ	Kvalifikátor	DiffServ PHB
Zaručená služba	---	EF
Služba s řízenou zátěží	L	AF(vysoká priorita)
	H	AF(nízká priorita)

Směrovače, které budou obsahovat jak nástroje pro obsluhu RSVP, tak i nástroje pro DiffServ služby, budou provádět toto mapování služeb a budou situovány většinou jako okrajové směrovače domény. Kdyby nicméně klasifikace probíhala mimo DS, pak by taková klasifikace probíhala za použitím mechanizmu RSVP DCLASS objektu.

4.2 ZÁKLADNÍ INTSERV/DIFFSERV ARCHITEKTURA

V základním modelu viz. Obrázek 4.2 je uvažováno vyjednání zásobení zdrojů staticky (SLA) [9].



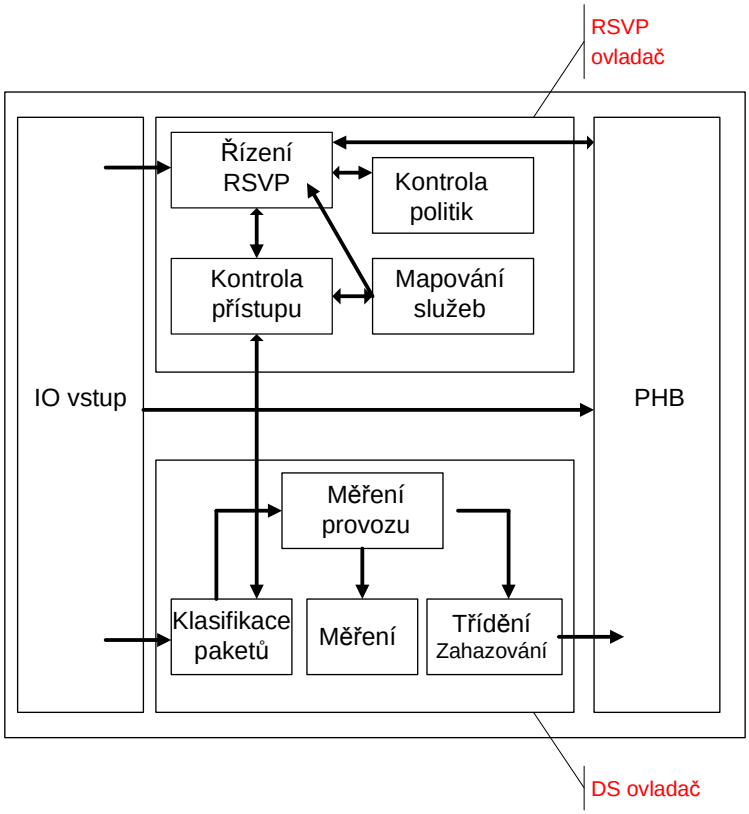
Obrázek 4.2: Model IntServ/DiffServ s pojmenováním směrovačů

- **IR** - jsou „Ingress" vstupní směrovače, standardní RSVP/IntServ směrovače, které provádí RSVP signalizaci, kontrolu přístupu a třídění.
- **ER** – jsou „Edge“ hraniční směrovače, neboli okrajové směrovače . Zajišťují konektivitu do DiffServ domény. Provádějí RSVP signalizaci a funkce související s komunikací s DiffServ doménou. Mohou vykonávat i další funkce, pokud se bude jednat o domény s dynamickým přidělováním zdrojů. Ku příkladu vyjednávání šířky pásma pomocí BB, nebo pokud by vystupoval jako agregační nebo deagregační směrovač v případě agregace RSVP.
- **CR** – „Core“ směrovače, vnitřní směrovače DiffServ domény. Aplikují PHB podle DSCP značky. Zde procházejí RSVP zapouzdřené. Směrovače nemusejí RSVP zprávy podporovat.
- **BR** – okrajový směrovač DiffServ domény. Mapuje IntServ na PHB a ku příkladu tuneluje RSVP zprávy. Je nejdůležitějším prvkem ve spolupráci obou zmíněných architektur. Je také pojmenován jako RSVP/Intserv Diffserv (RID) směrovač.

4.3 RSVP/INTSERV – DIFFSERV OKRAJOVÝ SMĚROVAČ (RID)

Jedná se o klasický DiffServ směrovač, viz. Obrázek 4.3, který je navíc vybaven o ovladač RSVP zpráv. Ten obsahuje prvky kontroly přístupu, mapování služeb, RSVP managera a prvek kontroly politik [9]. „RSVP message handler“, neboli RSVP ovladač, přijímá příchozí RSVP zprávy a podle způsobu konfigurace je zpracovává. Provozní data jsou zařazeny do zpracování DS ovladačem (DS packet handler).

Klasifikátor paketů v RID je konfigurován tak, aby klasifikoval jak RSVP zprávy tak i DiffServ pakety. Tato činnost je pro oba ovladače společná. Může být konfigurován jako MF nebo BA klasifikátor. Podle toho mohou být sestaveny filtry pro třídění RSVP paketů a DiffServ paketů .



Obrázek 4.3: RID směrovač [9]

4.3.1 INTSERV ZARUČENÁ SLUŽBA V DS

Při této realizaci je nejvýhodnější namapování služeb na EF PHB a zaručit tak konstantní časové zpoždění a šířku pásma. V DiffServ doméně může nastat několik druhů zpoždění. Tato zpoždění mohou být způsobena frontami paketů, dále mohou být způsobena serializačním a propagačním zpožděním. Většinou jsou jednotlivé parametry kvality dohodnuty předem se zákazníkem a je zde dohodnuto tzv. statické SLA a provedena konfigurace tak, aby bylo dohodnutých parametrů zajištěno.

4.3.2 INTSERV SLUŽBA S ŘÍZENOU ZÁTĚŽÍ V DS

V této variantě jsou dvě možnosti namapování služeb. A to buď na AF PHB nebo EF PHB. Pokud nebude AF PHB přístupné budou se služby mapovat na EF PHB. Po namapování je zapsána příslušná hodnota kvality služby do DSCP pole, jak bylo uvedeno v kapitole o DiffServ architektuře. Data jsou posílána přes DiffServ doménu transparentním způsobem dle zařazení do příslušné služby.

4.3.3 RSVP AGREGACE S VYUŽITÍM TUNELU V DIFFSERV

Většinou se jedná o tzv. „RSVP Not Aware DiffServ Network Region“ [2], neboli ne všechny síťové směrovače v doméně podporují RSVP komunikaci. Zde jsou signalizační data IntServ domény zasílány pomocí RSVP tunelování DiffServ doménou. Za normálních okolností při vstupu RSVP zprávy do domény, kde není podpora RSVP, jsou tyto zprávy ignorovány. Stejně tak mohou být tyto RSVP zprávy ignorovány v DiffServ doméně.

Pokud by každý směrovač v DiffServ doméně zpracovával RSVP zprávy, jako směrovače IntServ domény, nastaly by stejné problémy se škálovatelností a rozšiřitelností, stejně jako v IntServ doméně. V architektuře „IntServ/ RSVP over DiffServ“, jsou RSVP zprávy samostatné na mechanizmech použitých v DiffServ. To je vyřešeno tunelováním RSVP zpráv v IP tunelech přes DiffServ doménu.

4.3.4 RSVP TUNEL

RSVP IP tunely mohou být tvořeny :

- staticky konfigurací
- dynamicky tzv. rezervací tunelu.

Pro vytvoření RSVP tunelu jsou využity směrovače na okraji DiffServ domény tj. RID směrovače. Při vytvoření IP RSVP tunelu jsou RSVP zprávy zasílány odděleně od dat.

Tím je zajištěna jejich nezávislost. Tunelování zpráv je primárně vytvořeno přidáním IP hlavičky paketu RSVP okrajovým směrovačem RID. Tím dojde k zapouzdření RSVP zprávy, neboli „enkapsulaci“. Při výstupu následuje proces opačný. Uvnitř DiffServ domény směrovače nezpracovávají tyto zprávy, protože jsou, jak bylo zmíněno, zapouzdřené v klasické IP hlavičce a nejsou pro směrovače viditelné..

Okrajový směrovač zapouzdří zprávy pokud je mu znám výstupní směrovač. Tato informace je zapsaná v tabulce, která obsahuje údaje o IP tunelech. Tato tabulka je uložena v RID okrajových směrovačích, nebo je tato informace pevně na směrovači nakonfigurována.

Pokud se jedná o dynamické vytváření tunelů, jsou k tomuto účelu definované dvě RSVP zprávy a to SESSION_ASSOC Object a NODE_CHAR Object. Více o dynamickém vytváření v (RFC 2746) .

4.3.5 RSVP AGREGACE S VYUŽITÍM DIFFSERV

Jedná se o možnou spolupráci IntServ/DiffServ architektur dle RFC 4860 [4]. Tato problematika je rozsáhlejší a v tomto případě se jedná o nástin celého řešení. V takovém způsobu rezervace síťových zdrojů se jedná o implicitní postup. V případě explicitního postupu by se jednalo také o RSVP agregaci s využitím DS, ale hodnoty DSCP by byly nastaveny v hostitelích za použití explicitního mechanizmu RSVP CLASS objektů a jednalo by se v tomto případě o emulaci DS domén.

Jedná se ale vždy o „RSVP Aware DiffServ Network Region“, směrovače v DS podporují tyto modifikované RSVP. Tato agregace tzv. „RSVP-AGG“ definuje způsob RSVP rezervace zdrojů „E2E“ RSVP neboli „end-to-end“ pomocí agregovaných rezervací v DS.

Společnost IANA modifikovala za tímto účelem registr RSVP parametrů a definovala dvě nové podtřídy do CLASS SESSION třídy. GENERIC-AGGREGATE-IP4 [RFC4860] a ENERIC-AGGREGATE-IP6 [RFC4860] Agregace rezervací v DS využívá objektu SESSION ve třídě RSVP CLASS, který obsahuje IP adresu odesílatele a příjemce a hodnotu DSCP z PHB identifikující, které zdroje DiffServ budou využity .

SESSION objekt je specifikován jako:

- Class = SESSION
- C-Type = RSVP-AGGREGATE-IP4

Tato agregace rezervací využívá objektů SENDER_TEMPLATE a FILTER_SPEC.

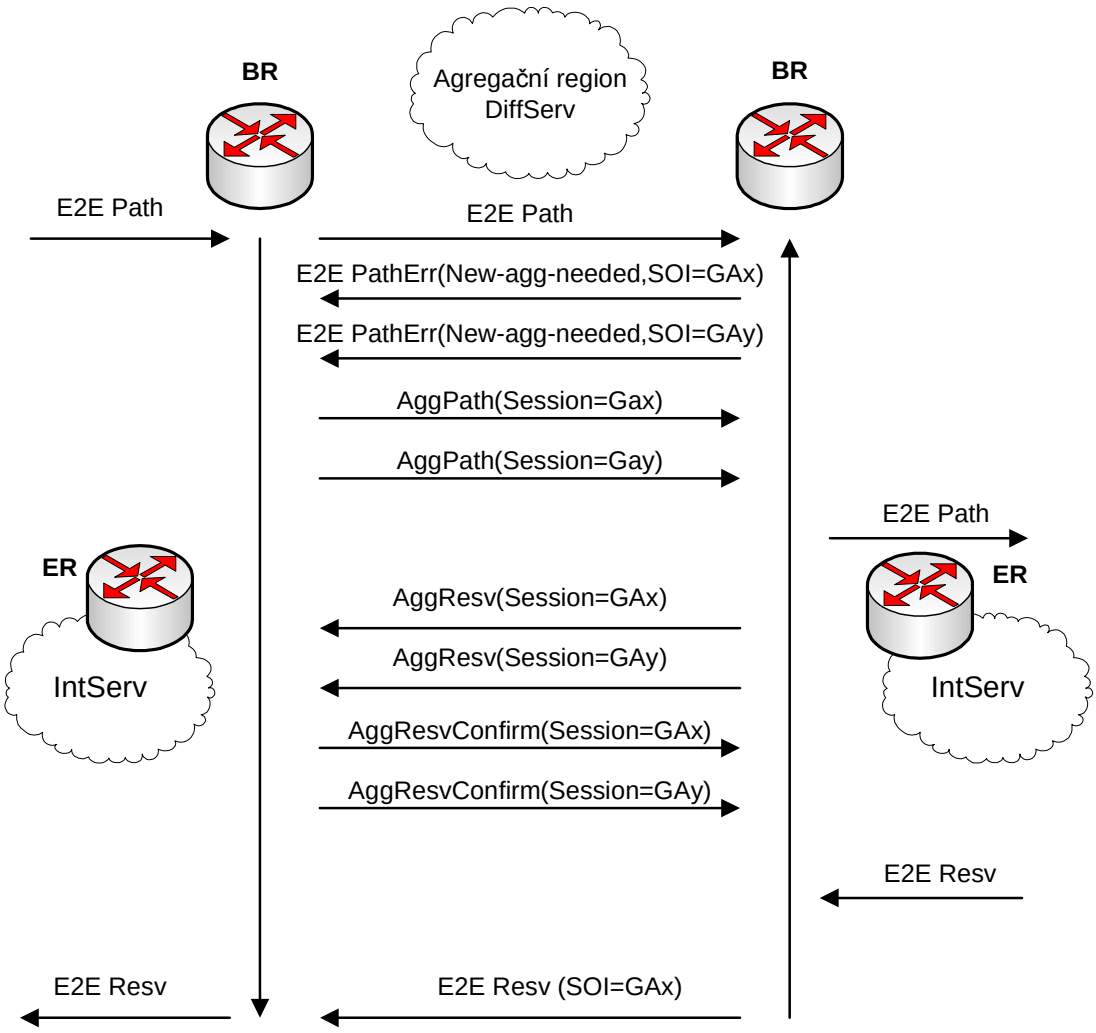
SENDER_TEMPLATE je specifikován jako:

- Class = SENDER_TEMPLATE,
- C-Type = RSVP-AGGREGATE-IP4

V tomto případě je vstupní směrovač DS domény agregátor a výstupní deagregátor. Jedná se především o transparentní end-to-end RSVP rezervaci zdrojů. Zde se považuje DiffServ doména za agregační region a síťové prostředky musí podporovat tyto typy modifikovaných RSVP zpráv. V tomto typu součinnosti jsou dedikovány i další objekty RSVP jako je například RSVP-IPSEC pro vytváření zabezpečeného spojení či další objekty pro vytváření virtuálních spojení VPN. Poslední úprava RFC 4860 byla definována v roce 2007 a nabízí široké možnosti využití a to především v „multicastovém“ sezení a dynamickém vytváření spojení a rezervací prostředků. [6] Ukazuje možnost sestavení rezervace za použitím objektů viz Obrázek 4.4:

- New-Agg-Needed PathErr - Požadavek na novou rezervaci zdroje
- SESSION-OF-INTEREST (SOI) - Požadovaný typ (IPv4 nebo IPv6)

GENERIC-AGGREGATE SESSION (GAx,y) - PHB-ID odesílatele zprávy zapsané v hodnotě x, y (AF nebo EF), zpráva dále obsahuje informace o cílové adrese a deagregačním směrovači.

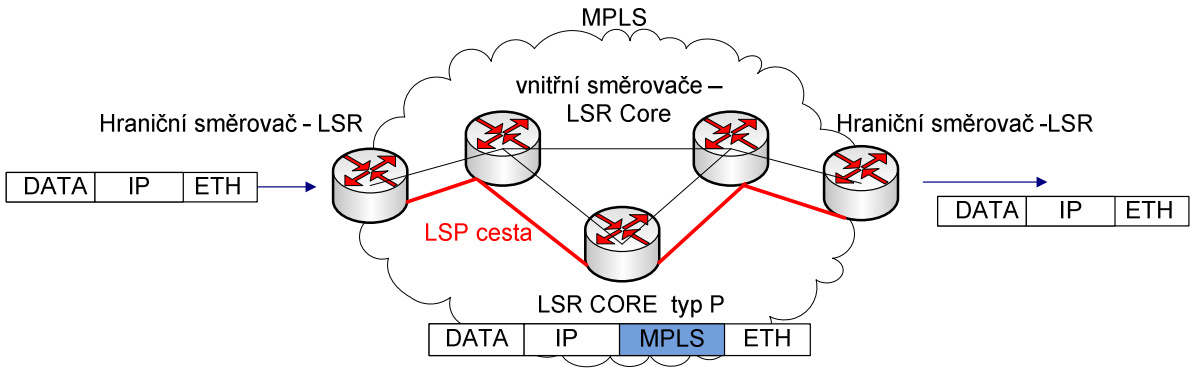


Obrázek 4.4: Způsob agregace pomocí modifikovaného RSVP dle RFC 4860.

4.4 MPLS – ZÁKLADNÍ MODEL

MPLS, jak je z názvu patrno, je určen pro Multi Protokol Label Switching a spolupracuje právě s různými typy sítí jako je Frame Relay či ATM.
MPLS podporuje veškeré QoS služby. Podporuje lepší alokaci zdrojů, nabízí jednodušší management, vysokou přizpůsobivost, menší velikost směrovacích tabulek, transparentní DiffServ služby. [11]

Přepínání značek je založeno na oddělení směrování (routing) a předávání paketů (forwarding). Přepíná pakety na základě návěstí v doplněném záhlaví protokolu MPLS.



Obrázek 4.5: Schéma MPLS sítě

Na okraji této sítě se nachází ELSR směrovače (Edge Label Switching Router) a to buď jako vstupní (ingress) nebo výstupní (egress). Vstupní směrovač zajišťuje analýzu informací v IP paketu jako je třída QoS služby, síť VPN, adresa cílového uzlu. Na základě těchto informací přidělí ELRS router paketu skupinu FEC. Pro zvolenou skupinu FEC je do MPLS (Shine) přidáno návěstí (Label). Jedná se o klasifikaci paketů Obrázek 4.6.

Přenos záhlaví v rámci MPLS:

PPP/Ethernet	MPLS (Shine) 4 bity	IP	Data

MPLS (Shine):

Label 20 bitů	Experimental 3 bity	Bottom of Stack 1 bit	TTL 8 bitů

Obrázek 4.6: Detail protokolu

- *Label* – návěstí přiřazené k dané třídě FEC
- *Experimental* – např pro DiffServ DSCP
- *BoS* – identifikátor umístnění návěstí v zásobníku
- *TTL* – doba života MPLS paketu

Toto návěstí použijí LSR směrovače uvnitř MPLS sítě. Ty se označují jako typ P (Provider). Samotné předávání funguje podle jednoduché tabulky značek. Směrovače se nemusejí starat o směrovací tabulky. Hraniční LSR směrovač odebírá záhlaví z přijatého MPLS paketu a posílá IP paket na výstupní port. Obsah záhlaví se nemění až na hodnotu TTL. Pakety ve specifikované třídě jsou posílány přes LSR směrovače stejnou cestou . (Label Switched Path).

4.4.1 Vytvoření návěstí

Existují i další metody vytvoření návěstí než podle skupiny FEC. A to podle topologie sítě (Topology- based). Návěstí jsou přenášena s přiřazenými síťovými adresami s využitím směrovacích protokolů BGP a OSPF), dále podle požadavků (Request-based) na třídu

4.4.2 LPS cesta

K vytvoření LSP cesty jsou dvě možnosti. A to nezávislým výběrem cesty nebo explicitním směrováním. V prvním případě jsou po cestě přenášeny zprávy mezi vstupním a výstupním směrovačem podle směrovacích tabulek. Ve druhém případě vstupní směrovač předem definuje cestu paketů. Cesta LSP je jednosměrná. K MPLS síti se externí sítě připojují pomocí Customer Edge směrovačů (CE). Tyto směrovače nepotřebují zvláštní mechanizmy. Vystačí si s běžným IP směrováním.

4.4.3 Směrování a signalizace

Ke směrování a signalizaci se používá protokol LDP (Label Distribution Protokol). Ten slouží k předávání informací o přidělených značkách v LSP. Tento protokol se rozšířil i na signalizaci. Pro signalizaci se používají protokoly LDP/CR, BGP, TDP a explicitně se používá i rozšířený protokol RSVP a to RSVP-TE.

4.4.4 LDP signalizační protokol

Je specializovaný protokol vyvinutý pro MPLS. Využívá 4 třídy zpráv.

- Discovery – vzájemná detekce směrovačů (CDP)

- Adjacency – pro vytváření signalizačních spojení mezi LSP
- Label Advertisement – deklarace mapování návěstí a FEC
- Notification – přenos alarmů v síti

4.4.5 AutoQoS

Jedná se o nasazení automatizovaného přizpůsobení sítě požadavkům QoS pomocí tzv. Policy Managementu. [3]

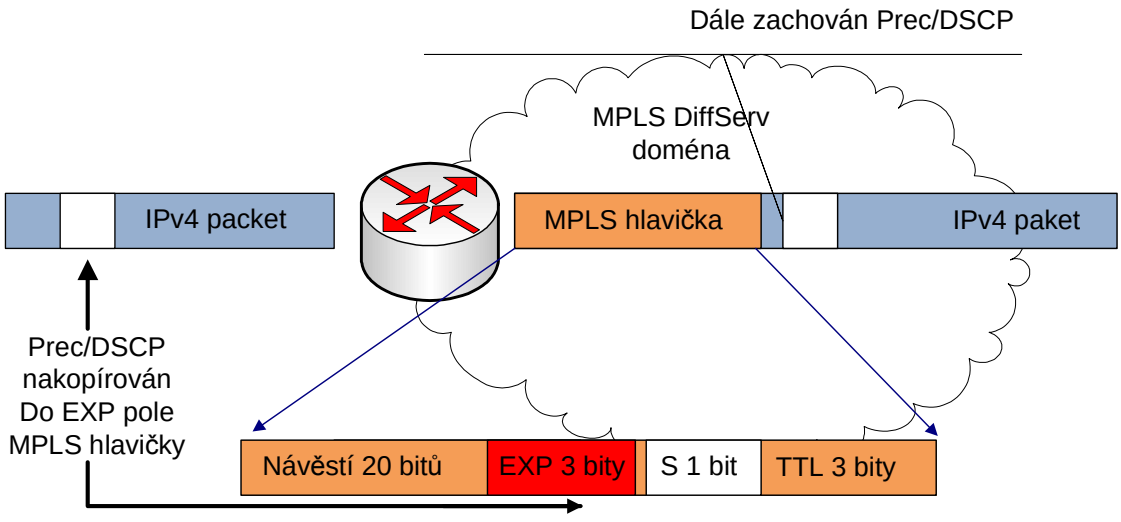
- Policy – neboli politika. Podmínky, podle kterých jsou prováděny jednotlivé interakce
- Policy Management – automatizovaná aplikace politik

V každém síťovém prvku je potřeba nastavit jednotlivá pravidla a i nadále je udržovat. Zde se využívá tzv. centrální definice politik. Z tohoto důvodu existují prvky sítě, které tuto definici propagují na jednotlivé směrovače v celé síti. Těmi jsou :

- PDP (Policy Decision Point) – server s konzolí. Zde jsou vytvářena a prováděna distribuce pravidel pro jednotlivé prvky. Zároveň i Policy server.
- PEP (Policy Enforcement Point) – Jedná se o prvky sítě, kde jsou politiky prosazovány (směrovače, přepínače)

4.5 MPLS DIFFSERV

MPLS Diffserv je definována v RFC3270. Nedefinuje novou architekturu, jen kooperaci MPLS sítě s implementací DiffServ služby. Viz. Obrázek 4.7 je patrná architektura rámce.



Obrázek 4.7: Mapování DiffServ v MPLS

PrecedenceIP/DSCP není přímo viditelné pro MPLS směrovače. Ke definici hodnot dochází pomocí MPLS hlavičky a EXP pole. Proto dochází k namapování hodnoty DSCP pole dopole EXP v MPLS hlavičce
Vyvstává určitý problém s překladem hodnot. Pole DSCP má 6 bitů, přičemž pole EXP jen 3 bity. Nabízí se tyto dvě řešení:

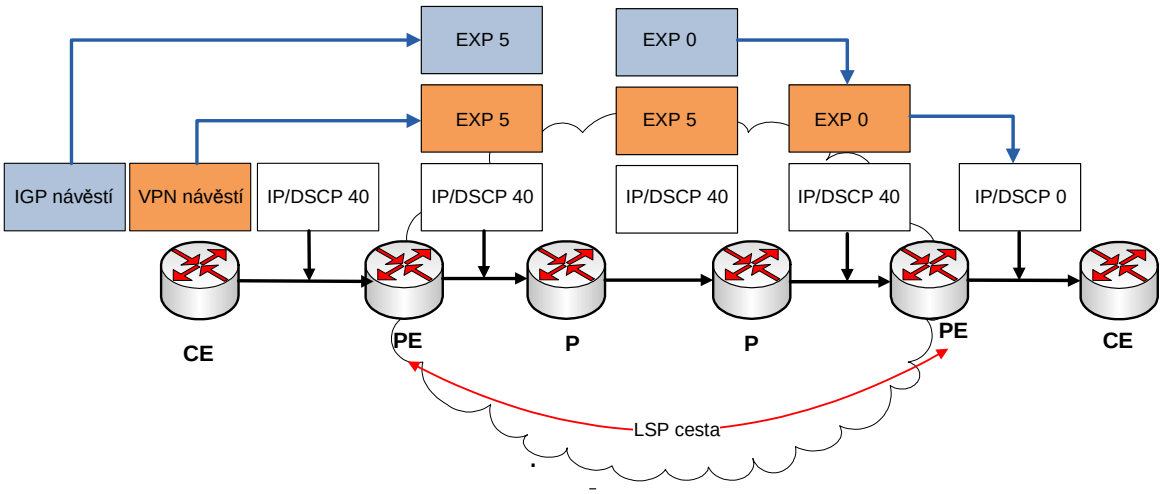
- E-LSP - vážení jen prostřednictvím EXP pole. Maximálně 8 tříd podobně jako ToS pole
- L-LSP – využití pole LABEL (návěstí) a následně EXP pole. 64 tříd podobně jako DiffServ. Zde je do pole LABEL přidána hodnota třídy FEC viz. Kapitola MPLS.

4.5.1 MPLS DiffServ způsoby tunelování

Základ v RFC3270 [4]. Rozlišují se zde tři základní modely:

- Uniform
- Short pipe
- Pipe

První z modelů „Uniformní“ tunelování způsobí, že hodnota EXP na výstupním PHB MPLS domény je namapována jako nová hodnota pro pole DSCP na výstupu jak je vidět názorně viz. Obrázek 4.8.



Obrázek 4.8: Uniformní tunelování

„Short pipe“ nemění hodnotu DSCP na výstupu.Používá se v případě, že chce zákazník zachovat DSCP beze změny. Uvnitř IP/MPLS páteře se zachovává jednotná DiffServ doména. Pipe je stejné jako Short pipe s rozdílem , že výstupní WFQ metoda na rozhranní PE – CE je založena na politice sousedních DiffServ domén

4.5.2 MPLS IntServ

O IntServ v MPLS je zmíněno krátce, v podstatě se jedná o skoro identický postup jako v případě Diffserv s rozdílem způsobu signalizace a sestavení LSP cesty. Podobně jako Diffserv je IntServ také mapován do MPLS sítě. RSVP zprávy jsou konvertovány do MPLS tunelu nebo do MPLS LSP cesty podobně jak je tomu v RSVP tunelování do IP tunelu.

Poslední verze MPLS obsahuje podporu RSVP signalizace, kde slouží LDP protokol (label distribution protocol) k sestavení LSP cesty skrze MPLS doménu. Zde se také vykonává explicitní směrování, což dovolí uzlům v DS síti sestavit LSP cestu s tím, že je tato procedura nezávislá na směrovacích protokolech 3 vrstvy. Proto nejsou tedy omezovány směrovací procesy .

4.6 MOŽNOSTI KONFIGURACE QOS PRO SMĚROVAČE CISCO

V tomto oddíle budou popsány možnosti konfigurace QoS na zařízeních od firmy Cisco. Jak bude popsáno v následujícím textu, takto se v praxi definují jednotlivé pravidla QoS a jejich konfigurace. Obvykle se konfigurace liší, podle použitého zařízení jiných firem. Směrovače CISCO jsou využity v praktické části práce a proto je zde uvedeno jakými možnostmi konfigurace disponují.

Souhrnné možnosti konfigurace se dají popsat [3]:

- MQC modulární řádkové rozhranní
- Metody podle klasifikace paketů
- Metody pro správu proti zahlcení
- Metody předcházení zahlcení
- Metody pro řízení přenosových politik a řízení rychlostí
- Metody pro signalizaci QoS
- QoS na fyzických linkách

4.6.1 MQC

Toto rozhranní je založeno na modelu DiffServ. Veškerý provoz se definuje prostřednictvím map tříd. Tyto mapy tříd se dále používají v mapách politik a tyto se pak aplikují na rozhranní směrovače. Mapy politik definují QoS pomocí značením provozu, správami zahlcení WFQ a LLQ, předcházením zahlcení WRED

4.6.2 Metody podle klasifikace paketů

Do této kategorie se řadí :

- Rozpoznávání síťových aplikací
- Směrování, které je založené na politikách
- Propagace QoS pomocí protokolu BGP
- QoS určené pro VPN

Do rozpoznávání síťových aplikací se řadí metoda NBAR. Tato metoda využívá databázi protokolů, které se mapují a následně aplikují politiky na rozhranní. Je možné ji využít i pro aplikace, které používají dynamické přidělování TCP a UDP portů. Tato metoda vyžaduje směrovač s funkcí CEF. Nelze ji použít na rozhranních, které používají šifrování nebo tunelování provozu.

Do druhé třídy se řadí metoda směrování PBR. Zde je možné provoz klasifikovat pomocí přístupových seznamů, nastavovat IP prioritu a směrovat jej na různá rozhranní. Pokud bude využita propagace QoS pomocí protokolu BGP, je možné politiky klasifikace propagovat do velkých sítí prostřednictvím aktualizací tohoto protokolu. Ve virtuálních privátních sítích lze provoz klasifikovat ještě před jeho zašifrováním nebo zapouzdřením. Klasifikace QoS se provádí na základě původní zdrojové a cílové IP adresy a čísel portů. V tomto případě jsou podporovány všechny typy tunelů jako je L2PT, IPSec, L2F, IP-in-IP, GRE.

4.6.3 Metody pro správu proti zahlcení

V tomto případě se do těchto metod zařazují:

- Metoda PQ prioritní fronty
- Metoda CQ vlastní fronty
- Metoda WFQ

V metodě PQ je provoz při odesílání rozdělen na rozhranní do čtyř prioritních skupin. Oproti tomu metoda CQ rozděluje provoz do skupin front a každá z těchto front obdrží poměrnou část kapacity rozhranní.

Metoda WFQ automaticky klasifikuje provoz do toků a každý z těchto toků obdrží váhu podle typu provozu. Provozy, které mají nejmenší objem, budou mít vyšší prioritu než provoz z velikým objemem. Vhodné zejména pro rychlé doručování nízkoobjemových interaktivních provozů. Existují i další typy metod, které vycházejí z kombinací předchozích jako je kupříkladu metoda CBWFQ apod.

4.6.4 Metody předcházení zahlcení

Do této skupiny se řadí metoda WRED. Tato metoda je založena na zahazování paketů, v případě zjištění začínajícího zahlcení. To vede ke snížení rychlosti vysílaných paketů na straně zdroje.

4.6.5 Metody pro řízení přenosových politik a řízení rychlosti

V této skupině jsou zařazeny tyto metody:

- CAR
- GTS
- FRTS

Při použití metody CAR je rychlost jak příchozího, tak i odchozího provozu omezována podle nastavených politik CAR. Zde je možné provoz identifikovat podle typu rozhranní, IP adres, klasifikace paketů, aplikací, nebo přístupových seznamů. Každá z definovaných politik má nastaveno pro specifikovaný provoz omezení rychlosti a dále také akce, které se mají vykonat při překročení rychlosti.

V metodě GTS je podobně jako v předchozí metodě možné odchozí provoz omezovat na rozhraní. Předchází se tak zahlcení provozu. Metoda FRTS je určena pro frame relay provoz a odchozí provoz na rozhranní je možné omezovat podle nastavení hodnoty CIR.

4.6.6 Metody pro signalizaci QoS

Do této metody se zařazuje jako jediná signalizace pomocí RSVP. Výsledkem je zaručená kvalita služeb po celé délce spojení. Je to metoda, při které směrovač žádá o rezervaci.

4.6.7 QoS na fyzických linkách

Zde se využívají mechanizmy pro efektivní využití linky. Využívá se zde mechanizmus LFI. Ten může upravit velikost přenášených paketů a řadit je v takovém pořadí aby data, která jsou kritická na čas jako je hlas, video atp. , byla vkládaná do datového toku se zaručenou prodlevou. Protokol CRTP komprimuje hlavičky a tím se snižuje režie těchto časově kritických paketů.

4.7 KONFIGURACE PRO SPOLUPRÁCI INTSERV A DIFFSERV SÍTÍ

Jak vychází z předchozího teoretického rozboru spolupráce architektur IntServ a DiffServ, nebo architektury DiffServ s jinými je možná. Jak lze toho dosáhnout pomocí konfigurace směrovačů CISCO popisuje následující kapitola. Možnosti jsou shrnuty následovně [13, 8].

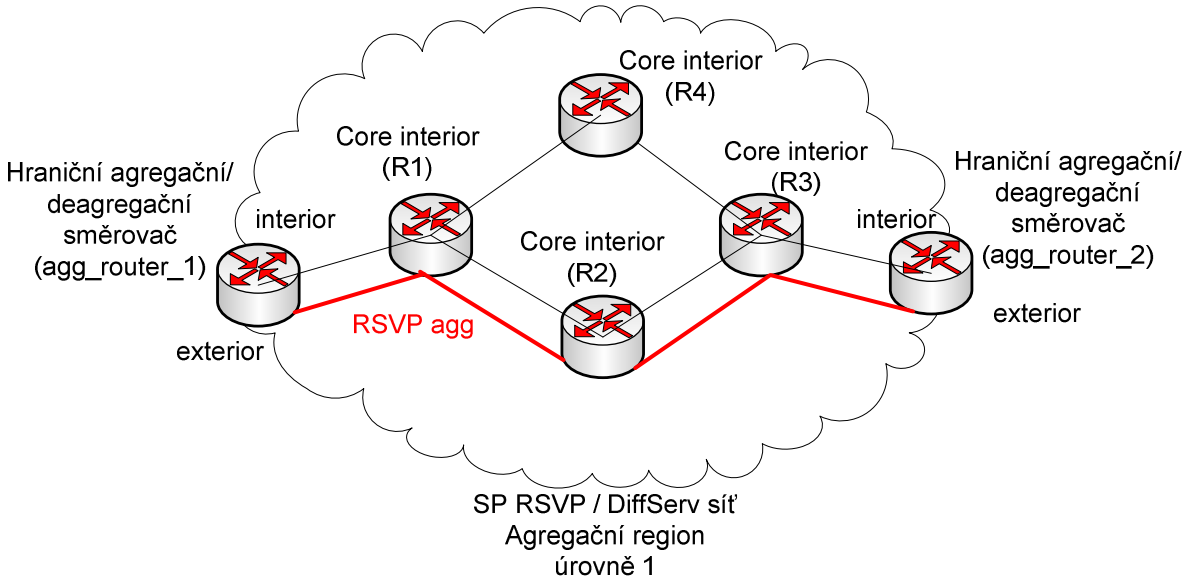
- RSVP Intserv / Agregace RSVP v DiffServ
- RSVP IntServ/DiffServ
- DiffServ / Nedefinované architektury

Pokud bychom chtěli prakticky dosáhnout spolupráce výše uvedených architektur, je nutné na směrovačích nakonfigurovat následující parametry:

- Konfigurace agregace RSVP – směrovače DiffServ domén, v případě spolupráce IntServ a DiffServ
- Konfigurace RSVP – směrovače IntServ domén, jednotné pro veškeré typy spolupráce s jinými doménami, které podporují RSVP.
- Konfigurace DiffServ – směrovače DiffServ domén, v jakémkoliv typu spolupráce.

4.7.1 Konfigurace agregace RSVP na směrovačích DiffServ domény

Pro zajištění agregace RSVP v DiffServ síti je nutné nakonfigurovat směrovače podle jejich umístnění v síti. [5] V této síti viz. Obrázek 4.9 se nacházejí hraniční směrovače, na kterých se konfigurují jejich rozhranní na straně DS. Rozhranní které slouží jako přístupové pro jiné sítě nese označení exterior. Rozhranní, které je na straně DiffServ sítě nese označení exterior.. Směrovače s označením Core interior jsou klasické směrovače s podporou agregace RSVP.



Obrázek 4.9: Agregace RSVP

4.7.1.1 Možnosti konfigurace fyzického rozhranní na směrovačích mimo agregační region (interface) :

- Aktivace RSVP na rozhranní směrovače:

interface *název a číslo*
ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*]

- Nastavení zdroje poskytovatele (poskytovatel QoS)

ip rsvp resource-provider none [**none** | **wfq-interface** | **wfq-pvc**]

- Deaktivování klasifikace paketových dat

ip rsvp data-packet classification none

- Konfigurace mapy politik a tříd:

class-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold**}] [**match-all** | **match-any**] *class-map-name*
match access-group { *access-group* | **name** *access-group-name* }

policy-map [**type access-control**] *policy-map-name*
class {*class-name* | **class-default**}
priority {*bandwidth-kbps* | **percent** *percentage*} [*burst*]

- Nastavení nakonfigurovaných politik a mapy na rozhranní:

interface *type numer*
service-policy [**type access-control**] {**input** | **output**} *policy-map-name*

4.7.1.2 Konfigurace fyzického rozhranní, které slouží jako agregační:

Tato konfigurace je použitá na rozhranní, kterého se týká vstup dat do agregačního regionu a používá se na všech směrovačů, které působí jako agregační:

interface typ číslo
ip rsvp aggregation role interior

- **Konfigurace mapování agregací na deagregačním rozhranní**

Typicky se používá na to samé rozhranní, které je agregační. Je to kvůli jednostranné orientaci RSVP rezervací. Většina aplikací vyžaduje oboustrannou orientaci. Proto se konfigurují tyto parametry, které jsou využívány během mapování dynamické E2E rezervace.

Nezbytným předpokladem je i nakonfigurování ACL listů, které definují skupinu RSVP koncových bodů, jehož rezervace budou agregovány na celkovou rezervaci podle DSCP hodnoty. Klasické RSVP rezervace jsou definované podle IP adresy a protokolu. V RSVP agregaci je identifikace prováděna podle IP adresy cíle a DSCP hodnoty definované v session_object v RSVP zprávě. E2E rezervace je namapována na zvláštní agregační RSVP sezení identifikované podle E2E rezervace ve zprávě session_object nebo v kombinaci session_object, filter_spec, sender_template.

- **Rozšířené ACL**

Zdrojová IP adresa a port obsažena v RSVP PATH zprávě odesílatele nebo RSVP RESV zprávě definované ve filter_spec, tj IP adresa zdroje nebo RSVP odesílatele.
Cílová IP adresa a port obsažená v RSVP PATH/RESV zprávě , tj. IP adrese cíle nebo RSVP příjemce.

- **Standard ACL**

Je použitá IP adresa zdroje, nebo RSVP odesílatele, obsažena v RSVP RESV zprávě.

ip rsvp **aggregation ip map** {**access-list** {*acl-number*} | **any**} **dscp** *value // říká směrovači jak má namapovat E2E rezervaci do agregační rezervace.*
příklad : ip rsvp aggregation ip map any dscp af41

- **Konfigurace agregačních atributů na deagregátorovi**

Většinou se jedná o stejné rozhranní jako agregační. Také se definuje (nazývá) jako token bucket parametr. Konfigurují se parametry rezervačních atributů.

ip rsvp aggregation ip reservation dscp *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*]
Příklad: **ip rsvp aggregation ip reservation dscp** af11 **aggregator** 192.168.2.1 **traffic-params static rate** 10 **burst** 8 **peak** 10

- **Konfigurace ID identifikace agregačního směrovače**

interface *loopback [number]*
ip address *ip-address subnet-mask/prefix*

- **Aktivace RSVP agregace**

Globální povolení agregace , pokud jsou nastaveny předchozí konfigurace.

Pokud bude aktivováno globální RSVP i na interních směrovačích, je potřeba všechny rozhranní nakonfigurovat jako interní (interior)

ip rsvp aggregation ip

4.7.2 Konfigurace RSVP

RSVP je nutné v různorodých sítích provozovat společně s metodou WRED nebo WFQ [3, 2] RSVP zprostředkuje rezervaci a metody poté provádí implementaci rezervace. Dále je nutné provozovat rozhraní v režimu full duplex.

- Zapnutí RSVP na rozhranní

ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*]

- Požadavky na rezervaci přijímané pouze od určité stanice

ip rsvp neighbors *access-list-number*

- Simulace rezervací v případě pokud nemáme software, který generuje RSVP zprávy

ip rsvp reservation *session-ip-address sender-ip-address* [**tcp** | **udp** | *ip-protocol*] *session-dport sender-sport next-hop-ip address nexthop-interface* {**ff** | **se** | **wf**} {**rate** | **load**}[*bandwidth*] [*burst-size*]

- Simulace RSVP-PATH

K simulaci této zprávy od vysílače k přijímači použijeme následující příkaz, v případě, že nemáme software podporující RSVP. Konfiguračně podobné ip rsvp reservation.

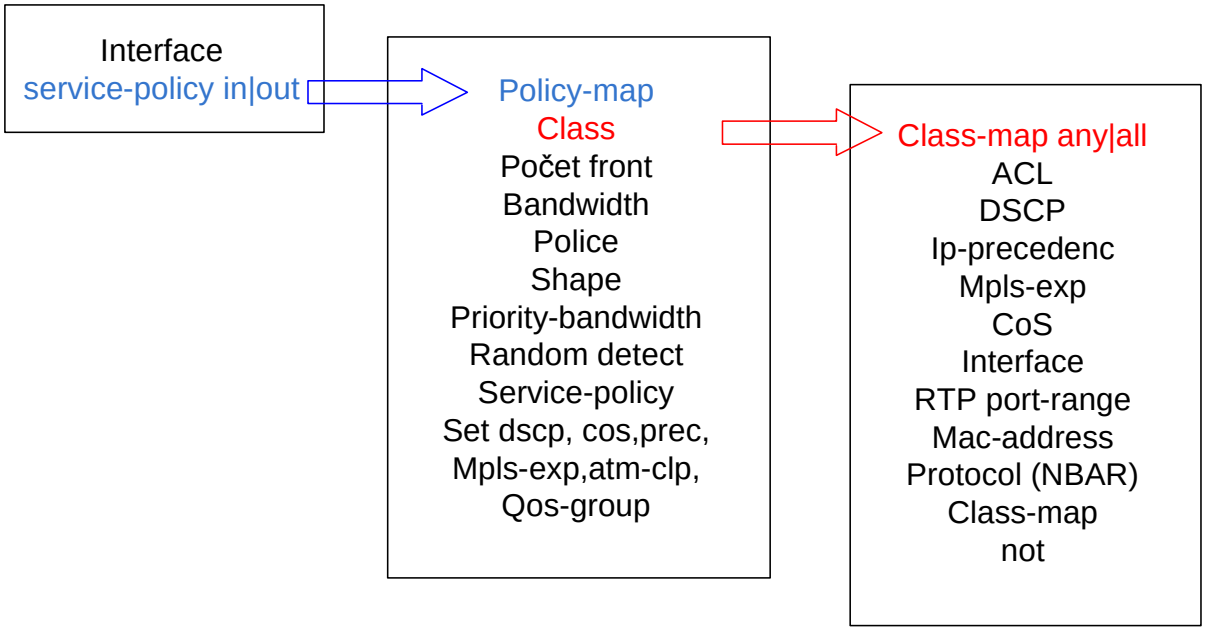
ip rsvp sender *session-ip address [tcp | udp | ip-protocol] session-dport sender-sport previous-hop-ip-address previous-hop-interface [bandwidth] [burst-size]*

4.7.3 Konfigurace DiffServ

Konfigurace DiffServ sítě je velice modulární záležitostí. Záleží jak danou síť navrhneme a jaké politiky chceme využívat pro provoz sítě. Schématický celek viz Obrázek 4.10 shrnuje možnosti modulární CLI konfigurace, které budou využity v emulaci sítě v DiffServ doméně.

Jedná se o modulární sadu nástrojů pro konfiguraci klasifikace a označování paketů, nastavení politik a třídění provozu, využití token-bucket , konfiguraci front s diferencovanou obsluhou a obrany před zahlcením. Pro restrikci provozu je využito funkce NBAR. (Network Based Application Recognition). Rozpoznává dynamicky přidělená čísla TCP/UDP portů pro známé protokoly. Takto můžeme lehce alokovat protokol RSVP, který je defaultně podporován touto metodou.

Tímto nástrojem se dá řídit http provoz podle URL adresy, HOST a MIME. Umožňuje funkcí Protocol Discovery analyzovat provoz. Při využití NBAR je nutné zapnout na směrovačích funkci CEF. (Cisco expres forwarding). NBAR je součástí MQC pro platformy 7200, 7100, 3600 a 2600



Obrázek 4.10:Modulární konfigurace DiffServ

5 PRAKTICKÁ ČÁST

Praktická část sestává z konfigurace QoS na směrovačích Cisco [1] a z vytvoření síťové topologie v programu GNS3 pro emulaci provozu sítě DiffServ. Zaměřuje se především na možnosti mapování, překlad provozu na hraničních směrovačích a na test kvality hlasového provozu v navržené konfiguraci sítě. V závěru jsou porovnány dosažené výsledky emulovaného provozu v závislosti na parametrech definovaných QoS konfigurací.

V případě konfigurace IntServ RSVP, její možnosti byly popsány v teoretické části. Z praktického hlediska se nepodařilo zajistit generování RSVP zpráv pomocí žádného klienta, ani daemona pod linuxem. Konfigurace simulovaných RSVP zpráv přímo na směrovači pro testovací účely vyžadují stejné odchozí i příchozí porty aplikace a data typu UDP nebo TCP. Jinak se tyto rezervace „nenamapují“. RSVP kupříkladu nepočítá v praxi s kompresí hlaviček RTP. RSVP v implementaci s CISCO směrovači naváže hovor i v případě nedostatku zdrojů sítě. RSVP zprávy jsou zasílány až po počatém hovoru, popřípadě se tyto zprávy nezasílají vůbec. RSVP zprávy se využívají ve specifických případech. Bylo zjištěno, že se v některých produktech od RSVP upustilo. Pro zajímavost firma TANDBERG ve svých nových výrobcích protokolu RSVP nevyužívá. RSVP protokol byl kupříkladu obsažen v H323 ve verzi 1, nebo v programu NetMeeting v operačním systému Windows 98 , jak je uvedeno v podpoře MSDN firmy Microsoft.

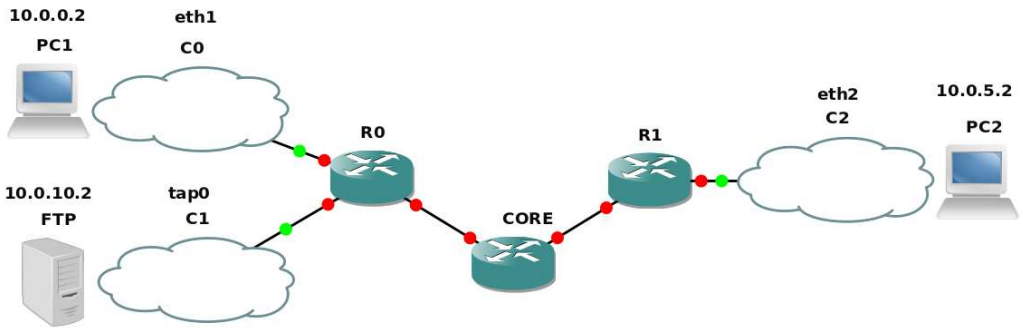
V praktické části je tedy provedena konfigurace nejzajímavější možnosti spolupráce sítě IntServ a DiffServ tj. agregace RSVP a vyhodnocení mapování RSVP. Měření parametrů QoS s využitím RSVP nebylo možné uskutečnit z důvodu absence operačního systému, či VoIP zařízení, které by jej podporovalo. Dále byla nakonfigurována DiffServ síť s následným vyhodnocením jednotlivých provozních parametrů této sítě.

5.1 MODEL SÍTĚ, SW A HW VYBAVENÍ

Pro testovací účely byly vytvořeny dva modely sítě v programu GNS3 [5]. Tento program slouží k emulaci sítě a využívá reálného operačního systému IOS od firmy CISCO. Pracuje na způsobu, jakým jsou například emulovány jiné operační systémy běžící nad hostitelským operačním systémem. Jedná se o freeware, což je jeho jistá výhoda. První vytvořený model sítě v tomto prostředí slouží pro spolupráci IntServ /

DiffServ a druhý pro testovací účely QoS a jeho vyhodnocení v případě použití DiffServ sítě.

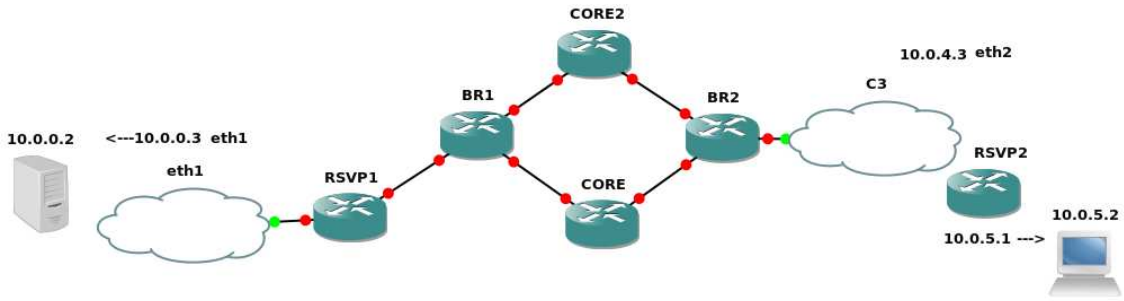
Hlavní část, tedy emulace sítě je spuštěna na počítači, na kterém je nainstalován operační systém Linux UBUNTU, který již v nabídce instalací obsahuje výše zmíněný software GNS3. V případě testování QoS v DiffServ síti jsou k tomuto počítači připojeny další dva počítače, které přistupují jako klienti sítě. Na jednom z těchto počítačů a to na PC1 běží software pro vyhodnocení kvality sítě. Obrázek 5.1 Dalším prvkem sítě je emulovaný počítač, zprovozněn pomocí programu Sun xVM VirtualBox na kterém je spuštěn FTP server .



Obrázek 5.1:Model sítě z programu GNS3 pro vyhodnocení parametrů DiffServ sítě

V modelu sítě, vytvořeném v programu GNS3 viz Obrázek 5.1 figurují směrovače R0 a R1 jako hraniční směrovače, které zajišťují značení a třídění paketů podle hodnoty DSCP. Směrovač CORE je konfigurován jako klasický směrovač a pouze předává daný provoz. C0, C1 a C2 jsou emulované propojení na fyzické síťové karty.

V dalším modelu sítě viz. Obrázek 5.2, který slouží pro ověření spolupráce architektur IntServ a DiffServ s využitím agregace RSVP, vystupují směrovač BR1 a BR2 jako hraniční směrovače DiffServ domény. Zde se konfiguruje agregace a deagregace RSVP. Směrovače RSVP1 a RSVP2 slouží ke generaci RSVP zpráv. Směrovač RSVP2 je reálný směrovač Cisco 1841. Dále jsou zde opět prvky C (C3, eth1), které emulují propoj na fyzické síťové karty, ke kterým jsou připojeny počítače. Ty tvoří opět přístupové prvky sítě.

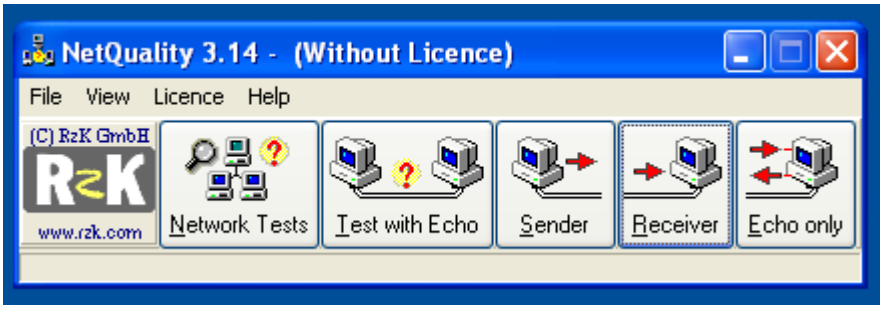


Obrázek 5.2: Model sítě v programu GNS3 pro kontrolu mapování RSVP

Realizace agregace RSVP lze uskutečnit na směrovačích řady c7200 a výše s číselnou řadou verze IOS 12.33. Jsou využity i pro síť DiffServ. K emulaci prostředí sítě program GNS3 dále využívá dva podpůrné programy. Těmi jsou program Dynamips a program Pemu [5], které jsou nezbytnou funkční součástí programu GNS3. K měření hodnot sítě, vyhodnocení správného mapování a parametrů sítě je využito programu NetQuality a Wireshark.

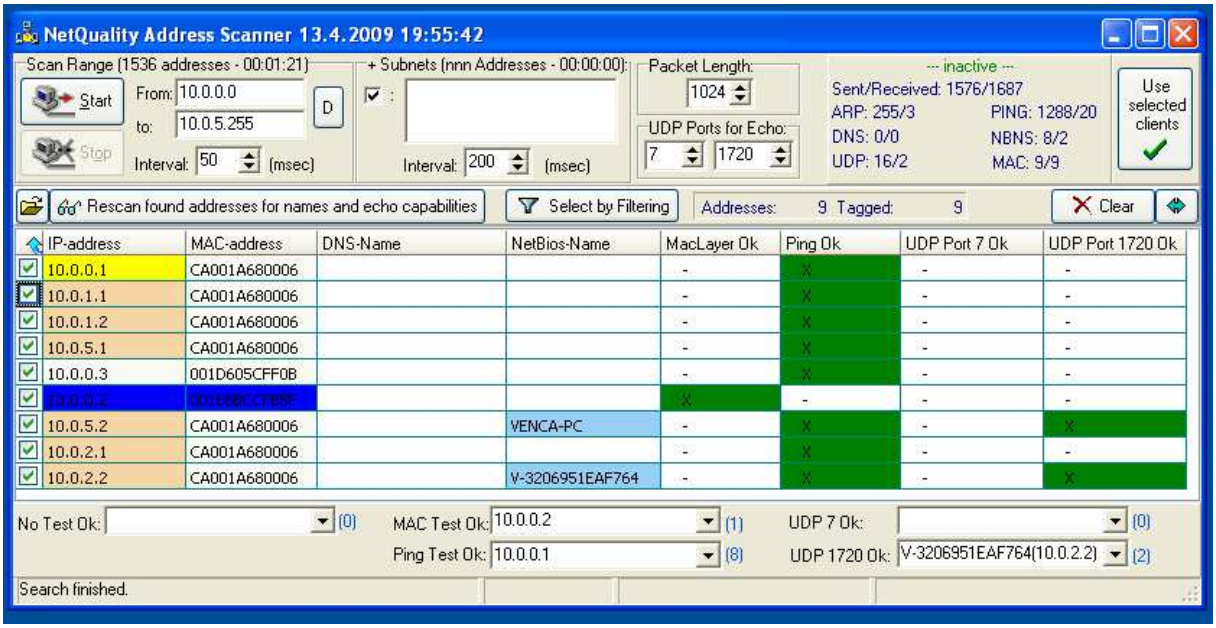
5.1.1 NetQuality

NetQuality je program z rozsáhlého souboru programů firmy RZK [10]. Je určen pro měření VoIP kvality přenosu pod Windows XP a Vista. Využívá nadefinovaných kodeků VoIP telefonie ke generování testovacích dat. NetQuality viz. Obrázek 5.3 je využit jako server a na druhé straně je použit NetQuality klient viz. Obrázek 5.5 . Proud vysílaných RTP dat je potom vyhodnocen NetQuality serverem.

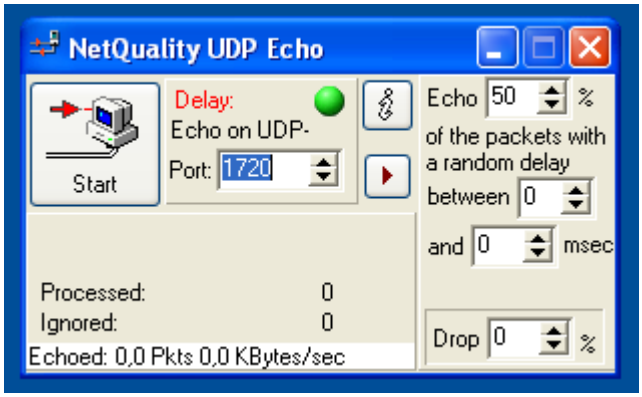


Obrázek 5.3: „NetQuality“ základní ovládací panel

Pomocí funkce „Network Tests“ prohledáme síť, tak abychom namapovali počítač na kterém je puštěn NetQuality klient viz Obrázek 5.4. Po tomto prohledání sítě již můžeme nadefinovat typ testu, který chceme provést, a následně jej spustit pomocí funkce Sender. Více o nastavení , provozu a výstupech tohoto programu v odkazu na internetových stránkách prodejce [10].



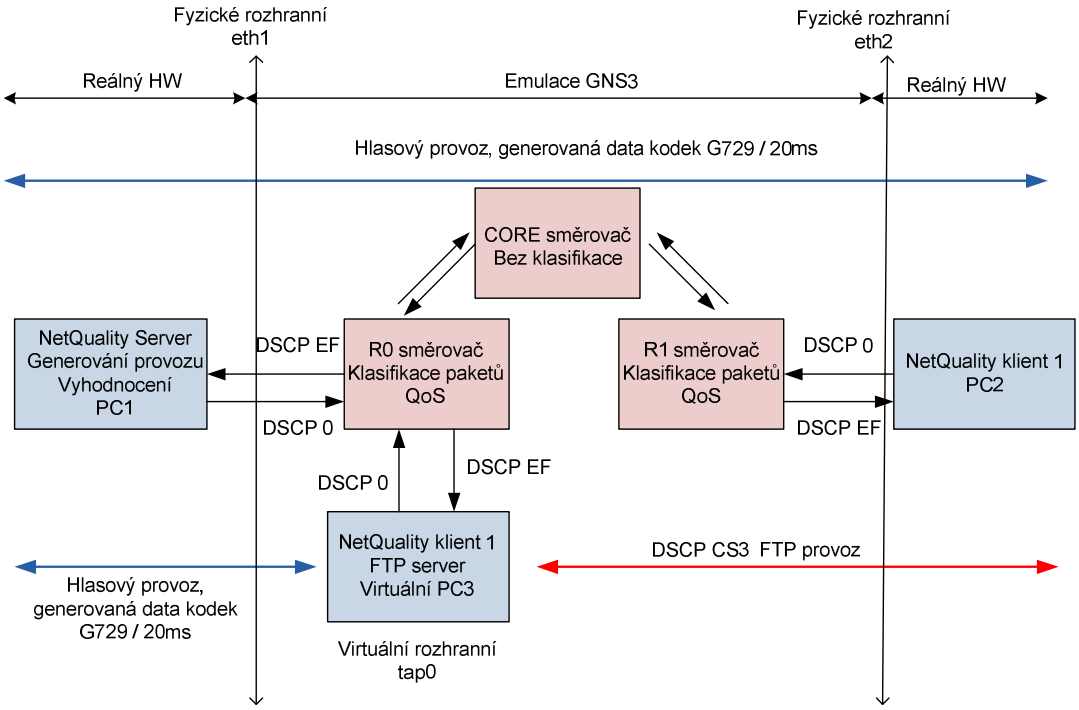
Obrázek 5.4: Výsledky skenované sítě programem NetQuality



Obrázek 5.5: NetQuality klient

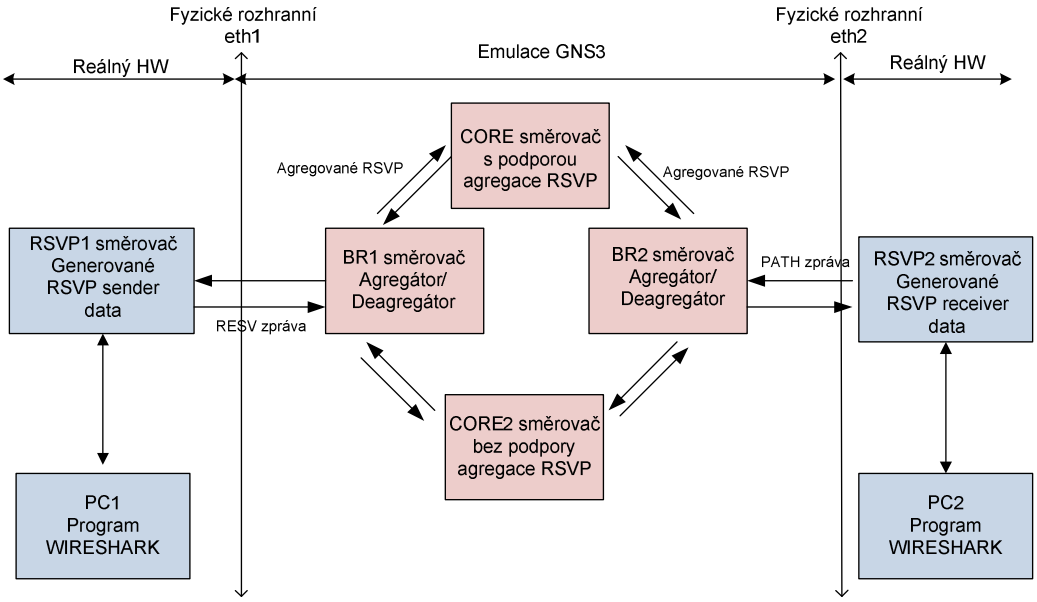
5.1.2 GNS3, nastavení rozhranní v UBUNTU Linux, parametry testů

V případě využití DiffServ domény jako páteřní sítě probíhá komunikace v režimu, kdy aplikace zasílají svá data s hodnotou DSCP 0 a hraniční směrovače definují QoS pro tyto data podle zadané konfigurace Obrázek 5.6. Program Wireshark je spuštěn za směrovačem R0 směrem ke směrovači R1. Na tomto spoji je implementováno QoS.



Obrázek 5.6: Klasifikace a rozdělení provozu v DS doméně

V případě testů pro ověření funkce agregace RSVP zpráv v DiffServ doméně je využito směrovačů RSVP1 a RSVP2 ke generování RSVP zpráv. Tyto RSVP zprávy by měli být mapovány podle konfigurace BR1 popřípadě BR2 směrem ke směrovači CORE, který podporuje agregaci RSVP viz. Obrázek 5.7



Obrázek 5.7: Agregace RSVP

- **Ethernetové propojení**

Všechny ethernetová rozhranní mají nastavenu rychlost 100 Mbit/s full duplex.

Přes vytvořené virtuální rozhranní tap0 v linuxu je připojený virtuální operační systém propojený do emulované sítě GNS3. Další počítače jsou připojeny přes fyzické rozhranní počítače s OS Linux přes emulovaný spoj v GNS3 směrem do okrajových směrovačů.

Aby bylo možné se připojit z virtuálního počítače na síť vytvořenou v programu GNS3, je nutné nakonfigurovat v OS Linux virtuální rozhraní. Je potřebné stáhnout podle verze balíček nástrojů uml-utilities zadáním příkazu „*apt-get install uml-utilities*“. Ta obsahuje funkci *tunctl,* která umožní emulaci virtuálních síťových karet. Následující postup je použit v konzoli linux serveru:

$ sudo modprobe tun
$ sudo tunctl –t tap0
$ sudo ip addr add {ip adresa}/{maska} dev tap0
$ sudo ip link set dev tap0 up

- **Parametry testovaných dat v testu DS domény.**

Pomocí programu NetQuality je proveden vždy 10x opakovaný 10 sekundový přenos dat ve formátu rámce G729 paketu s opožděním 20 milisekund. V první fázi bez QoS a

FTP přenosu, dále s FTP přenosem a naposledy s nadefinovanými QoS. A to také s FTP a bez FTP přenosu. S QoS je proveden test s nakonfigurovanými parametry MQC NBAR s WFQ, AutoQoS a jako poslední priority ip . Pro přenos generovaných dat programem NetQuality jsou využity čísla portu 1720. Tento typ portu využívá i H323. Na FTP serveru jsou uložena binární data o velikosti 389 MB, která jsou určena jako přídavná zátěž.

.

5.2 REALIZACE A VÝSLEDKY MĚŘENÍ

5.2.1 Testy provozu DS domény bez využití QoS parametrů

Tento test je proveden, aby bylo možné porovnat výsledky tohoto testu s výsledky testů s QoS. Na směrovačích nebylo nakonfigurováno žádné QoS. Test je proveden bez FTP zátěže, kdy v síti běží pouze hlasový provoz a dále s FTP zátěží.

Tabulky měření obsahují následující údaje:

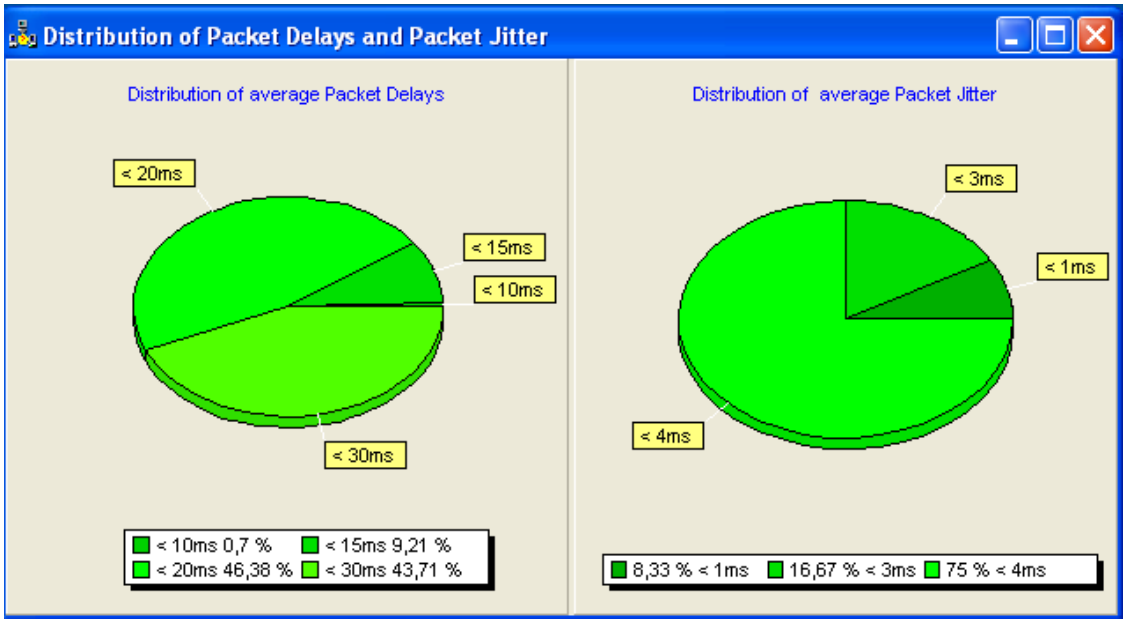
- Počet simulovaných hovorů v rámci jednoto testu
- Ztráta rámců – ztracené rámce při přenosu v testu
- Ztráta (údaj Loss) v % - ztráta rámců v procentech
- Počet simulovaných hovorů v rámci jednoto testu
- Ztráta rámců – ztracené rámce při přenosu v testu
- Ztráta (údaj Loss) v % - ztráta rámců v procentech
- Pseudo ztráta - ztráta paketů na straně odesílatele. Nastává při velké hodnotě zpoždění, v tom případě pakety dorazí mimo čas, který kodek akceptuje
- Pseudo ztráta v % - procentuální vyjádření pseudo ztráty
- Průměrné zpoždění – průměrné zpoždění paketů v milisekundách
- Maximální zpoždění - maximální zpoždění paketů v milisekundách
- Maximální jitter – maximální hodnota jitteru v milisekundách
- Diference – diference paketů
- Adresa – adresa UDP echo klienta
- Hodnota DSCP / TOS

Z výsledku je viditelné viz. Tabulka 5.1, jak FTP provoz ovlivnil kvalitu přenosu hovoru. FTP přenos vykazoval 641 kbit/s a při spuštění testu hovorů se snížil na přenosovou rychlost 182 kbit/s.

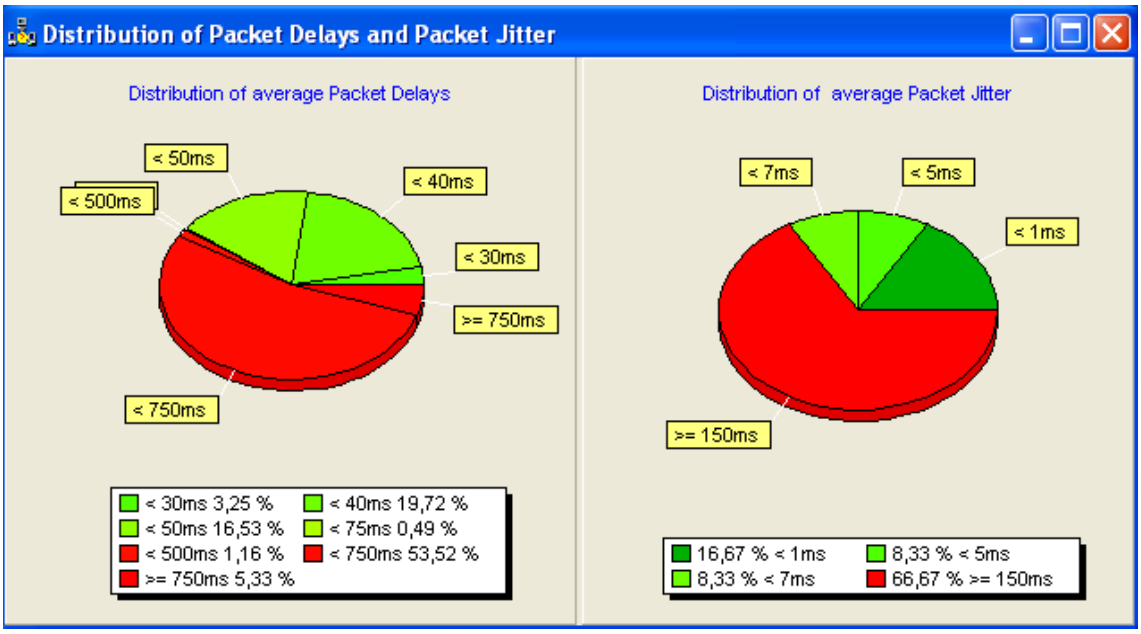
Program NetQuality umožňuje i grafický výstup měřených dat viz.Obrázek 5.8. Pro testovací účely byly vybrány výstupy paketového zpoždění a hodnoty jitter. Zelené znázornění ukazuje vyhovující hodnotu jitter a paketového zpoždění. Červené hodnoty jsou již nevyhovující viz. Obrázek 5.9. Jsou to hodnoty pro paketové zpoždění přesahující čas 100 ms a jitter přesahující 40 ms, což jsou zvolené hodnoty přednastavéné pro použitý kodek.

Tabulka 5.1: Výsledky provozu bez QoS

Typ testu	Typ paketu	Počet hovorů	Ztráta %	Pseudo ztráta%	Průměrné zpoždění	Max zpoždění	Avrg jitter	Max jitter	DSCP TOS	Diff
Bez FTP	G.729 (20ms)	7	0,0	0,0	9	21	1	12	0	0
S FTP	G.729 (20ms)	7	0,4	0,8	325	355	20	253	0	20



Obrázek 5.8: Grafický výsledek bez FTP přenosu a bez QoS

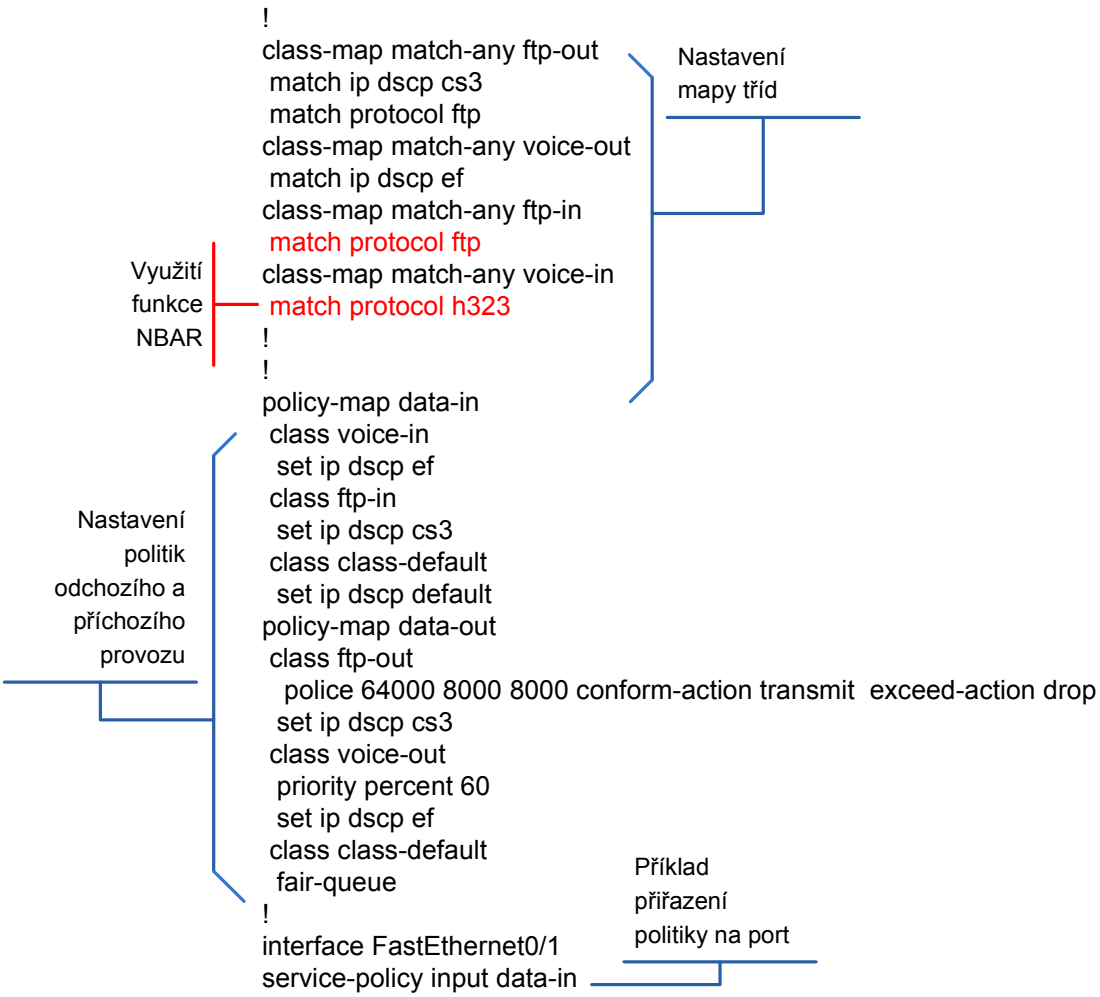


Obrázek 5.9: Grafický výsledek s provozem FTP bez QoS

5.2.2 Testy s využitím QoS parametrů v DS doméně

- **QoS MQC s NBAR, WFQ a LLQ**

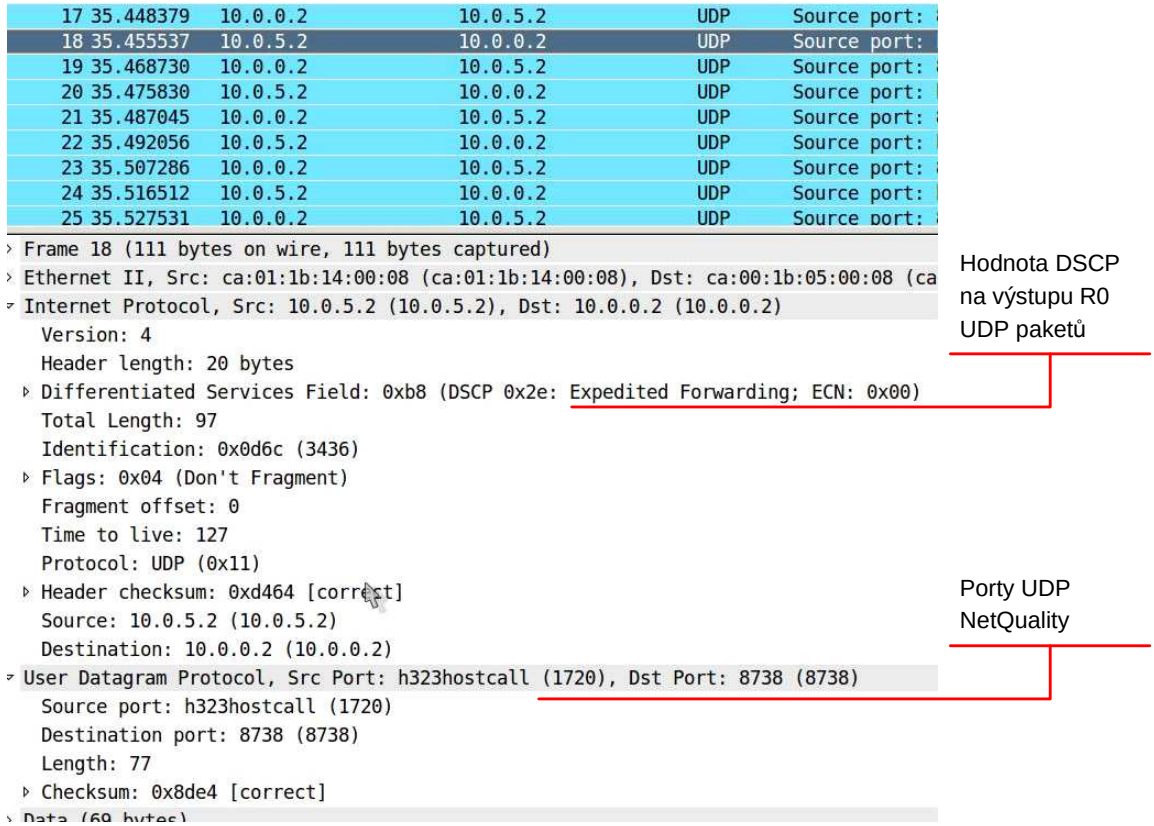
Jako první byl proveden test s nastavením MQC QoS použité jak na příchozí tak i na odchozí porty hraničních směrovačů. Hlasový provoz byl zařazen do třídy voice a FTP provoz do třídy FTP. Další provoz byl mapován jako „default“. Politiky byly nastaveny tak, že provoz z programu NetQuality měl hodnotu dscp ef, tj. expedited forwarding a na výstupu byla implementována striktní prioritní fronta s WFQ a LLQ. Provoz FTP měl nastavenu hodnotu DSCP na cs3 a na výstupu byl omezen na hodnotu 64 kbit/s se špičkovou hodnotou 8000 bajtů viz. Obrázek 5.10.



Obrázek 5.10: Konfigurace hraničních směrovačů.

Tato konfigurace výrazně zlepšila hodnoty hlasového provozu viz. Tabulka 5.2 při současném ftp provozu. Hodnota ftp přenosu vykazovala 7,6 kbajtů / s což odpovídá nastavené hodnotě v bitech. Mapování provozu bylo ověřeno programem Wireshark viz. Obrázek 5.11

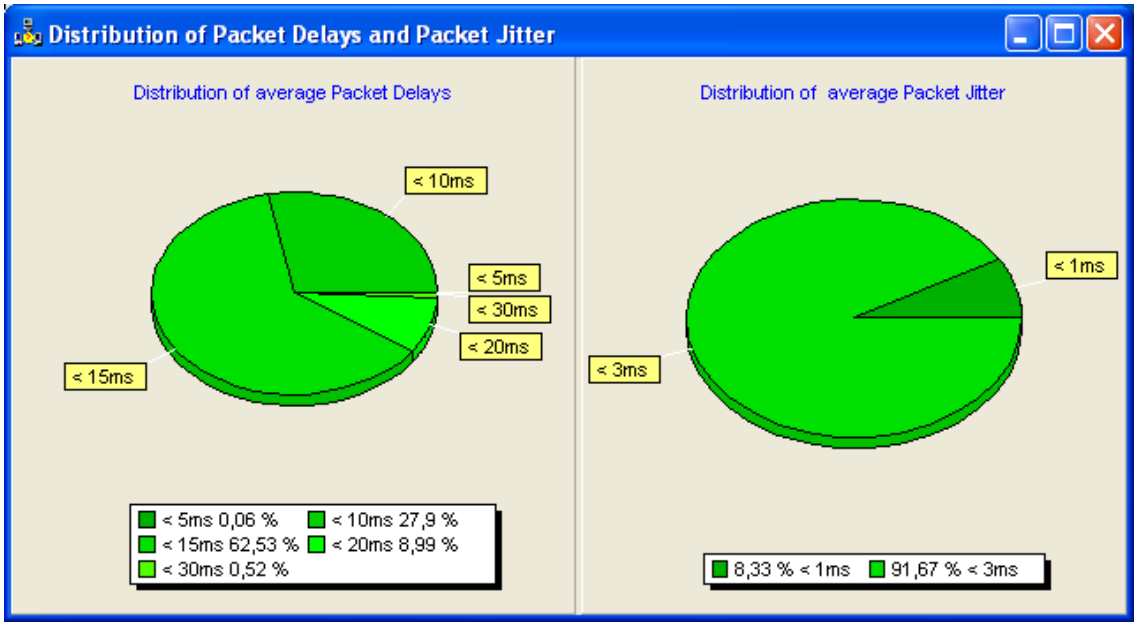
Z grafického výstupu programu NetQuality viz. Obrázek 5.12 je zřejmé dodržení parametrů pro použitý kodek. Hodnota jitteru se pohybovala v průměru 3 ms a hodnota paketového zpoždění v průměrném zpoždění 15 ms na datový rámec.. Porovnání výsledků je graficky zpracované v závěrečné části.



Obrázek 5.11: Ověření hodnoty DSCP

Tabulka 5.2: Výsledky provozu s QoS MQC

Typ testu	Typ paketu	Počet hovorů	Ztráta %	Pseudo ztráta%	Průměrné zpoždění	Max zpoždění	Avrg jitter	Max jitter	DSCP TOS	Diff
Bez FTP	G.729 (20ms)	7	0,0	0,0	10	20	1	10	ef	0
S FTP	**G.729 (20ms)**	**7**	**0.0**	**0,8**	**11**	**22**	**2**	**11**	**Ef Cs3**	**0**

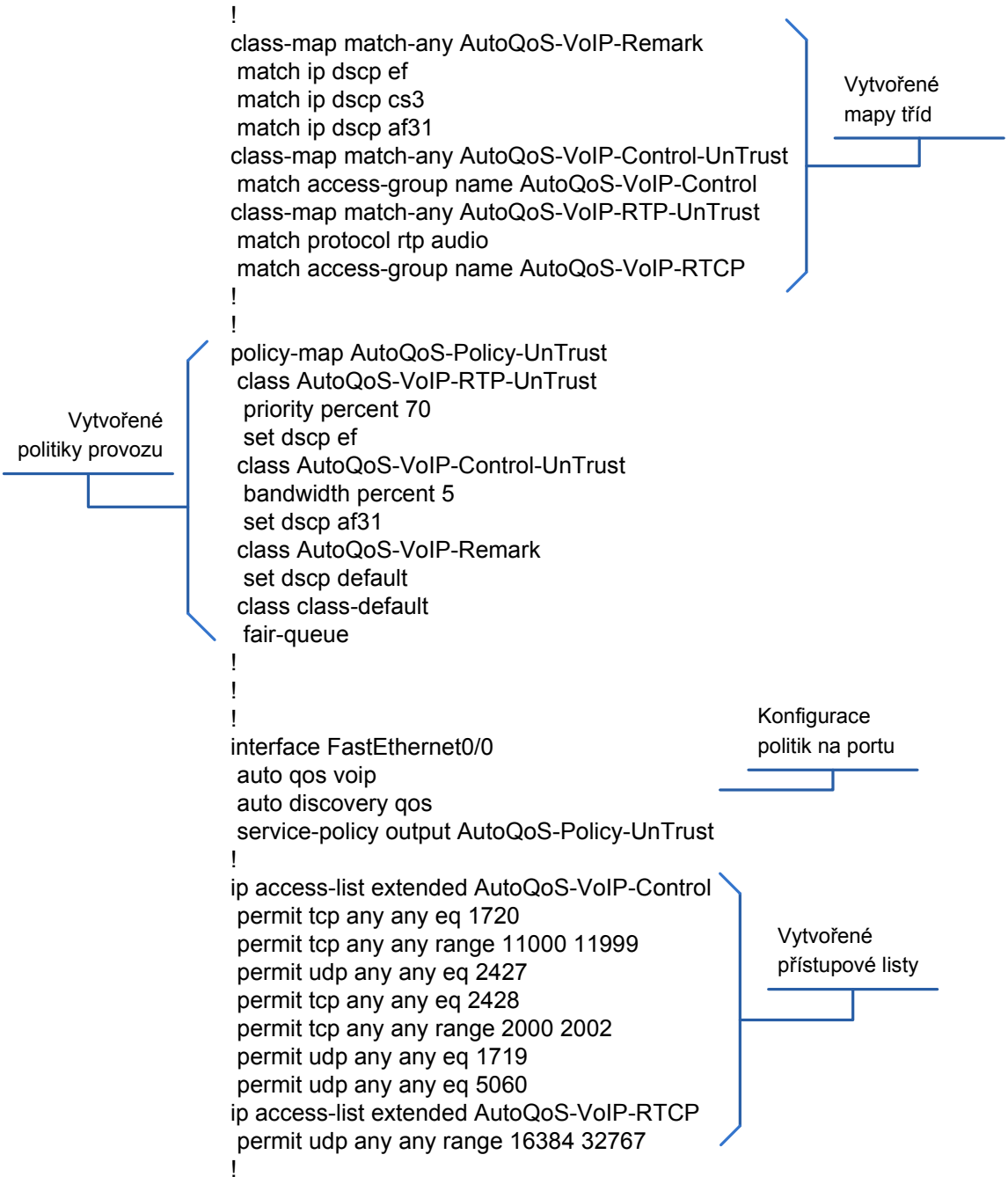


Obrázek 5.12: Výsledky provozu s QoS MQC s FTP přenosem

- **AutoQos v DS doméně**

Další konfigurací pro porovnání testů byla použita funkce AutoQoS VoIP. Je obsažena přímo ve směrovačích CISCO a stačí ji vyvolat v konfiguraci síťového rozhranní příkazem „auto qos“. Všechny parametry se předdefinují sami viz. Obrázek 5.13. přímo operačním systémem IOS. V tomto testu byly zachovány všechny předchozí nastavení a hraniční směrovače byly překonfigurovány touto funkcí QoS. Směrovač CORE neobsahuje QoS konfiguraci. Předává pouze provoz na základě hodnoty DSCP pole.

V tomto případě byly výsledky podstatně horší viz. Tabulka 5.3, protože parametry FTP provozu nebyly nakonfigurovány podle našich požadavků. Konfigurace FTP ovlivnila hlasový provoz více, než v předchozím případě, protože FTP provoz byl mapován do třídy „default“ a neměl omezené přenosové pásmo. Opět vše bylo tříděno do prioritních front s WFQ a LLQ a podle vytížení byla hlasovému provozu přidělovaná hodnota DSCP pole.



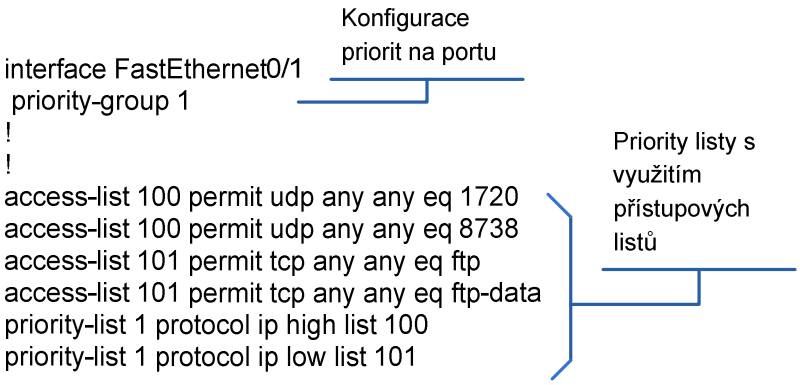
Obrázek 5.13: AutoQoS konfigurace

Tabulka 5.3: Provoz s AutoQoS

Typ testu	Typ paketu	Počet hovorů	Ztráta %	Pseudo ztráta%	Průměrné zpoždění	Max zpoždění	Avrg jitter	Max jitter	DSCP TOS	Diff
Bez FTP	G.729 (20ms)	7	0,0	0,0	10	31	2	21	Af31	0
S FTP	G.729 (20ms)	7	0.0	0,12	125	212	9	32	ef 0	40

- **Prioritní fronty**

Jako poslední byla odzkoušena konfigurace PQ prioritních front. Tyto prioritní fronty nastavují jednotlivým typům provozu priority. Provoz s vyšší prioritou se odesílá před provozem s nižší prioritou. Data jsou řazena do čtyř front: high, medium, normal a low. Každá fronta se přenáší tak dlouho, než je vyčerpaná a poté dojde k přenosu fronty s prioritou nižší. V tomto případě měl nakonfigurován hlasový provoz hodnotu high a ftp přenos hodnotu low viz Obrázek 5.14.



Obrázek 5.14: Konfigurace prioritních front

Při testu byla obsluhována jako první data hlasová, která se přenášela v jednotlivých sekvencích. Tyto hlasová data byla rozdělena do více front. Mezi jednotlivými frontami hlasového provozu byl obsluhován FTP. Tento fakt ovlivnil výsledek, ale s překvapením měla tato konfigurace lepší výsledky jak AutoQoS VoIP viz. Tabulka 5.4

.

Tabulka 5.4: Výsledky prioritních front

Typ testu	Typ paketu	Počet hovorů	Ztráta %	Pseudo ztráta%	Průměrné zpoždění	Max zpoždění	Avrg jitter	Max jitter	DSCP TOS	Diff
Bez FTP	G.729 (20ms)	7	0,0	0,0	11	30	2	19	0	0
S FTP	G.729 (20ms)	7	0.0	0,08	115	131	7	24	ef 0	0

5.2.3 Test agregace RSVP zpráv v DS doméně.

Tento test sloužil k ověření teoretických předpokladů spolupráce IntServ sítě a DiffServ sítě, neboli k ověření možnosti RSVP rezervací v DIffServ doméně. DiffServ síť byla použita jako transportní síť pro RSVP rezervace. Na směrovačích byly použity konfigurace dle kapitoly 4.7. Směrovače BR1 a BR2 měli roli agregátorů a deagregátorů RSVP rezervací.

Rezervace prostředků na směrovačích byly ověřovány přímo výpisem na směrovačích. Směrovače RSVP1 a RSVP2 generovali RSVP zprávy typu RSVP RESV a RSVP PATCH. Směrovač BR1 a BR2 generovali RSVP zprávy typu RSVP AGG, které zajišťovali agregaci RSVP rezervací. Směrovač CORE mapoval agregované RSVP podle hodnoty DSCP do kterého se mapovali tyto RSVP zprávy.

- Úspěšná signalizace E2E rezervací a agregace na směrovači BR1 aktuálním výpisem na směrovači:

```
BR1# show ip rsvp aggregation ip

RFC 3175 Aggregation:  Enabled
Level: 1
Default QoS service: Controlled-Load

Number of signaled aggregate reservations:  2
Number of signaled E2E reservations:        2
Number of configured map commands:          1
Number of configured reservation commands:  2
```

Pokud byly nakonfigurovány porty jako porty agregačního regionu, na směrovačích BR1, BR2 a CORE byla přiřazena jejich role jako interní, patřící do agregačního regionu, nebo externí, patřící mimo agregační region.

- Aktuální výpis portů na směrovači BR1:

```
BR1# show ip rsvp aggregation ip interface

Interface Name       Role
-------------------- --------
FastEthernet0/0      interior
FastEthernet0/1      exterior
FastEthernet1/0      interior
```

Rezervace RSVP se opět potvrdili na výpisech směrovačů. V našem případě šlo o dvě nakonfigurované rezervace ze směrovače RSVP1 na směrovač RSVP2. Podle určeného DSCP se namapovali do jednoho agregovaného toku mezi BR1 a BR2, položka AGG.

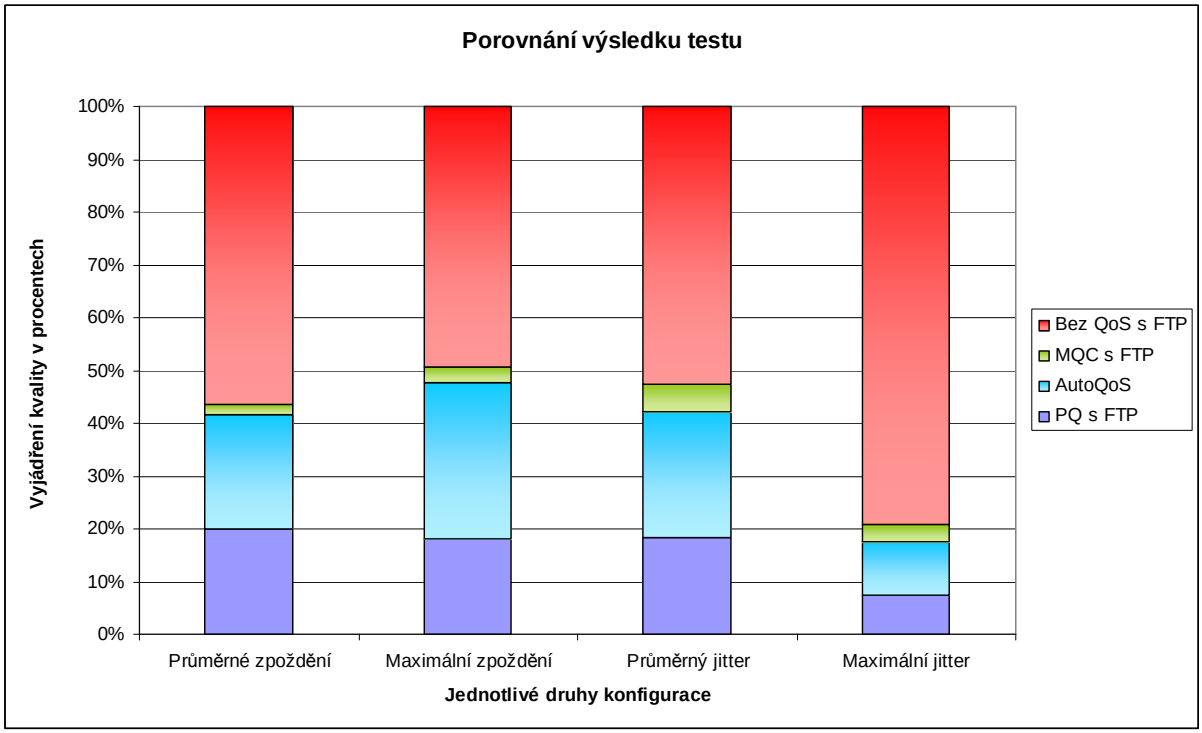
- Výpis mapování a rezervace agregace mezi agregátorem a deagregátorem

```
BR1# show ip rsvp aggregation ip endpoints detail

Role  DSCP Aggregator      Deaggregator    State  Rate    Used    QBM
PoolID
----- ---- --------------- --------------- ------ ------- ------- ------
----
Agg   46      10.10.10.2         10.10.10.4        ESTABL 100K    100K
0x00000003
Agg   46      10.10.10.2         10.10.10.4        ESTABL 10K     10K
0x00000003

   Aggregate Reservation for the following E2E Flows (PSBs):
To            From          Pro DPort Sport  Prev Hop       I/F      BPS
10.10.10.4    10.10.10.2    UDP 8000  8000   10.0.1.2     Et0/1     100K
10.10.10.4    10.10.10.2    UDP 8001  8001   10.0.1.2      Et0/1     10K

   Aggregate Reservation for the following E2E Flows (RSBs):
To            From          Pro DPort Sport  Next Hop       I/F      Fi
Serv BPS
10.10.10.4    10.10.10.2    UDP 8000 8000    10.10.10.3     Et1/0    FF
RATE 100K
10.10.10.4    10.10.10.2    UDP 8001 8001    10.10.10.3     Et1/0    FF
RATE 10K

   Aggregate Reservation for the following E2E Flows (Reqs):
To            From          Pro DPort Sport  Next Hop       I/F      Fi
Serv BPS
10.10.10.4    10.10.10.1    UDP 8000 8000    10.0.1.2       Et0/1    FF
RATE 100K
10.10.10.4    10.10.10.1    UDP 8001 8001    10.0.1.2       Et0/1    FF
RATE 10K
```

5.2.4 Souhrn výsledků testů

- **Test QoS v DiffServ síti**

V testu, kde se testovali vlastnosti DiffServ domény, dopadla nejlépe ruční konfigurace politik přenosu dat, ve kterém byl upřednostněn hlasový provoz. Jak je vidět na obrázku viz. Obrázek 5.15 konfigurace ovlivnili hodnoty přenosu dat z přístupové sítě a příslušně zlepšili hlasový provoz na úroveň, kdy nebyla ovlivněna jeho kvalita.



Obrázek 5.15: Výsledky testů

- **Test agregace RSVP v DiffServ síti**

V tomto testu se potvrdila možnost spolupráce obou architektur IntServ a DiffServ. Síť DiffServ sloužila jako tranzitní síť. Podařilo se provést rezervaci zdrojů agregací RSVP rezervací v DiffServ doméně.

Ověření jednotlivých parametrů kvality přenosu nebylo prováděno a to z důvodu uvedených v úvodu praktické části. Nepodařilo se vést datový provoz těmito vytvořenými rezervacemi. Aplikace měnily dynamicky přidělované porty, což nekorespondovalo se statickou konfigurací rezervací na směrovačích RSVP1 a RSVP2 .

ZÁVĚR

K hlavní výhodě technologie IntServ patří to, že umožňuje rezervaci prostředků bod – bod v IP sítích. Mezi jistou nevýhodu technologie IntServ jsou vysoké nároky na směrovače, které vykonávají velice paměťově náročné operace. Musí podporovat rezervaci síťových zdrojů protokolem RSVP, nebo jiným rezervačním protokolem. Směrovače uvnitř IntServ domény musí být schopné zpracovat veliké množství dat. Je zde podmínka orientace RSVP protokolu na příjemce, který musí inicializovat rezervaci zdrojů. RSVP selhává pokud chce odesílatel předem stanovit definované QoS. Je zde nutná opakovaná rezervace síťových zdrojů, která také zatěžuje síť.

Nevýhodou DiffServ technologie je poskytnutí stabilní QoS mezi koncovými uzly pomocí PHB. Je zde nutná statická konfigurace SLA a DS je orientovaný pouze na zdroj datového spojení. Pokud je to nutné, dá se tato nevýhoda kompenzovat spoluprácí s IntServ sítí pomocí agregace RSVP. Výhodou je rozšiřitelnost tohoto typu sítě a velice široké možnosti konfigurace QoS.

Při použití uvedených technologií dochází k separátnímu oddělení signalizačních a směrovacích protokolů. Nemusí se vždy podařit najít požadované zdroje a cesty, popřípadě nové zdroje při náhlém rozpadu alokovaných cest. Za zmínku stojí a jistým řešením je využití TE (Traffic Engenniring) a MPLS pro zajištění požadované kvality služeb.

IntServ architektury, pokud jsou vyžadovány, jsou nasazovány především na okrajích sítí a DiffServ architektury v páteřních sítích, zajišťující tranzitní dopravu dat. Nejdůležitější funkcí v IntServ doméně je generování RSVP zpráv. Měli by jej podporovat všechny síťové prvky. Naopak v DiffServ doméně je nejdůležitějším prvkem hraniční směrovač RID, který zajistí namapování dat na jednotlivé PHB, či podporu RSVP agregace.

Výhledem do budoucna pro zajištění kvality služeb, definované nejen kvalitou přenosového pásma, ale i zabezpečením proti neustálým útokům v dnešních IP sítích jsou MPLS sítě a jejich nástavby. V současné době převládá využití DiffServ technologie a jejich nástaveb.

V praktické části bylo zjištěno, že podpora RSVP v e veřejných sítích je nahrazována postupně jinými protokoly implementovanými přímo do aplikací, které zpětně kontrolují kvalitu sítě a podle toho přizpůsobují vlastní provoz.. Tento fakt je například zveřejněn ve zdrojích MSDN firmy Microsoft, kde je uvedeno, že podpora RSVP zpráv byla naposledy využívána ve verzi Windows 2000 / NT. V privátních sítích, kde je potřeba rezervovat pevně síťové zdroje jsou IntServ sítě nepostradatelnou

součástí. Zde záleží již jen na tom, aby koncové stanice podporovali RSVP zprávy a na dohodě s poskytovatelem transportní sítě.

V praktické části byla vytvořeny dva typy emulované síťě v programu GNS3. Na jedné z těchto emulovaných sítí byl popsán a analyzován dopad použití různých typů konfigurace DiffServ na kvalitu simulovaného hlasového přenosu zatíženou FTP přenosem. Za pomocí programu NetQuality byly ověřovány jednotlivé parametry. Dále zde v této síti byla ověřena správná funkce mapování hodnoty DSCP a překlad na hraničních směrovačích. Nejefektivnější se jeví využití modulární řádkové konfigurace, kde je možné definovat vlastní pravidla provozu ať už jakéhokoliv podle konkrétních požadavků. Vyniká velikou modularitou konfigurace oproti jiným typům konfigurace QoS.

Na druhém typu sítě byla ověřena možnost spolupráce RSVP IntServ/DiffServ, kde se podařilo pomocí agregace RSVP staticky rezervovat zdroje v DiffServ síti. . Spolupráce RSVP s DiffServ a její potřebné konfigurace byly detailně popsány v teoretické části. Měření kvality přenosu dat zde nebylo prováděno z důvodu, že se nepodařilo zajistit takové koncové stanice či software, který by RSVP zprávy dynamicky generoval.

POUŽITÁ LITERATURA

[1] Cisco Systems, Inc. ,[cit. 2008-12-10], zdroje dostupné na WWW: www.cisco.com

[2] Cisco Systems, Inc. : Cisco IOS Quality of Service Solutions Configuration Guide, 12.2 IOS, 2008, zdroje dostupné na WWW: www.cisco.com

[3] HUCABY D., McQUERRY S.: Konfigurace směrovačů Cisco, Computer Press 2004 , ISBN: 80-722-6951-8

[4] Kolektiv autorů, práce RFC IETF, [cit. 2008-12-15] , zdroje dostupné na WWW: http://tools.ietf.org/html/

[5] Kolektiv autorů, program GNS3, [cit. 2009-04-14] , zdroje dostupné na WWW: www.gns3.net

[6] KUN I. PARK: QoS in Packet Networks , 2005 Springer Science + Business Media, Inc., Boston, ISBN: 0-387-23390-3

[7] PARK, K.: QoS in Packet Networks. Boston: Springer, 2004,ISBN: 0-387-23390-3.

[8] PING P. HENNING S.: YESSIR: A Simple Reservation Mechanism for the Internet, ACM New York, NY, USA, 1999, ISSN:0146-4833

[9] REXHEPI, V.. HEIJENK, G. J.. Interoperability of Integrated Services and Differentiated Services Architectures. University of Twente. 30.10. 2000.

[10] RZK GMBH,[cit. 2009-14-04], zdroje dostupné na WWW: http://download.rzk.net

[11] SZIGETI, T., HATTINGH, C.: End-to-end QoS network design. Indianapolis: Cisco Press,2005,ISBN:1-58705-176-1.

[12] TOBY J. VELTE, ANTHONY T. VELTE: Síťové technologie Cisco, Computer Press 2003, ISBN: 80-7226-857-0

[13] WANG, Z.: Internet QoS: Architectures and Mechanisms for Quality of Service. San Francisco: Morgan Kaufmann, 2001, ISBN: 1-55860-608-4.

SEZNAM ZKRATEK

ATM	Asynchronous Transfer Mode
BB	Bandwidth Broker
CAR	Committed Access Rate
CRTP	Comprimate Real Time Protocol
CBFQ	Credit-Based Fair Queuing
COPS	Common Open Policy Service
CoS	Class of Service
CS	Controlled Load Service
DiffServ	Differentiated Services
DS	DiffServ Domain
DSCP	DiffServ Codepoint
E2E	Edge to Edge
FIFO	First in First out
FRTS	Frame Relay Time Shifting
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
GS	Garanted Service
H323	Systems of Voice
HTTP	Hypertext Transfer Protocol
Hz	Hertz
IANA	Internet Assignet Numbers Authority
IntServ	Integrated Services
IP	Internet Protocol
IPER	Data Error Ratio
IPLR	Data Packet Discard
IPSec	Internet Protocol Security
ISP	Internet Service Provider
ITU	International Telecommunication Union
L2F	Layer 2 Forwarding
L2PT	Layer 2 Protocol Tunneling
LFI	Link Effeciency
LLQ	Low Latency Queuing
MAC	Media Access Control
MOS	Mean Opinion Score

MPLS	Multi Protocol Layer Switching
MQC	Modular QoS CLI
NBAR	Network Based Application Recognition
NP	Network Performance
OSI	Open Systems Interconnection
P2P	Peer to Peer
PHB	Per Hop Behavior
PQ	Packet Queue
QoS	Quality Of Services
RED	Random Early Detection
RFC	Request for Comments
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTI	Real Time Intolerant
RTP	Real Time Protocol
RTT	Real Time Tolerant
SLA	Service Lever Agreement
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
ToS	Type of Service
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice Over IP
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WWW	World Wide Web

Přílohy

A: Obsah CD

- Soubor BP_prace (Bakalářská práce ve formátu PDF)
- Soubor Zadani_prace (Zadání práce ve formátu PDF)
- Složka Obrazky_BP (Obrázky použité v práci ve formátu pro program Visio)