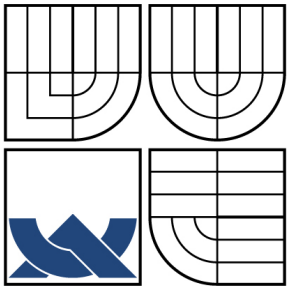
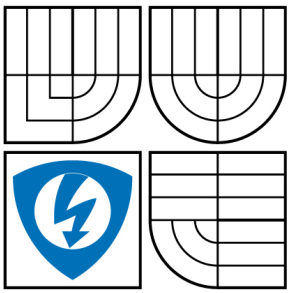


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

EXPERIMENTÁLNÍ SÍŤ PRO TESTOVÁNÍ PODPORY QOS

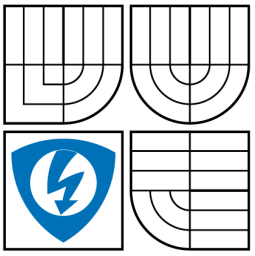
EXPERIMENTAL NETWORK FOR QOS SUPPORT TESTING

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MIROSLAV FOGL
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÍT NOVOTNÝ, Ph.D.
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Miroslav Fogl	***ID:***	73046
Ročník:	3	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Experimentální síť pro testování podpory QoS

POKYNY PRO VYPRACOVÁNÍ:

Seznamte s problematikou podpory kvalitativních požadavků služeb v sítích IP. Uvažujte jak linkovou, tak i síťovou vrstvu modelu komunikace. Prostudujte způsoby konfigurace podpory QoS v síťových prvcích laboratoře ÚTKO a navrhněte experimentální síť. Připojte stanice s různým typem provozu (VoIP, FTP, HTTP) a otestujte chování aplikací citlivých na podporu QoS pro různá nastavení podpory QoS v jednotlivých síťových prvcích. Výsledky přehledně zpracujte a vyhodnoťte. Na jejich základě navrhněte laboratorní úlohu.

DOPORUČENÁ LITERATURA:

[1] Wang Z.,Internet QoS: Architectures and Mechanisms for Quality of Service. Morgan Kaufman Publishers, ISBN 1-55860-608-4,2001
[2] Marchese M. QoS over Heterogeneous Networks. John Wiley & Sons, ISBN 978-0-470-01752-4, 2007

Termín zadání:	9.2.2009	***Termín odevzdání:***	2.6.2009

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

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

UPOZORNĚNÍ:

Anotace

Práce rozvádí problematiku podpory kvalitativních požadavků služeb v sítích IP na síťové i linkové vrstvě. Jsou zde popsány možnosti podpory kvalitativních služeb jednotlivých síťových prvků v laboratoři UTKO (směrovače, L3 přepínače). Vytvořená experimentální síť je zatížena různým druhem provozu (VoIP, FTP, HTTP, Video). Realizace datových služeb je pomocí dostupných terminálů (IP telefony, IP kamery, IP video-telefony, servery, klientské stanice). Měření je zaměřeno na zacházení s pakety v směrovači. Možnosti nabízející směrovač Cisco jsou ověřeny analýzou paketů. Dostupné metody zahazování jsou porovnány na základě měření a vyhodnoceny. Nejvhodnější obsluhou výstupní fronty je po měření v experimentální síti mechanizmus LLQ. Dokáže pakety upřednostňovat podle jejich priority v IP hlavičce. Dále je simulován rozdíl přetížení linky velkým datovým tokem po použití politiky QoS. K dosažení dostupnosti datových služeb v celé síti je žádoucí se zabývat mechanizmy k podpoře kvalitativních služeb ve všech síťových prvcích v síti.

Abstract

The work specifies problems with support of qualitative requirements in IP network services on the network and link layer. There are also described options of qualitative support of individual networking components in the UTKO laboratory (routers, L3 switches). Created experimental network is loaded by various types of service (VoIP, FTP, HTTP, Video). Data services realization is ensured by available terminals (IP phones, IP cameras, IP video-phones, servers, client stations). Metering is targeted on the manipulation with packets in the router. Options which Cisco router offers are verified by packet analysis. Available methods of dropping are compared on the base of metering and evaluated. Optimal handling with output queue after metering in experimental network is LLQ mechanism. It is able to prefer packets according to their priority in the IP header. Further the difference of link overloading by huge dataflow after QoS policy using is simulated. To reach availability of data services in the whole network is necessary to deal with mechanisms for qualitative services support in all the network components in the network.

Klíčová slova

Kvalita, priorita, klasifikace, fronta, zahazování, provoz, směrovač

Key words

Quality, priority, classification, queue, dropping, service, router

Bibliografická citace práce

FOGL, M. *Experimentální síť pro testování podpory QoS*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 38s. Vedoucí bakalářské práce doc. Ing. Vít Novotný, Ph.D.

Prohlášení o původnosti práce

Prohlašuji, že svou bakalářskou práci na téma Experimentální síť pro testování podpory QoS jsem vypracoval samostatně pod vedením vedoucího bakalářské práce s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny uvedeny v seznamu literatury na konci práce.

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

V Brně dne ..... ……

podpis autora

Poděkování

Děkuji vedoucímu práce doc. Ing. Vítu Novotnému, Ph.D., za velmi užitečnou metodickou pomoc a cenné rady při zpracování bakalářské práce.

V Brně dne ..... ……

podpis autora

OBSAH

ÚVOD

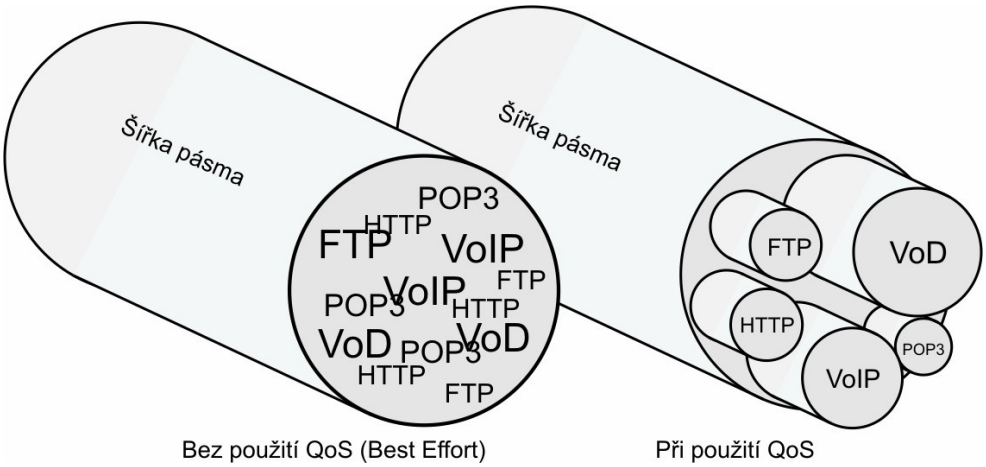
Před několika lety byla síť Internet využívána hlavně k dosažení datového spojení s protější stranou v síti. Využívání Internetu se však stále rozšiřuje. Posílání klasických dopisů či prohlížení inzertních novin se tak stává pro mnoho lidí téměř minulostí. Elektronická pošta, přenos souborů, prohlížení internetových stránek či vzdálený přístup byly hlavním využitím tehdejší sítě Internet. Jelikož tyto služby nebyly nijak extrémně náročné na šířku pásma a časové parametry přenosu nehrály takovou roli, nebylo potřeba tolik řešit zajištění propustnosti v síti a dohled nad časovými parametry komunikace. Postupným rozšiřováním možností Internetu a integrací takových aplikací jako jsou video přenosy, IP telefonie, on-line poslech hudby videa, počítačové hry po síti a další, je kladen stále větší důraz na zajištění dostatečné šířky kmitočtového pásma komunikačního kanálu, zaručení časových parametrů (zpoždění a jeho proměnlivost) a zaručení přijatelné chybovosti přenosu pro jednotlivé typy služeb. Pokud v dané firmě bude probíhat jednání formou videokonference s klienty, sídlící na druhé straně Země, je potřeba zajistit plynulé bezvýpadkové přenesení obrazu a zároveň i zvuku, aniž by účastníci poznali, že po většině úsecích spojení je provozováno mnoho dalších služeb, které by mohly ovlivnit kvalitu námi provozované služby např. posíláním elektronické pošty či stahováním souborů z FTP serveru. Jestliže před deseti lety zůstávala výrazná většina datových toků uvnitř lokálních sítí, je dnes situace přesně opačná a většina zátěže leží na páteřní infrastruktuře všech úrovní. Tradiční datové aplikace podporované mechanismy TCP jsou ještě vcelku dobře schopny vyrovnat se s přetíženými linkami, horší je to však s aplikacemi multimediálními a speciálně pak interaktivními, které jsou velmi citlivé na zpožděna jeho proměnlivost při přenosu digitalizovaného obrazu a zvuku a využívají nezabezpečený transportní protokol UDP. Všechny služby a aplikace potřebují ke svému provozu dostatečnou šířku pásma závislou na typu služby, a řada z nich vyžaduje také co nejmenší dobu zpoždění a ztrátovost. Současné paketové sítě však mají své problémy. Především jde o to, že jednotlivé aplikace vzájemně soupeří o společnou šířku pásma sdíleného kanálu a některé služby (audio a videokonverzační řízení, gaming, aj.) jsou méně tolerantní ke zpoždění než jiné aplikace, jako například přenos souborů přes FTP. Datové přenosy v Internetu se stále ve většině případů realizují v režimu best effort. Best effort je však také problematický z hlediska marketingu, neboť nelze zaručit domluvenou kvalitu připojení. Poskytovatelé připojení tak vlastně nabízejí produkt, jehož parametry závisí na řadě náhodných okolností zátěže spojů a spojovacích uzlů, které nemohou ovlivnit. Mnozí jejich zákazníci jsou přitom ochotni za služby také řádně zaplatit.

V této práci se chci zabývat možnostmi, které nabízí využití řízení kvality služeb v síti IP. V dnešní době se využití kvality služeb teprve začíná realizovat v rozsáhlých sítích. Je více mechanizmů, které jsou součástí k vytvoření řízení kvality služeb. Nejpoužívanější způsoby možné realizace se budu snažit popsat a zhodnotit. Získané znalosti budou ověřeny v praktické části, kde bude sestavena experimentální laboratorní síť a na ni nasazena řada služeb s různými požadavky na zajištění kvalitativních parametrů. Budou sledovány kvalitativní parametry služeb v konfiguraci best effort“ a při aktivaci a konfiguraci podpory dodržování kvalitativních parametrů v jednotlivých přepojovacích uzlech experimentální sítě.

1 PŘÍSTUPY K PODPOŘE KVALITATIVNÍCH POŽADAVKŮ SLUŽEB

V poslední době dochází k rozvoji služeb, jejichž úspěšnost z pohledu uživatele významně závisí na kvalitativních charakteristikách komunikace přes počítačovou síť. Uživatel požaduje, poskytnutí určité kvality služeb (Quality of Service - QoS). Pojem kvalita služeb v podstatě znamená, že daná komunikační síť může rozlišovat jednotlivé typy datového provozu a zacházet s nimi tak, aby splnila jejich požadavky na zpoždění, ztrátovost a jitter. V současné době je termín kvalita služeb především skloňován v souvislosti s dnešním Internetem. Internet jako celosvětová síť je založena na protokolové sadě TCP/IP, a ta ve své základní podobě není schopna poskytovat kvalitu služeb. To znamená, že není schopna rozlišovat jednotlivé druhy služeb, např. real-time datové proudy vůči klasickým datovým přenosům a zachází s nimi zcela shodně.

Technologie pro podporu QoS pomáhají zajistit rovnoměrné vyvážení zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé zákazníky dle nastavených priorit a zabraňuje přetížení v síti.



Obr. 1.1: Porovnání toků dat s využitím QoS mechanizmů

Myšlenka o rozlišování typů paketů a následné možnosti jejich zpracování v rámci QoS, byla již v počáteční době specifikací IP a jedná se o pole ToS (Type of Service) v hlavičce IP paketu. V ranných dobách internetu nebyla podpora ToS důležitá, a proto ji většina IP implementací ignorovala.

Počátkem 90. let 20. století se začaly uplatňovat mechanismy pro plánování front paketů na směrovačích pro eliminaci stavů jejich zahlcení. Dále rozšířením aplikací, které mají striktní požadavky na šíři pásma, byl zaveden model Integrated services pro garanci předem definovaného chování sítě pro náročné aplikace. Zatímco u Integrated services rezervují požadavky na provoz v síti přímo koncové aplikace, u následného modelu Differentiated services síť filtruje provoz a jednotlivým paketům přiřadí úroveň třídy služeb.

2 HLAVNÍ PARAMETRY

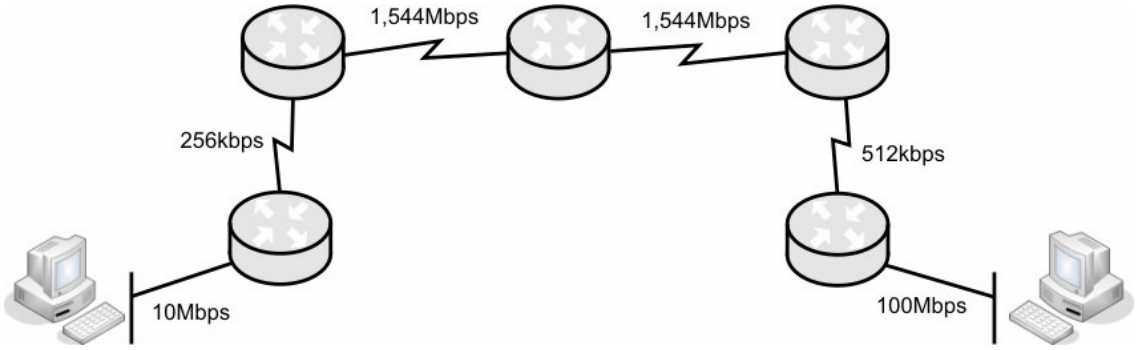
Parametry QoS jsou veličiny, které ovlivňují výslednou kvalitu služby. Tyto veličiny jsou nejvíce závislé na síťovém vybavení podél celé datové cesty paketu.

Mezi hlavní parametry QoS patří:

- Přenosová rychlost
- Zpoždění
- Rozptyl zpoždění
- Ztrátovost

Přenosová rychlost

Šířka pásma, která je k dispozici pro přenos dat po daném médiu závisí na fyzikálních možnostech přenosového média na jednotlivých úsecích přenosové cesty, na výkonu přepojovacích uzlů, na úrovni provozu od dalších zdrojů sdílející některé úseky trasy a na výkonnosti vysílací a přijímací strany. Přenosová kapacita je závislá převážně na šířce pásma, útlumové charakteristice kanálu, na úrovni rušení a na maximálním povoleném vysílacím výkonu [4]. Fyzikálně možná přenosová rychlost je výrazně vyšší, než skutečně využívaná šířka pásma během přenosu. Jednotlivé úseky v síti mohou být propojeny různou šířkou pásma. Skutečná (Efektivní) šířka pásma, je šířka pásma nejpomalejšího spoje na celé trase, jak je znázorněno na obrázku obr. 2.1. Na obr. 2.1 je zakreslena síť, kde koncoví uživatelé budou využívat maximální dostupnou šířku pásma po celé trase, tedy 256kb/s.



Obr. 2.1: Efektivní šířka pásma

Zpoždění

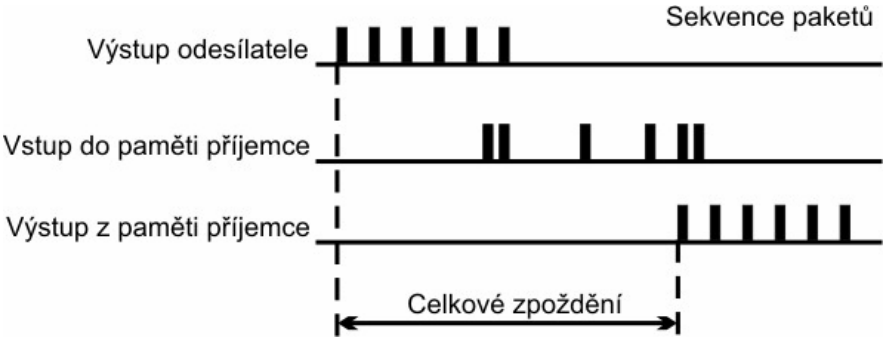
Celkové zpoždění nebo také jednocestné zpoždění je čas, který je třeba pro přenos informace ze zdroje ke spotřebiči. Většina lidí nadměrné zpoždění zaregistruje tím, že plynulost přenášeného hlasu či videa je velmi špatná. Z hlediska rychlosti přenosu dat sítí je výhodné volit velikost paketů spíše menší, neboť tyto pakety je možno v komunikačních uzlech rychleji zpracovat a odeslat do dalšího uzlu. Zvýšením poměru záhlaví k délce užitečných dat paketu se snižuje průchodnost spoje mezi komunikačními uzly, neboť narůstá režie přenosu. Z hlediska zpoždění je výhodné přenášet spíše malé bloky dat.

V paketové síti existují tři druhy zpoždění:

- **Zpoždění dané šířením signálu** – čas potřebný k předání informace přímo po fyzickém přenosovém médiu. Má význam hlavně při komunikaci přes satelitní spoje.

- **Doba zpracování** – doba nutná k předání paketu fyzické vrstvě. Zpoždění vzniklé přenosem z aplikační k fyzické vrstvě. Může se jednat o softwarové zpoždění.

- **Zpoždění na rozhraní** – doba, která je nutná pro zpracování paketu v uzlu při předání k vysílání v závislosti na rychlosti mechanizmů zajišťujících reprezentaci na fyzické medium.



Obr. 2.2: Celkové zpoždění sestávající ze zpoždění způsobeného vlastním přenosem a zpoždění pozdržením ve vyrovnávající paměti pro odstranění jitteru

Rozptyl zpoždění

Hodnota rozptylu zpoždění nazývána jitter představuje rozptyl zpoždění paketů vzniklý z důvodu proměnlivosti přenosových podmínek v síti. Vysílací strana v případě hlasové služby posílá pakety v pravidelných intervalech. Ideálně by přijímací strana měla přijímat pakety také v pravidelných časových okamžicích, v tomto případě by velikost parametru jitter byla nulová. Ale mnoho různých zařízení může určité pakety v datové síti zpomalit, a tak některé pakety přijdou dříve a jiné mnohem později. Jestliže „pomalé“ pakety jsou doručeny příliš pozdě, jsou dle použitého protokolu zahozeny, protože jejich obsah už není příjemci k ničemu („zastaral“). Jedna metoda potlačení náhodnosti příchodu zpožděných paketů vkládá mezi síťovou vrstvu a aplikaci paměť pro vyrovnávání proměnlivosti zpoždění, tzv. jitter buffer. Jitter buffer pozdržuje pakety na přijímací straně. To pomůže vyrovnat proměnlivost zpoždění příchodu paketů, a tedy umožní k dalšímu zpracování předávat pakety opět se správnými časovými odstupy, tak jak byly vysílány ze zdroje. Poté pošle příchozí pakety aplikaci ve správném pořadí. Jitter paměť podrží pakety po určitý čas ve vyrovnávací paměti za cenu zvýšení celkového zpoždění. Další problémy nastanou, když jitter buffer přeteče a další příchozí pakety jsou ztraceny.

Ztrátovost

Různé služby jsou různě citlivé na ztrátovost paketů a vypořádávají se se ztrátovostí paketů různými způsoby, závislými na typu služby, použitém kodeku a na přenosovém protokolu. U služeb v reálném čase pakety, které jsou ztraceny, nemohou být obnoveny (z důvodu neakceptovatelného zpoždění), a tím vznikají problémy v dekodéru, kterému pak chybí určitý úsek dat, což může mít za následek i znatelné mezery v konverzaci. Pokud je ztráta paketů rozložena náhodně, nevede to k tak významnému zhoršení hlasové kvality, vliv však závisí na typu použitého kódování hlasu či obrazu. Malé mezery nevadí, ale vysoká ztrátovost paketů nebo ztráta většího množství paketů následujících za sebou, vede k výraznému zhoršení kvality přenášené řeči. Právě ztráta většího množství paketů následujících za sebou, znamená největší problém pro kvalitu hovoru. Tento efekt má za následek mnohem větší zhoršení v kombinaci s vysokým zpožděním.

3 MODELY PRO ZAJIŠTĚNÍ KVALITY SLUŽEB

3.1 ARCHITEKTURA INTEGROVANÝCH SLUŽEB (INTEGRATED SERVICES)

Model Integrovaných služeb, dále již Intserv, byl první model, který měl za úkol zajistit požadovanou kvalitu služeb v počítačových sítí protokolem IP. Tento model byl uveden v roce 1994. Model předpokládá záruky pro QoS po celé trase mezi zdrojovou a cílovou stanicí. Počítačová síť ověří, zda jsou k dispozici požadované prostředky, a rozhodne, zda požadavkům vyhoví. Tato funkce je označována jako admission control (řízení přístupu). V případě, že síť nemůže požadavku vyhovět, není spojení povoleno a aplikace se může rozhodnout, zda požádá o méně náročné požadavky služeb. Pokud je požadavek přijat, musí počítačová síť informovat všechny komponenty, přes které bude probíhat přenos, aby pro dané spojení rezervovaly odpovídající objem prostředků, např. šířku pásma mezi dvěma směrovači, kapacitu fronty paketů, atd. K tomuto účelu slouží rezervační protokoly. Nejrozšířenějším rezervačním protokolem je RSVP (Resource reSerVation Protocol), který je však poměrně složitý a představuje významnou režii při řízení chodu sítě. Proto se v poslední době objevují návrhy jednodušších protokolů pro rezervaci, např. YESSIR.

Integrované služby rozlišují následující kategorie aplikací:

- **Elastické aplikace** – bez požadavku na brzké doručování. Do této kategorie zapadají aplikace nad TCP. Nejsou kladeny striktní požadavky na omezení zpoždění nebo kapacitu spojení. Příkladem je el. pošta, http protokol, atd.

- **Real Time Tolerant (RTT) aplikace** – požadují omezení na maximální zpoždění v síti. Občasná ztráta paketů je přijatelná. Příkladem jsou video aplikace využívající bufferování, které před aplikací skryjí ztrátu paketů.

- **Real Time Intolerant (RTI) aplikace** – tato třída požaduje minimální odezvu (latency) a rozptyl zpoždění (jitter). Příkladem jsou videokonference.

Pro správnou funkci Intserv musí být ve směrovačích a hostitelích implementovány následující komponenty:

- **Plánovač paketů**

Plánovač paketů řídí zasílaní různých proudů paketů, používáním souborů front a dalších mechanizmů jako např. časovače. Plánovač paketů musí být implementován v místě, kde jsou pakety řazeny do front. Většinou je každá služba implementovaná ve směrovači, řešena samostatnou frontou a plánovač řídí posílání jednotlivých paketů z front podle předem daných algoritmů.

- **Kontrola přístupu**

Kontrola přístupu realizuje rozhodovací algoritmus, který směrovač nebo hostitelský počítač používá k určení, zda-li novému toku může být udělena rezervace bez dopadu na dřívější záruky. Kontrola přístupu je spuštěna v každém uzlu, aby mohl rozhodnout, zda bude daná QoS akceptována nebo odmítnuta.

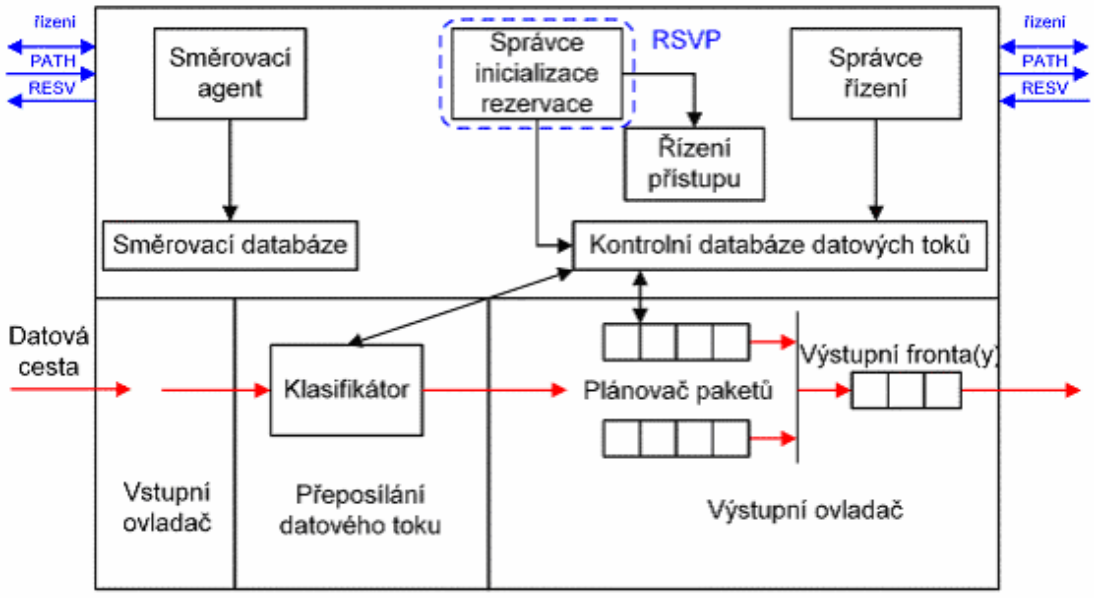
- **Klasifikátor**

Klasifikátor paketů identifikuje v hostitelích a směrovačích pakety, které budou přijímat určitou úroveň služby. Pro efektivní řízení datové dopravy je každý příchozí paket namapován klasifikátorem do určité třídy. Se všemi pakety, které byly zařazeny do stejné třídy, bude v plánovači paketů

zacházeno stejně. Volba třídy je založená na zdrojové a cílové IP adrese a čísle portu či na dalších hodnotách, které musí být přidané ke každému paketu.

- **Protokol RSVP**

Čtvrtou součástí implementace je protokol pro rezervaci zdrojů, který je nutný k vytvoření a udržování stavů v koncových zařízeních a ve směrovačích podél cesty toku dat. Tímto protokolem se budeme zabývat v kapitole 3.1.1.



Obr. 3.1: Komponenty IntServ

Nevýhody Integrated Services

Tento přístup má však řadu nevýhod. Všechna zařízení, přes která procházejí IP pakety datových toků, a pro které je potřeba zajistit určitou kvalitu služby, včetně koncových zařízení (PC, servery), musí podporovat protokol RSVP. Každý směrovač v síti musí udržovat stavovou informaci pro každou rezervaci (každý datový tok s požadavkem na zajištění kvality služeb), je rozšiřitelnost IntServ modelu omezená. Ve větších sítích, kde množství datových toků roste do statisíců, bychom narazili na vysoké paměťové a výkonnostní nároky na směrovače. Proto bychom model IntServ stěží hledali v sítích poskytovatelů internetových služeb. V podnikových sítích však nalézá model IntServ uplatnění např. při zajišťování QoS pro přenos hlasu v IP síti, kdy před ustavením komunikace probíhá kontrola přijetí spojení (CAC – Call Admission Control) právě protokolem RSVP.

Proto byl definován další model pro zajištění QoS v komunikační síti, diferencované služby (Diffserv), které jednotlivé toky slučuje do skupin, se kterými je pak zacházeno ve směrovačích shodně.

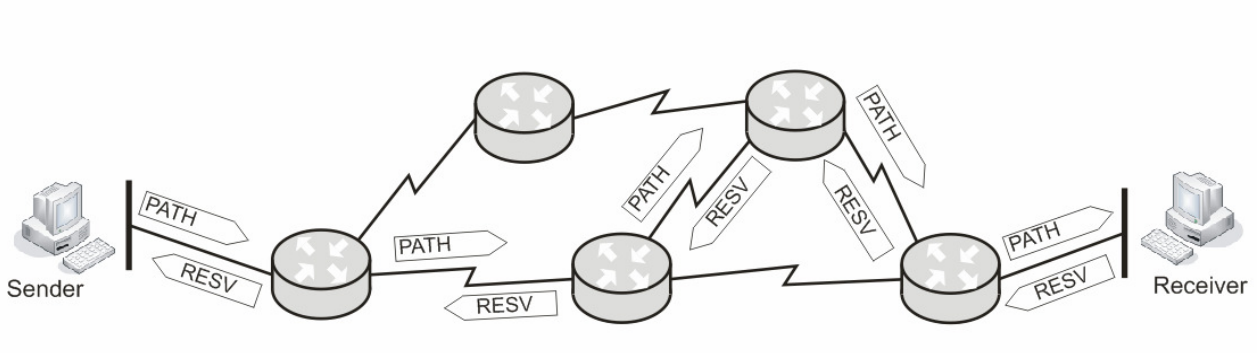
3.1.1 Protokol RSVP

Ačkoliv původní specifikace integrovaných služeb měla být nezávislá na protokolu, v praxi se pro tento účel používá výhradně protokol RSVP, který je přenášen pomocí IP protokolu. RSVP definuje několik typů zpráv, které se rozlišují pomocí osmibitového pole v hlavičce protokolu. Kromě vlastní hlavičky může RSVP přenášet další údaje ve formě tzv. objektů. Některé obecné objekty jsou definovány přímo ve specifikaci RSVP [8].

RSVP (Resource reSerVation Protocol) je protokol pro rezervaci zdrojů na Internetu. Protokol RSVP je používán k získání určité kvality služeb pro jednotlivé aplikační datové proudy nebo toky. RSVP je také užíván ve směrovačích k doručení QoS žádostí všem uzlům podél cesty datových toků a k vytvoření a udržování stavů, které jsou nutné pro poskytnutí požadované služby. V každém uzlu se RSVP pokusí vytvořit rezervaci zdrojů pro daný datový proud.

Některé aplikace vyžadují spolehlivé doručení dat, ale nevyžadují žádné přísné požadavky na včasnost doručení. Ale aplikace jako videokonference, IP telefonie či NetRadio vyžadují téměř přesný opak. Doručení dat musí být včasné, ale nemusí být stoprocentně spolehlivé. RSVP má za cíl poskytnout IP sítím schopnost podporovat odlišné výkonové požadavky různým aplikacím.

V protokolu RSVP je datový tok sekvence paketů, které mají stejný zdroj, cíl a kvalitu služeb. V architektuře QoS založené na protokolu RSVP existují dva základní prvky – zdroj a cíl. Na obou prvcích běží RSVP procesy, které se podílejí na protokolu RSVP a vyměňují si RSVP zprávy jménem svých hostitelů. Vyměňují si v podstatě dva druhy zpráv: PATH a RESV zprávy. Zdroj služby pošle PATH zprávu, která je obsažena v IP nebo UDP paketu. Když je tato zpráva přijata příjemcem služby, tak pokud chce učinit rezervaci pro daný RSVP tok, odpovídá RESV zprávou. Ta je poslána zpět k odesílateli po stejné cestě jako PATH zpráva. V opačném případě je vygenerována RESV ERROR zpráva, která je také poslaná zpět k příjemci. Koncová rezervace je úspěšně ustanovená, když RESV zpráva dosáhne odesílatele a je zpracována ve všech průchozích uzlech. RSVP je protokol k vyjednání kvality služeb pro konkrétní použití a nejedná se o směrovací protokol. Proto využívá směrovací tabulky směrovačů k určení nejlepší cesty k doručení.



Obr. 3.2: Udržování spojení v IntServ (RSVP)

Pro řízení sítě se používají následující strategie:

- Udržování stavu propojení,
- hlídání a úprava přenosu,
- předcházení zahlcení,
- management předcházení nebo odstranění zahlcení,
- mechanizmus sledování výkonnosti linky.

Vlastnosti protokolu RSVP:

- RSVP je výhradně signalizační protokol, který pro své šíření využívá informací získaných běžnými směrovacími protokoly.

- Zajištění QoS je založeno na explicitních rezervacích zdrojů ve všech směrovačích podél datové cesty. Každý směrovač musí v paměti uchovávat potřebné stavové informace. Všechny tyto informace mají omezenou životnost a musí být periodicky obnovovány zprávami typu PATH a RESV. Informace a rezervace příslušející danému toku lze též zrušit explicitně pomocí zpráv typu PATHTEAR a RESVTEAR.

- Rezervace jsou iniciovány příjemcem a realizují se postupně proti směru datového toku. To je velmi výhodné zejména pro multicastové toky, protože se tím rozděluje zátěž spojená s instalací cest pro datový tok a umožňuje se též efektivní využití rezervačních požadavků.

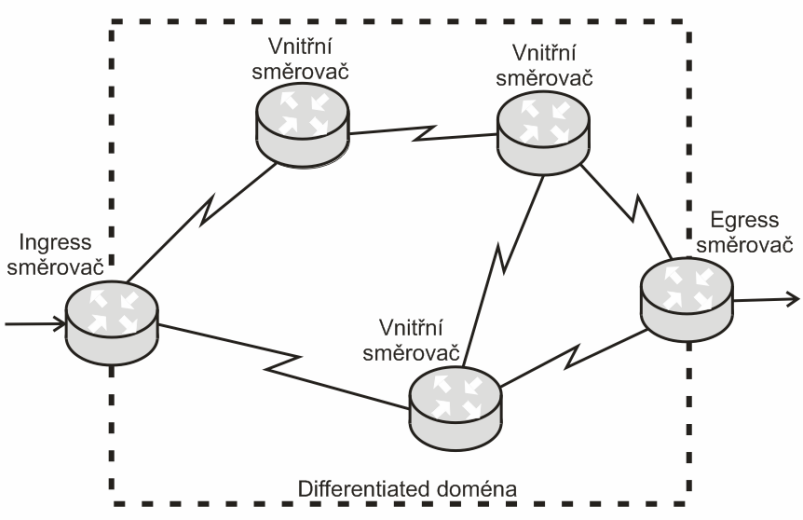
3.2 DIFFERENTIATED SERVICES

Motivací pro hledání alternativ k integrovaným službám byly oprávněné obavy ze špatné škálovatelnosti protokolu RSVP, zejména pokud by se měly rezervace realizovat napříč celým Internetem. Pro velmi zatížené směrovače přenášející statisíce toků by totiž nároky na paměť a výpočetní kapacitu byly skutečně extrémní.

Model DiffServ se snaží problematiku zajištění kvality služby zjednodušit a snížit tak nároky na systémové zdroje uzlů sítě. Rozlišované služby se od integrovaných služeb liší zejména tím, že aplikace neoznamuje předem počítačové síti své požadavky na QoS. Použití rezervačních protokolů není nutné. Jednotlivé směrovače neudržují žádnou stavovou informaci o jednotlivých spojeních. Implementace QoS je řešena tak, že každý paket, vstupující do počítačové sítě je označen značkou, která určuje třídu přenosu, poskytovanou paketu. Označování paketů probíhá pouze na vstupu do počítačové sítě, během přenosu směrovače čtou značku a podle této značky se k danému paketu chovají, tedy například jej upřednostní před ostatními pakety čekajícími ve frontě.

Úprava provozu v Diffserv doménách je vykonávána v hraničních uzlech, tj. v uzlech, které spojují dvě domény. Úpravou v hraničních uzlech je vstupní a výstupní doprava zformovaná tak, aby byla přizpůsobena volným zdrojům v cílové doméně. Prvek upravující provoz obsahuje měřiče, značkovače, zahazovače a tvarovače. Tato zařízení měří vstupní datovou dopravu a podle výsledku mohou přeznačit pakety.

Rozlehlé počítačové sítě lze rozdělit na organizačně menší oblasti, které jsou řízeny lokálním administrátorem. V těchto oblastech mohou být použity různé typy směrovačů, vybavené různými protokoly pro zajištění QoS. Proto je velmi obtížné zajistit jednotné zpracování požadavků na QoS. Z hlediska rozlišovaných služeb je síť rozdělena na oblasti se samostatnou správou rozlišovaných služeb, tzv. Diffserv domény. Doména obsahuje dva druhy směrovačů. Vnitřní směrovače, zajišťující spojení uvnitř Diffserv domény a hraniční směrovače, zajišťující značkování a odznačení paketů včetně jejich posílání vnitřním směrovačům. Hranové směrovače lze rozdělit podle funkce na ingress směrovače, zajišťující značkování paketů a egress směrovače, zajišťující jejich odznačení. Pakety vstupují do Diffserv domény přes ingress směrovač, jsou přenášeny interními směrovači a vystupují přes egress směrovač, jak je znázorněno na obr. 3.3. Jsou-li propojeny dvě Diffserv domény, pracuje hranový směrovač současně jako egress směrovač jedné domény a ingress směrovač domény druhé.

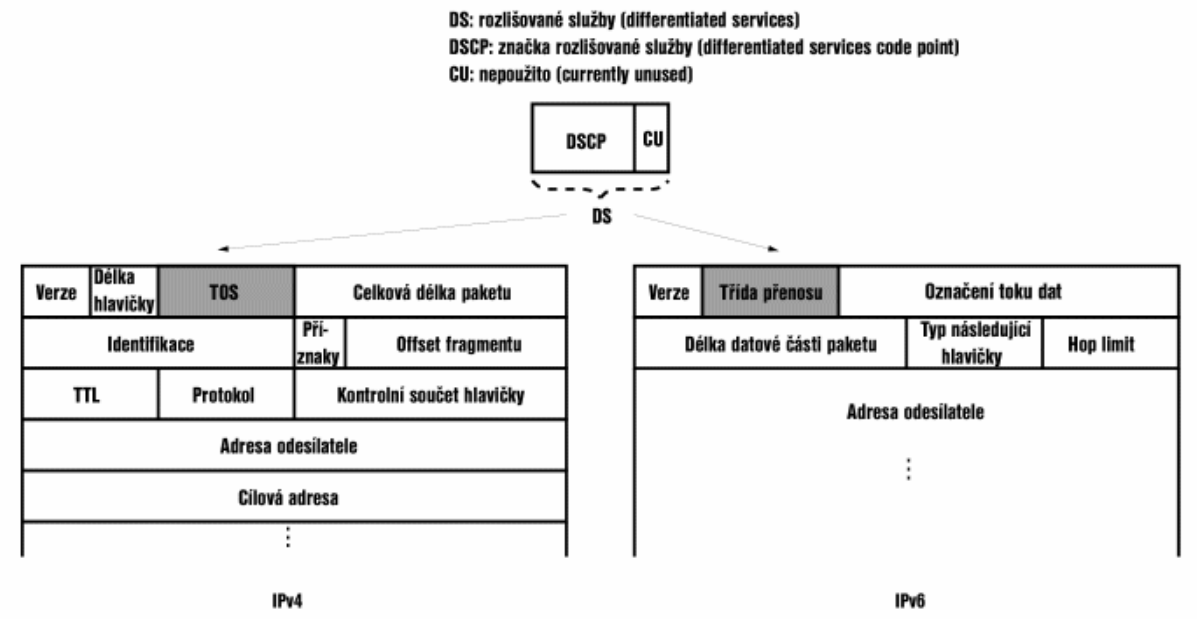


Obr. 3.3: Směrovače v DiffServ doméně

3.2.1 Klasifikace paketů

Klasifikace paketů probíhá v ingress směrovačích. Výběr značky může být proveden na základě IP adresy odesílatele nebo adresáta, číslem portu služby, podle výsledků měření dynamických vlastností přicházejících dat apod. [2]. Uvnitř Diffserv domény zůstává značka nezměněna, ale při přechodu do jiné domény se může změnit na jinou značku se stejným významem nebo na jinou značku s jiným významem. Pakety mohou být klasikovány již aplikací, posílající pakety do sítě. První ingress směrovač může tuto značku pozměnit nebo zachovat.

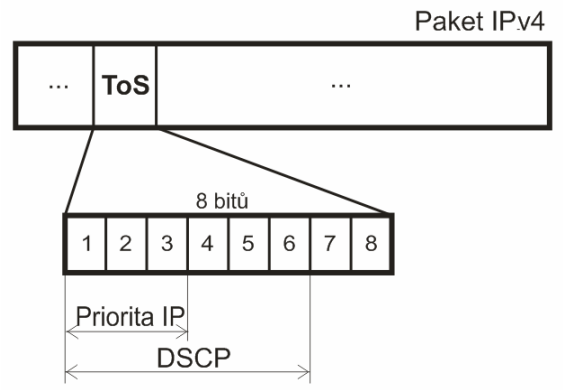
Způsob označení paketu závisí na technologii nebo protokolu použitém pro přenos paketů. Značka může být buď obsažena uvnitř hlavičky paketu, pokud je tam pro ni vhodné místo, nebo připojena vně paketu. Nejčastější je implementace Diffserv na úrovni síťové vrstvy modelu sítě při použití protokolu IP. V tomto případě je značka obsažena v poli označeném jako DS (Differentiated Services), které je uloženo buď v místě určeném pro pole ToS (Type-of-Service) hlavičky protokolu IP verze 4 nebo v místě pro pole Traffic Class hlavičky protokolu IP verze 6. Pole ToS bylo původně určeno pro obdobné účely, související se zpracováním paketu ve směrovačích nebylo však plně využíváno. Pole Traffic Class bylo navrženo pro určitý způsob klasifikace paketů bez bližší specifikace. Obě místa se využívají k uložení značky Diffserv. Pole DS má 8 bitů, z toho 6 bitů je určeno pro vlastní značku DSCP (Differentiated Services Codepoint) a zbývající 2 bity jsou využity pro techniku ECN (Explicit Cogestion Notification) [2]. Umístění a struktura pole DS u obou verzí IP paketu jsou znázorněny na obr. 3.4.



Obr. 3.4: Umístění pole DS v IPv4 a IPv6

Pakety můžeme označit pomocí bitů uvnitř bajtu ToS, a to buď prostřednictvím IP precedence (priority IP) nebo kódu DSCP.

Pole „IP precedence“ využívá první tři bity, které se v bajtu ToS nachází. Pomocí tří bitů můžeme rozlišit až osm úrovní priorit značené od 0 do 7. Hodnoty 6 a 7 by se však neměly používat, protože jsou vyhrazeny pro komunikaci mezi síťovými uzly.



Obr. 3.5: Byte ToS

Pro větší rozlišení provozu můžeme použít kód DSCP, který pracuje se šesti bity umístěnými zcela vlevo v bajtu ToS, viz obr. 3.5. Šest bitů poskytuje 64 možných hodnot. U takového množství dostupných hodnot vzniká problém, že hodnota, kterou vybereme, aby představovala danou úroveň priority, může být na jiném směrovači nebo přepínači, který je pod správou jiného poskytovatele, zpracována odlišným způsobem. Proto se používá standardizované chování paketů značené pomocí Per Hop Behaviours.

Per Hop Behaviour

V poli DSCP je možné pomocí šesti bitů docílit až 64 úrovní, které mohou znázorňovat prioritu daného paketu. V praxi se zatím tolik úrovní nepoužívá. Per Hop Behaviours (PHB) značí chování paketu v každém směrovači na cestě od zdroje k cíli. Nejnižší priorita paketu je značena nejmenší

hodnotou v poli DSCP, tedy hodnotou 0. K zajištění zpětné kompatibility se pakety, u kterých není známa hodnota PHB mapují právě na hodnotu nula.

Všechna chování PHB spadají do jedné ze tří kategorií [1]:

- Selektor třídy (Class Selektor – CS)
- Urychlené předávání (Expedited Forwarding – EF)
- Zajištěné předávání (Assured Forwarding – AF)

Selektor třídy (CS-PHB)

Paketový provoz je rozdělen do osmi základních úrovní pro určení priority přenosu. Zde se využívají pouze první tři bity. Následující tři bity jsou v této metodě ignorovány. K zajištění kompatibility priorit s dalšími metodami využívá CS-PHB právě první tři bity MSB v poli DSCP. Přepojovací prvek nepodporující kvalitu služeb, vykazuje chování typu Best Effort, jenž je namapováno na nejnižší úroveň viz tab. 3.1. Vyšší hodnota precedenčních bitů představuje vyšší prioritu paketu. Prioritní bity z IPv4 QoS pole jsou široce využívány v existujícím síťovém vybavení, a proto jsou také podporovány v Diffserv doméně.

Tab. 3.1: Selektor třídy PHB

Selektor třídy PHB	
Hodnota DSCP	**Priorita**
000xxx	Best Effort
001xxx	7.
010xxx	6.
011xxx	5.
100xxx	4.
101xxx	3.
110xxx	2.
111xxx	1.

Urychlené předávání (EF-PHB)

Kategorie EF (Expedited Forwarding) chování PBH má pole DSCP přesně stanovenou na hodnotu 46, která odpovídá třetí úrovni v CS-PHB. EF PHB poskytuje nástroje pro vytvoření nízké ztrátovosti, zpoždění a jitteru a zajištění šířky pásma pro koncové služby přes Diffserv domény. Například hlas, typicky dostane označení EF chování PHB. Urychlené předávání předpokládá, že data jsou upravena na Diffserv hranicích tak, že směrovače uvnitř Diffserv domény budou posílat pakety dále ihned, bez rizika překročení vyjednané rychlosti přenosu. Služba realizovaná touto PHB je podobná zaručené službě v modelu Intserv. Diffserv uzel zabezpečuje, že jednotlivá agregace bude mít minimální odchozí rychlost nezávislou na další datové dopravě v síťovém uzlu. Datový tok by měl být upraven tak, aby maximální příchozí rychlost v uzlu byla menší než minimální odchozí rychlost poskytnutá pro EF PHB. EF PHB znamená přísnou kontrolu bitové rychlosti a rychlé předávání dat mezi směrovači v Diffserv doméně.

Zajištěné předávání (AF-PHB)

Motivace pro AF (Assured Forwarding) PHB bylo potřeba pevné šířky pásma spoje. V typické aplikaci může společnost užívat Internet pro propojení svých geograficky rozdělených míst a bude chtít záruku, že IP pakety uvnitř tohoto intranetu budou posílané s vysokou spolehlivostí, pokud datová agregace z určitého místa nepřesáhne předepsanou rychlost danou v profilu. Pakety, které jsou mimo profil, jsou poslány dále s nižší pravděpodobností.

AF PHB skupina poskytuje čtyři třídy úrovní záruk a zdrojů (prostor vyrovnávací paměti a šířka pásma) pro IP pakety přijaté od klientské DS domény. Pakety patřící do každé třídy mohou být také označené na jednu ze tří priorit AF PBH. Tato priorita se využívá v případě přetížení směrovače. Je-li v něm implementován algoritmus řízení přetížení RED, jsou pakety s nižší hodnotou DSCP zahazovány častěji, než pakety s vyšší hodnotou DSCP. Konkrétní binární hodnoty pole DSCP jsou uvedeny v tab. 3.2.

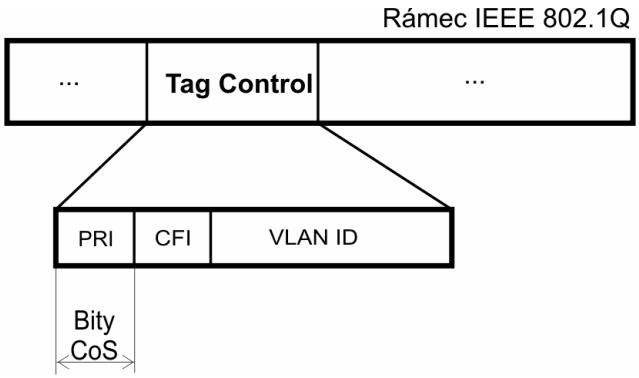
Tab. 3.2: Zajištěné předávání PHB

Priorita AF PBH	Třída 1	Třída 2	Třída 3	Třída 4
Nízká	001010	010010	011010	100010
Střední	001100	010100	011100	100100
Vysoká	001110	010110	011110	100110

3.2.2 Klasifikace rámců

Dříve než se objevily zmíněné modely IntServ a DiffServ pro zajištění QoS na 3. vrstvě modelu OSI Existuje také podpora pro QoS i na 2. vrstvě modelu OSI. Technologie jako ATM nebo FrameRelay disponují bohatou podporou pro zajištění QoS. Podmínkami pro dosažení opravdové end-to-end podpory QoS jsou nezávislost implementace na médiu resp. na technologii 2. vrstvy OSI a vzájemné mapování mezi QoS na 2. a 3. vrstvě modelu OSI. Modely IntServ a DiffServ lze implementovat nad technologiemi ATM a Frame Relay, které pracují pouze na linkové vrstvě.

Provoz je možné značit již na druhé vrstvě modelu OSI. Například rámce, proudící po ethernetovém spoji můžeme značit hodnotou třídy služby CoS (Class of Service) druhé vrstvy, jak je znázorněno na obrázku obr. 3.6.



Obr. 3.6: Značení třídy služby na linkové vrstvě

Hodnoty CoS se pohybují v rozsahu od 0 do 7, ačkoliv společnost Cisco doporučuje nepoužívat hodnoty 6 a 7, protože tyto hodnoty jsou vyhrazeny pro použití v síti, obdobně jako v ToS. Rámec

IEEE 802.1Q používá 3 bity v bajtu Tag Control k označení hodnoty CoS. Implementace priorit do značek rámce proudící přes ethernetový spoj dle IEEE 802.1Q se označuje jako IEEE 802.1p [3].

Důležitá věc, kterou je třeba mít při plánování na paměti, je, že značka CoS zasílaná přes ethernetový spoj neprochází směrovačem. To znamená, že pokud identifikujeme priority provozu pouze pomocí značky CoS, musí být tato značka před průchodem směrovačem, přeznačena na značku třetí vrstvy, jelikož samotný směrovač nemusí brát zřetel na označení na linkové vrstvě. V opačném případě je situace podobná. Je třeba zajistit, aby paket označen s vysokou prioritou byl přeznačen k hodnotě CoS na linkové vrstvě, čímž docílíme plnohodnotné zajištění kvality služeb jak na síťové vrstvě, tak i na vrstvě linkové.

I když společnost Cisco doporučuje značit provoz co nejblíže u zdroje, většinou nebudeme chtít, aby si koncoví uživatelé nastavovali vlastní značku priority. Proto můžeme pomocí přepínačů vytvořit tzv. trust boundary (hranici důvěry), což jsou přepínače v síti, které nedůvěřují příchozím značkám. Výjimkou, kdy nebudeme chtít, aby přístupový přepínač byl na hranici důvěry, je případ, kdy používáme IP telefon připojený přímo k tomuto přepínači. Jelikož většina IP telefonů značkuje pakety, je možné rozšířit hranici důvěry až IP telefonu.

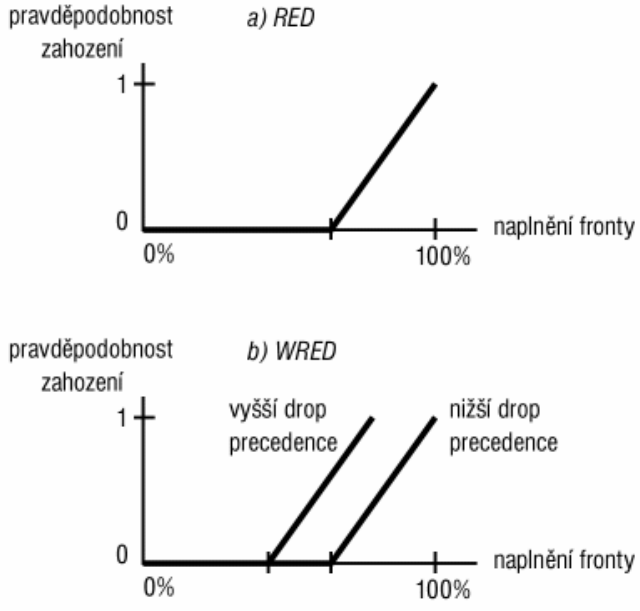
4 PREVENCE PŘED ZAHLCENÍM

Prevence techniky před zahlcením monitorují zátěž sítě ve snaze předvídat a předejít zahlcení, ještě než k němu skutečně dojde. Algoritmy jsou navrženy za účelem zajištění maximální průchodnosti a využití kapacity sítě při snaze o minimalizaci ztrátovosti a zpoždění paketů. Pro pochopení problému si představme větší množství TCP toků sdílejících společný spoj. Nevyužijeme-li žádného ochranného algoritmu, potom v případě zahlcení spoje začne směrovač náhodně zahazovat pakety náležící libovolnému z komunikačních toků, čímž většina koncových uzlů po uplynutí určité doby aktivuje mechanismus opětovného vyslání ztraceného paketu. Uvedený postup vede na problém globální synchronizace v síti, který způsobuje degradaci přenosových rychlostí všech toků, nehledě na jejich prioritu. Algoritmy prevence před zahlcením sledují stav vyrovnávacích pamětí a provádí zahazování paketů pouze u vybraných toků s nejnižší prioritou, proto mohou ostatní toky i nadále procházet bez znatelné degradace rychlosti [6], [1].

4.1 SNÍŽENÍ TOKU ZAHAZOVÁNÍM

Random Early Detection (RED)

Přesáhne-li naplnění fronty určitou mez, začne směrovač zahazovat pakety z náhodně vybraných TCP spojení. Pravděpodobnost zahození paketu se zvyšuje se zvyšujícím se naplněním fronty. Tím dojde ke snížení objemu dat od některých odesílatelů a plynulému vyrovnání celkového objemu přicházejících dat s kapacitou odchozí linky. Cisco IOS využívá jako prostředek prevence před zahlcením algoritmus WRED (Weighted RED) [2]. Jedná se o firemní implementaci algoritmu RED tak, aby využíval hodnotu pole IP Precedence záhlaví IP paketu. Algoritmus RED byl původně navržen pro protokol TCP jako mechanismus adaptivního přizpůsobování rychlosti odesílatele na základě zjištění ztracených rámců. Jestliže dojde k překročení nastavené prahové hodnoty zaplnění fronty směrovače, začnou se náhodně zahazovat pakety TCP datových toků a jejich rychlost se následně sníží. U modifikované metody WRED závisí pravděpodobnost zahození paketu na značce paketu přidělené klasifikací v poli ToS. Limit naplnění fronty, při jehož překročení může být paket zahozen, je různý pro pakety s různými drop precedencemi, tedy značkami PHB.



Obr. 4.1: a) Random Early Detection (RED), b) Weighted Random Early Detection (WRED)

4.2 ŘÍZENÍ POMOCÍ FRONT

Základním obranným mechanizmem, k zabránění zahlcení rozhranní směrovače a poté přerušení propustnosti sítě je pomocí front. Každé rozhranní směrovače i přepínače má svou paměť, do které vkládá pakety či rámce připravené k odeslání. Existují paměti, jak na vstupním rozhranní, tak i na výstupním. Nyní se zaměříme na výstupní fronty, jelikož pomocí nich lze upřednostňovat vybrané toky. Realizace je pomocí vytvoření místo jedné fronty více front, které mají pevně definované priority mezi sebou. Výchozím kritériem pro přiřazení do dané fronty je hodnota DSCP. Metody se liší způsobem obsluhy front.

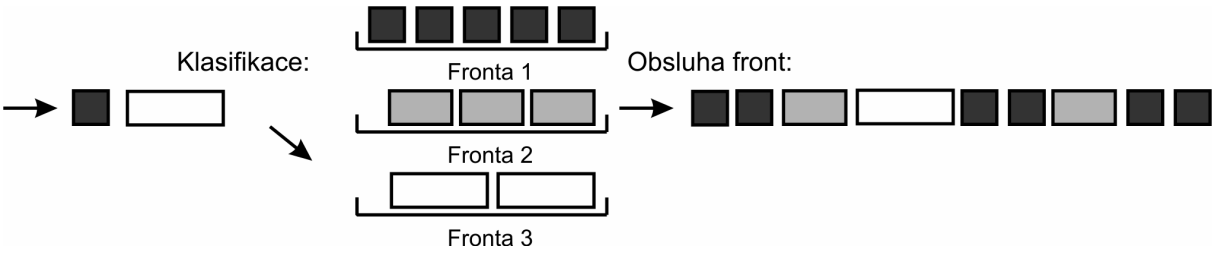
Metoda řazení FIFO

Metoda FIFO ve skutečnosti neprovádí žádné operace QoS. Používá pouze jednu frontu. Jak již název napovídá, první paket, který přijde do fronty, je také první paket, jenž ji opustí. Směrovače používají metodu FIFO ve svých hardwarových frontách. Metoda FIFO v softwarové frontě pracuje stejně jako metoda FIFO v hardwarové frontě. Fronta má omezenou délku, a pokud je zaplněna dojde k zahazování všech dalších příchozích paketů, bez ohledu na jejich hodnotu DSCP. I když je metoda FIFO široce podporovaná na všech platformách IOS, může také vyhladovět provoz tím, že umožní tokům s velkými požadavky na šířku pásma zabrat nespravedlivý díl pásma. Když se například ve frontě současně objeví pakety přenosu souboru FTP a hlasové pakety, přirozeně vysoké požadavky FTP na šířku pásma, mohou vyhladovět hlasové pakety, čímž způsobí znatelné mezery v přenosu telefonního hovoru.

Obr. 4.2: Fronta FIFO

Metoda WFQ (Weighted Fair Queuing)

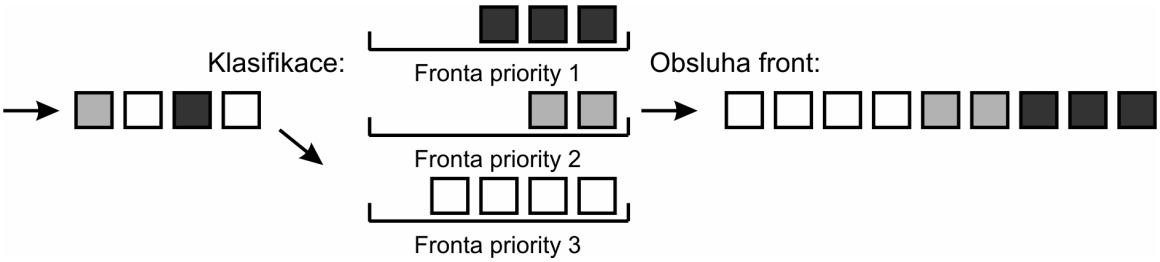
U WFQ jsou průběžně obsluhovány vždy všechny fronty. Žádná fronta nemá vyšší prioritu, než jiná fronta. Jednotlivým frontám je přitom přidělována alikvotní část kapacity výstupní linky podle váhy přiřazené ke každé frontě. Není-li však kapacita přidělená určité frontě právě využívána, může být využita pro obsluhu jiné fronty. Každý paket ve frontě má přidělené pořadové číslo a nižší čísla jdou jako první. Pořadové číslo představuje váhu paketu vynásobenou počtem posunů ukazatele, které je třeba provést, aby byl paket odbaven. Systém Cisco IOS počítá váhu odlišně v závislosti na verzi směrovače IOS. Po skončení obsluhy každého paketu se určí, který z paketů čekající ve frontách má být obsloužen nejdříve. WFQ může být spolu s WRED použito pro implementaci AF PHB.



Obr. 4.3: Řazení front metodou WFQ

Metoda PQ (Priority Queuing)

Na rozdíl od metod řazení FIFO a WFQ, prioritní řazení PQ umožňuje určit provoz s vyšší prioritou a nařídit směrovači, aby daný provoz poslal vždy jako první. Prioritní řazení umísťuje provoz do jednotlivých front. Každé frontě je přiřazena různá úroveň priority a fronty s vyšší prioritou musí být kompletně vyprázdněny dříve, než jakýkoliv paket opustí frontu s nižší prioritou. Této vlastnosti lze využít například pro implementaci expedited forwarding PHB (EF PHB). V tomto případě stačí dvě fronty – jedna pro EF PHB, druhá pro "best-effort" provoz. Tento režim dokáže vyhladovět provoz s nižší prioritou. Je-li zpoždění paketů příliš veliké, jsou navíc v protokolu vyšší vrstvy obvykle považovány již za ztracené a mohou být poslány znovu, čímž dále zatíží počítačovou síť.



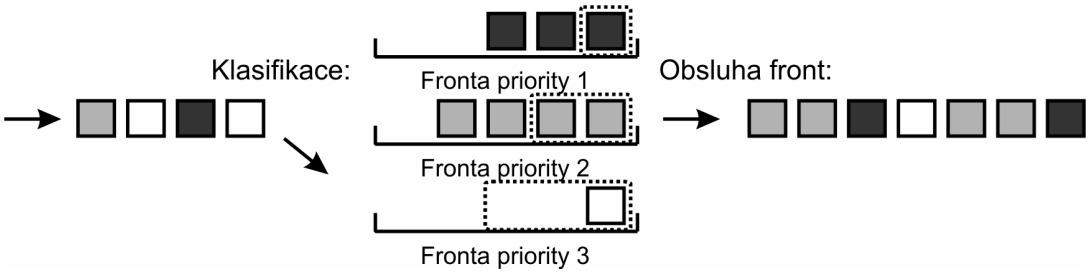
Obr. 4.4: Řazení front metodou PQ

Řazení CB-WFQ (Class-Based Weighted Fair Queuing)

Mechanizmus řazení WFQ od řazení PQ zajišťuje, že žádný provoz nevyhladoví, čili není opomíjen. Nicméně ani řazení WFQ ani PQ nezajistí dostupnost určité velikosti pásma pro definované typy provozu. Pomocí mechanismu CB-WFQ však můžeme určit minimální šířku pásma, která bude pro různé typy provozu dostupná. Řazení CB-WFQ dokáže definovat šířku pásma až pro 64 tříd provozu. Provoz pro každou třídu vstupuje do samostatné fronty. Proto může jedna fronta přetékat, zatímco jiné fronty stále přijímají pakety.

Řazení CB-WFQ tedy nabízí výhodu určit šířku pásma pro různé typy provozu. CB-WFQ také nevyhladoví provoz s nižší prioritou. Rozdělení paketů do tříd lze zajistit pomocí access listu. Podporuje práci jak s polem precedence, tak s DSCP v záhlaví IP paketu. CB-WFQ může být použito například pro implementaci assured forwarding PHB (AF PHB). V tomto případě jsou potřeba čtyři fronty – jedna pro každou třídu AF PHB. CB-WFQ však musí být ještě doplněno dalším mechanizmem pro implementaci drop precedence jednotlivých tříd AF PHB, například WRED.

Jedinou větší nevýhodou je nedostatek mechanizmů pro prioritní řazení. PQ dokáže dát určitému provozu, například hlasu, prioritní zpracování, zatímco řazení CB-WFQ to nedokáže. Tento problém dokáže vyřešit drobná úprava řazení CB-WFQ, která se nazývá LLQ.



Obr. 4.5: Řazení front metodou CB-WFQ

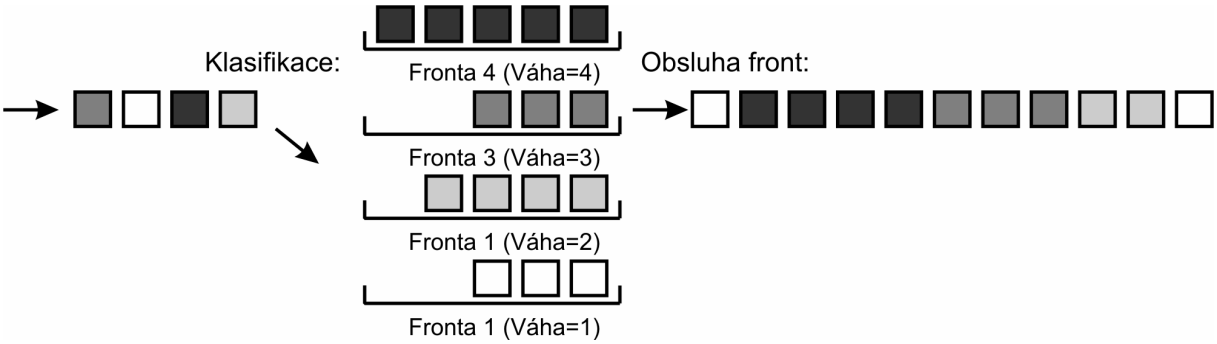
Řazení LLQ (Low Latency Queuing)

Mechanizmus řazení LLQ je kombinací předešlých mechanizmů. Ve skutečnosti je řazení LLQ ve své konfiguraci téměř identické s řazením CB-WFQ. LLQ však může jedné nebo více třídám provozu nařídit směrovat provoz do prioritní fronty.

4.3 ŘAZENÍ NA LINKOVÉ VRSTVĚ

Některé přepínače Cisco Catalyst však také podporují vlastní metodu řazení, která se nazývá WRR (Weighted Round Robin). Například přepínač Catalyst 2950 obsahuje čtyři fronty a metodu řazení WRR lze nakonfigurovat tak, aby umístila rámce s určitým značením CoS do jednotlivých front.

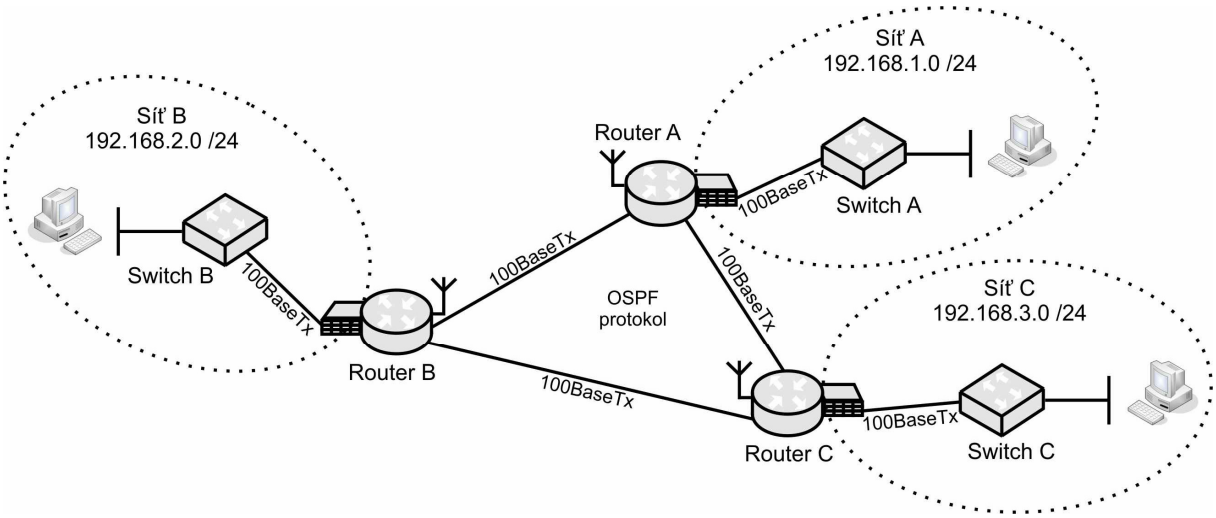
Frontám mohou být přiděleny váhy, které ovlivní, jakou šířku pásma rámce s různým značením dostanou. Princip metody řazení WRR je znázorněn na obrázku obr. 4.6. Každá fronta má stanovené množství rámců, které může poslat během jednoho cyklu. Tedy cyklus začínající ve frontě 1 odešle dle své váhy dané množství rámců, v našem případě pouze jeden a předá oprávnění vysílat frontě číslo 2, která opět vyšle dle své váhy počet rámců. Nejvíce rámců odešle fronta 4, protože má nastavenou váhu 4, čímž je patrné že tato fronta je upřednostňována před ostatními. U této metody nedochází k vyhladovění provozu s nízkou prioritou.



Obr. 4.6: Řazení metodou WRR

5 EXPERIMENTÁLNÍ SÍŤ

Pro vytvoření experimentální sítě k testování podpory kvalitativních služeb byly použity síťové prvky dostupné v laboratoři UTKO. Byly navrženy a následně vytvořeny tři hlavní sítě. Každá síť vlastní svůj místní přepínač, pomocí kterého se připojují koncové stanice využívající různé aplikační služby. Pomocí směrovačů jsou jednotlivé sítě vzájemně propojeny, aby mohly mezi sebou komunikovat. Topologie navržené a následně realizované experimentální sítě je naznačena na obr. 5.1.



Obr. 5.1: Návrh experimentální sítě pro testování kvalitativních služeb

Jádro sítě tvoří tři stejné směrovače Cisco, které simulují síť WAN. V jednotlivých sítích jsou připojena koncová zařízení, která komunikují pomocí více druhů služeb (HTTP, FTP, VoiceIP) a zatěžují tím testovanou síť mezi směrovači. O dosažitelnost mezi sítěmi se stará směrovací protokol OSPF, který je aktivní na všech směrovačích. Všechna kabelová spojení mezi síťovými prvky jsou realizována pomocí krouceného čtyř-páru označovaného UTP Cat-5e. Přenosová rychlost mezi síťovými prvky je maximálně 100Mb/s, je závislá na rozhranní směrovače. Všechny tři směrovače použité v experimentální síti jsou Cisco 1812W.

5.1 IMPLEMENTACE PODPORY KVALITATIVNÍCH SLUŽEB V SMĚROVAČI CISCO 1812W

Směrovače Cisco používají ke své činnosti operační systém IOS. Cisco IOS má charakteristický příkazový řádek (CLI), jehož styl se rozšířil do ostatních síťových produktů nejen od společnosti Cisco. Pomocí CLI lze dosáhnout plného nastavení směrovače přes konzolový vstup. Směrovače podporují i webové rozhraní, kterým lze také provádět některá nastavení. Námi nastavované směrovače Cisco1812W pracují s IOS verzí 12.4. Tento směrovač podporuje řadu protokolů či mechanizmů pro optimální nastavení sítě včetně zabezpečení a podpory různých rozhraní, například disponuje i bezdrátovou technologií. Směrovač má k dispozici dvě Fast-Ethernetová i dvě bezdrátová rozhraní a také jeden integrovaný osmi portový přepínač.

Obr. 5.2: Směrovač Cisco 1812W

Politika QoS v směrovači Cisco

Směrovač Cisco 1812W podporuje problematiku kvalitativních služeb QoS. Pro správnou funkčnost jsou v Cisco směrovačích zavedeny mapy tříd a mapy politik [9]. K nastavení kvalitativních požadavků je třeba provést následující kroky.

QoS se nastavuje modulárně:

- Provoz se klasifikuje jednou nebo více mapami tříd.
- Mapy tříd se uplatní na mapy politik.
- Mapy politik se uplatní na rozhraní jako politiky služby.

Klasifikace provozu prostřednictvím mapy tříd.

Mapa tříd má přidělen libovolný název. Provoz se testuje proti jedné nebo více podmínkám mapy. Standardně musí vyhovovat všem podmínkám (match-all), pak bude paket prohlášen za paket dané třídy. Nebo lze zvolit (match-any) a poté stačí, aby vyhovoval pouze jedné z definovaných podmínek třídy. Příkaz k vytvoření mapy tříd:

(global) class-map *název_třídy*

Shoda s danou třídou se definuje příkazem match. Volbou přepínače příkazu match je možné definovat shodu s IP precedencí, protokolem sedmé vrstvy ISO OSI, konkrétní adresou IP, hodnotou CoS a další. Přiřazení hodnoty CoS do třídy je možné definovat, ale z důvodu nekompatibility s naším rozhraním směrovače ji nelze dále použít. Příklad nastavení mapy tříd použité v experimentální síti je zobrazen na obr. 5.3.

```
class-map match-any voice_ip
 match protocol rtp audio
class-map match-any video_real
match protocol rtp video
class-map match-any www
 match protocol http
class-map match-any video_stream
match protocol udp 1234
class-map match-any file
 match protocol ftp
```

Obr. 5.3: Výpis map tříd

Použili jsme pět základních tříd rozdělených pro přenos hlasu, videa v reálném čase, webový provoz, video-služby a datový přenos souborů. Ve všech třídách je pro určení shody použit daný protokol nebo konkrétní port, který daná služba využívá.

Nastavení mapy politik

Vytvoření mapy politiky se provede příkazem:

(global) policy-map *název_politiky*

Mapa politiky definuje chování jednotlivých tříd provozu. Politika musí vlastnit minimálně jednu třídu. Maximální počet tříd je omezen na 64. Přidělení třídy do konkrétní politiky se provede příkazem:

(pmap) class *název_třídy*

Pokud je paket klasifikován a přiřazen přes třídu do politiky, lze nyní nastavit chování dané třídy a její chování vůči ostatním třídám v dané politice. V politice lze provádět přeznačení paketu na odlišnou precedenci a nastavit například minimální šířku pásma pro danou třídu provozu. Také lze zvolit mechanizmus pro obsluhu a následné zahazování paketů z fronty při přetečení. Nastavení šířky pásma pro danou třídu se aplikuje pomocí přesně definované přenosové rychlosti, anebo pomocí procentuálního vyjádření k celkové přenosové rychlosti rozhraní. Pro využití 25% šířky pásma rozhraní použijeme příkaz:

(pmap-class) percent 25

Jako výchozí metoda obsluhy front je nastavena metoda LLQ, která upřednostňuje pakety s vyšší preferencí a zároveň nevyhladoví pakety s nižší preferencí. Další z nabízejících se možností v Cisco 1812W je metoda CB-WFQ. Příklad nastavení mapy politik použité v experimentální síti je zobrazen na obr. 5.4.

```
policy-map Policy5
  class voice_ip
    set dscp cs5
    priority percent 10
  class video_real
    set dscp cs4
    priority percent 20
  class www
    set dscp cs3
    priority percent 20
 class video_stream
    set dscp cs2
    priority percent 20
  class file
    set dscp cs1
    priority percent 5
 class class-default
    set dscp default
```

Obr. 5.4: Výpis map politik

V tomto příkladu na obr. 5.4 jsou jednotlivým třídám provozu procentuelně nastaveny minimální šířky pásma, které budou garantovány dané třídě. Dále jsou všechny pakety značkovány prioritou DSCP vyjádřenou pomocí IP precedence.

Přiřazení mapy politik k rozhraní

Vytvořenou politiku je třeba aplikovat k rozhraní směrovače. K rozhraní se přiřadí zvolená mapa politiky. Každé rozhraní může mít přiřazenu pouze jednu mapu politiky. Lze přiřadit politiku pro aplikování v příchozím nebo odchozím směru. Příkaz pro přiřazení odchozí politiky k rozhraní:

(interface) service-policy output *název_politiky*

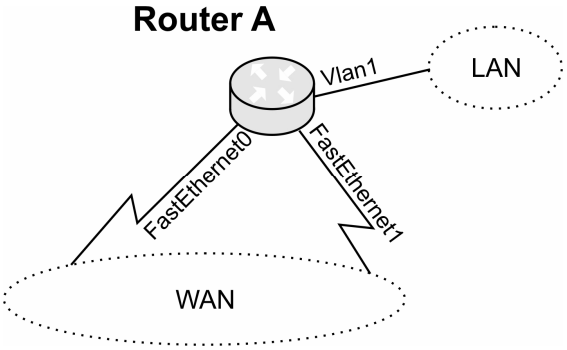
Příklad výsledného nastavení přiřazení politik k rozhraní použité v experimentální síti je zobrazen na obr. 5.5.

```
interface FastEthernet0
service-policy output Policy5
interface FastEthernet1
service-policy output Policy5
```

Obr. 5.5: Výpis přiřazení politiky k rozhraní směrovače

Námi dříve vytvořená politika Policy5 je přiřazena k rozhraním směrovače FastEthernet0 i FastEthernet1, které jsou spojeny s páteří sítě, viz obr. 5.6. V obou případech ve výstupním směru.

Pro zajištění kvalitativních služeb v celé experimentální síti jsou jednotlivé třídy a mapy politik nastaveny na všech směrovačích, čímž je dosaženo shodné zacházení s přenášenými pakety mezi vzdálenými sítěmi.

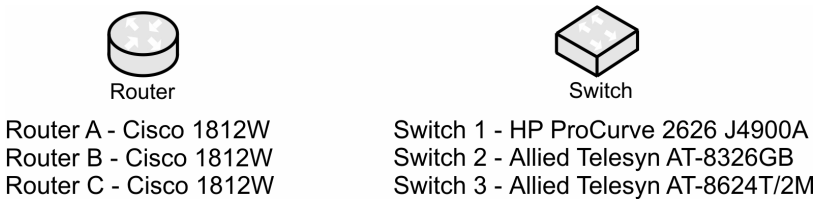


Obr. 5.6: Využitá rozhranní směrovače A

5.2 MOŽNOSTI NABÍZEJÍCÍ L3 PŘEPÍNAČE PRO KVALITU SLUŽEB

Díky svému rozšíření v Ethernetu se pojem přepínač vžil pro rychlý prvek rozhodující o dopravě rámců. Když se pak objevily Ethernetové přepínače s rozšířenými funkcemi, které dokázaly analyzovat protokol IP a fungovat téměř jako směrovače. Začal se pro ně používat pojem L3 přepínače. L3 zde označuje 3. vrstvu modelu OSI, na které takové zařízení dokáže pracovat. Původní L3 přepínače byly velmi rychlé a jednoduché. Typicky měly jen velmi omezenou podporu směrovacích protokolů a veškerých pokročilých funkcí. Postupem času se jejich schopnosti rozšiřovaly a v současnosti se pojem L3 přepínač používá víceméně jako synonymum pro směrovač.

V experimentální síti jsou zapojeny tři přepínače. Na obr. 5.7 jsou uvedeny modely použitých síťových prvků v síti včetně výrobce. Jednotlivé přepínače používají odlišný styl konfigurace, jak v příkazovém režimu přes konzoli, tak i v odlišném webovém rozhraní. Jelikož nejde o stejné modely, tak i podpora různých mechanizmů k realizaci kvalitativních služeb je velmi odlišná.



Obr. 5.7: Použité modely síťových prvků

Konfigurace přepínačů se provádí přes sériové rozhraní pomocí příkazového režimu. V každém přepínači jsou odlišné příkazy. Je možné aktivovat webové rozhranní na které je možné se připojit přes internetový prohlížeč z koncové stanice. U přepínačů Allied Telesyn dosahuje webové rozhranní stejných konfiguračních možností jako příkazový režim. Zato u přepínače HP ProCurve2626 je webové prostředí ochuzeno o řadu dalších možností nastavení včetně podpory QoS.

HP ProCurve 2626 J4900A

HP ProCurve Switch 2626 je kompaktní nastavitelný přepínač. Nabízí 24 portů 10/100 Mb/s a 2 výkonnější porty 10/100/1000 Mb/s. Disponuje nastavitelnými funkcemi jak na vrstvě linkové, tak i na vrstvě síťové. Lze zapnout podporu webového prostředí, které nedosahuje plné možnosti

konfigurace. K plné konfiguraci přepínače je třeba aktivovat službu telnet, nebo použít terminál připojený pomocí sériového rozhraní. Samotná konfigurace se provádí pomocí příkazového prostředí podobající se Cisco IOSu.

Obr. 5.8: Přepínač HP ProCurve 2626

Problematika QoS v přepínači HP ProCurve je řešena. Nedosahuje takových možností na síťové vrstvě jako u směrovače Cisco, ale podporou linkové vrstvy disponuje oproti směrovači Cisco 1812W, který nepodporuje CoS u námi použitých rozhranní. Je možné definovat metodu používanou k označování pomocí IP precedence (první 3bity v ToS) nebo DSCP (prvních 6bitů v ToS). Lze nastavit přímé mapování mezi DSCP hodnotou v ToS a hodnotou 802.1p v CoS. Pakety směřující na konkrétní IP adresu je možné také přeznačit pomocí priorit DSCP či IP precedenci. Přepínač nabízí možnost klasifikovat jednotlivé porty TCP a UDP paketů a přiřadit jim libovolnou prioritu DSCP. Jednotlivé možnosti nastavitelné v přepínači HP ProCurve jsou znázorněny na obr. 5.9.

```
SwitchA(config)# qos
 udp-port              Set UDP port based priority.
 tcp-port              Set TCP port based priority.
 device-priority       Configure device-based priority.
 dscp-map              Define mapping between a DSCP (Differentiated-Services
                       Codepoint) value and an 802.1p priority.
 resources             For 10/100 ports, groups of 8 adjacent ports share a
                       pool of port resources.
 type-of-service       Configure the Type-of-Service method the device uses to
                       prioritize IP traffic.
```

Obr. 5.9: Podpora QoS v přepínači HP ProCurve 2626

Přepínač řeší problematiku kvalitativních služeb pomocí mapování hodnot priorit z linkové vrstvy na síťovou vrstvu a opačně. Výsledkem nastavení QoS v přepínači HP je, že odchozí provoz má zapsanou hodnotu priority v poli ToS v paketu či CoS v rámci. Podle hodnot priorit je schopen rozdělit provoz do tří front (HI, MED a LOW).

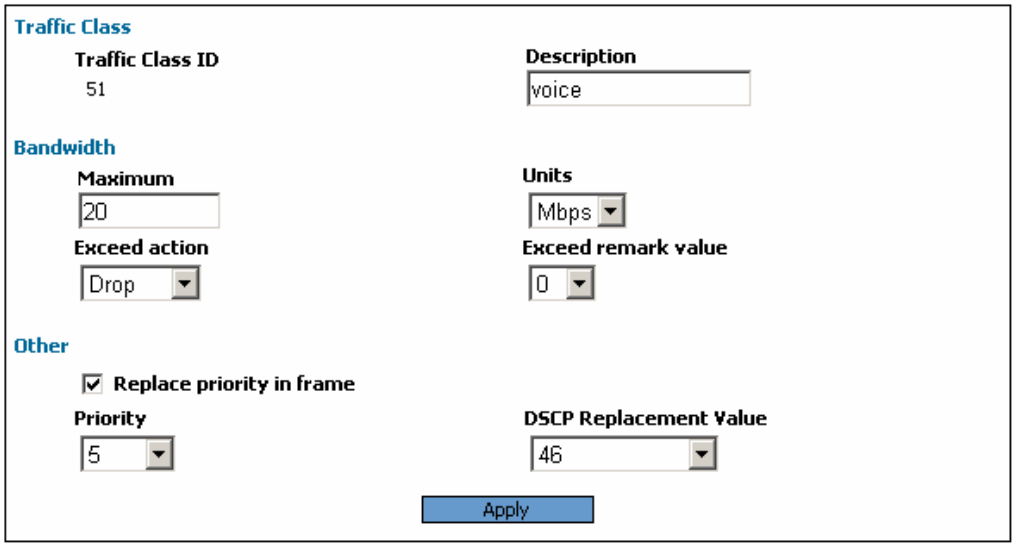
Allied Telesyn AT-8624T/2M

Přepínač Allied Telesyn AT-8624T/2M disponuje velkou řadou možností. Jeho možnosti sahají na úroveň směrovačů. Podporuje standardní směrovací protokoly, STP (Spanning Tree Protocol) a další síťové možnosti i technologie. Nabízí 24 portů 10/100 Mb/s a 2 rychlejší porty 10/100/1000 Mb/s. Základní konfigurační přístup je pomocí sériového rozhraní. Pohyb v příkazovém prostředí je odlišný od politiky Cisco IOS. Po aktivaci webového rozhraní je možné veškeré nastavení provádět přes webový prohlížeč z libovolné stanice v síti.

Obr. 5.10: Allied Telesyn AT-8624T/2M

Společnosti Allied Telesyn implementovala podporu QoS do produktu AT-8624T/2M, jak na vrstvu linkovou, tak i síťovou. Princip realizace nastavení QoS je hodně podobný Cisco směrovači. Nejprve je třeba pomocí klasifikátoru vybrat pakety či rámce. Klasifikovat je možné podle mnoha kritérií. Od hodnot CoS či ToS přes IP adresy, až po aplikační porty TCP a UDP. Klasifikovaný provoz se přiřadí k třídě provozu, v které se definují parametry zacházení, případně limitování s ohledem na výstupní provoz. Definuje se maximální přenosová rychlost a případně přeznačení pole

DSCP v paketu či CoS v přenášeném rámci, viz obr. 5.11. Všech 26 portů může mít přednastavenou odlišnou politiku QoS. Konfigurace a orientace je členěna pomocí čísel, čímž se celková správa a ohled nad správným nastavením kvalitativních služeb stane dosti nepřehledná.



Obr. 5.11: Zacházení s třídou provozu v přepínači Allied Telesyn AT-8624T/2M

Switch Allied Telesyn AT-8326GB

Středně velký model AT-8326GB je 24portový 10/100Mb/s řízený Fast Ethernet přepínač se dvěma rozšiřujícími GBIC sloty a dvěma 1000Mb/s pevnými porty. Přepínač 8326GB je stohovatelný s podobnými produkty prostřednictvím dodaného kabelu až do celkového počtu 144 portů. Svými funkcemi se řadí mezi jednodušší konfigurovatelné přepínače pracující pouze na linkové úrovni. Správa přepínače je pomocí sériového rozhraní. Je možné aktivovat webové prostředí, které je mnohem přehlednější k správě a dohledu nad celým přepínačem a umožňuje stejné možnosti konfigurace.

Obr. 5.12: Přepínač Allied Telesyn AT-8326GB

Podporu kvalitativních služeb přepínač AT-8326GB realizuje pouze na linkové úrovni. K upřednostnění provozu používá dvě výstupní fronty (HI a LOW). Přiřazení určitého provozu do vybrané fronty se definuje podle hodnoty CoS v přenášeném rámci nebo dle použitého fyzického portu. Konfigurace QoS v přepínači AT-8326GB je znázorněna na obr. 5.13.

Priority	Queue
0	Low: ◉ High: ○
1	Low: ◉ High: ○
2	Low: ◉ High: ○
3	Low: ◉ High: ○
4	Low: ○ High: ◉
5	Low: ○ High: ◉
6	Low: ○ High: ◉
7	Low: ○ High: ◉

Obr. 5.13: Přiřazení priority k frontě v přepínači AT-8326

5.3 DATOVÝ PROVOZ V EXPERIMENTÁLNÍ SÍTI

K ověření zacházení s datovým provozem v závislosti na nastavení kvalitativních parametrů v jednotlivých síťových zařízeních bylo třeba k dané páteřní síti připojit koncová zařízení. Aby bylo možné upřednostňovat jednu službu před druhou, bylo navrženo několik datových služeb, s kterými je možné se i setkat v komerční síti.

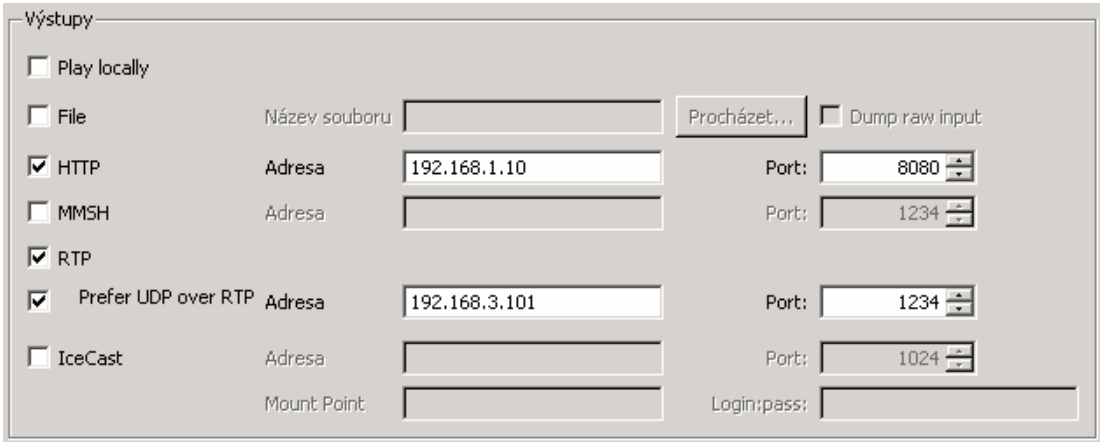
Realizované datové služby:

- Přenos souborů
- Sledování videa
- Provoz www
- Video v reálném čase
- Hlas v reálném čase

K realizaci jednotlivých služeb bylo třeba nainstalovat servery, které by byly schopny danou službu distribuovat v celé experimentální síti. Servery musí být dostupné z kterékoliv klientské stanice z vytvořených sítí. Dosažení konektivity mezi klientskými stanicemi přes páteřní síť nám zajišťují směrovače. V naší experimentální síti není nikde aplikován žádný síťový firewall, tudíž s konektivitou nebyl problém. K dosažení plné konektivity v komerčních sítích je třeba se zabývat i problematikou firewallu.

Přenos souboru byl realizován mezi FTP serverem a klientskými počítači. FTP server byl realizován instalací aplikace Serv-U od společnosti RhinoSoft na server v laboratoři UTKO od firmy AutoCont s operačním systémem Microsoft Windows Server 2003. FTP server podporuje webový přístup ověřený pomocí uživatelského jména a hesla. Software nabízí spoustu možností nastavení jak uživatelů, tak i samotného serveru. Přenos souborů pomocí FTP serveru probíhá pomocí protokolu FTP na portu TCP 21.

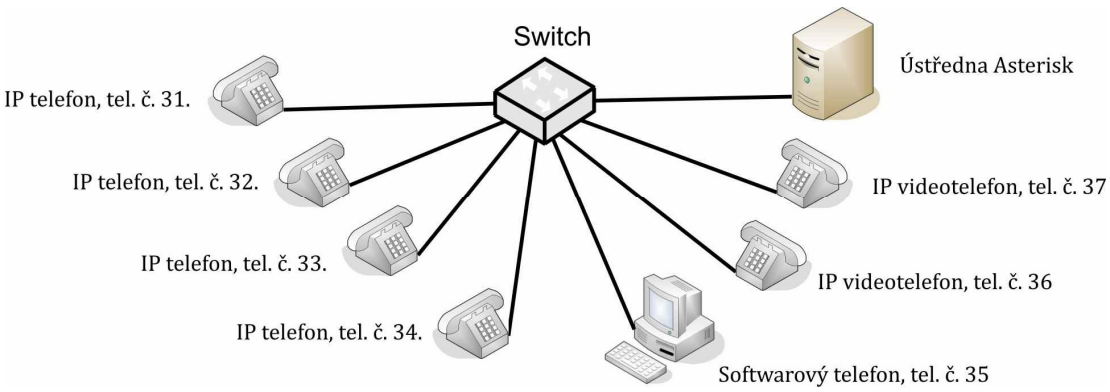
Sledování videa je možné realizovat mnoha způsoby. Nejpoužívanější způsob je pomocí multicastové adresy. Zdroj videa vysílá do sítě video pomocí známé multicastové adresy, která je směrována až ke klientské stanici, která si jej předem vyžádala. Tento scénář je nejefektnější, ačkoli je třeba proniknout do problematiky předávání multicastových adres mezi směrovači a distribuci pouze k stanicím, které si video vyžádali. Jednodušší varianta je pomocí konkrétní IP adresy příjemce. V tomto případě zdroj videa začne vysílat datový tok videa a všechny pakety mají v IP hlavičce uvedenou adresu příjemce. Video je směrováno sítí až k příjemci i v případě že příjemce video nechce přijímat. Jako zdroj vysílání byl použit software VideoLAN, který umožňuje přehrát video-soubor nebo připojit externí zařízení např. video kartu a distribuovat TV signál do počítačové sítě. Software nabízí distribuci videa do sítě několika způsoby, viz obr. 5.14. Z důvodu možnosti zasílat více video přenosů současně byl použit k přenosu protokol UDP na portech 1234,1235 a 1236. Video přenosu je možné definovat průměrnou přenosovou rychlost. V našem případě byla přenosová rychlost videa volena mezi hodnotami 700kb/s až 8Mb/s.



Obr. 5.14: Volby nastavení výstupního videa pomocí aplikace VideoLAN

Provoz www je v dnešních komerčních sítích velmi rozšířen. Pomocí internetového prohlížeče generuje koncový uživatel provoz využívající protokol http. K vytvoření www spojení je třeba se připojit na konkrétní server, na němž běží webová aplikace. Ke generování provozu www v experimentální síti byl použit opět software VideoLAN, který podporuje odesílání videa prostřednictvím protokolu http. K přesné identifikaci byl použit port 8080. Použitím tohoto softwaru je možno regulovat datový tok přenosu stejně jako v případě přenosu videa pomocí protokolu UDP.

Služby v reálném čase se stále více používají a je třeba jim zaručit přednost před ostatním provozem. Pokud dochází k zahazování, ztrácejí tyto služby svůj významu a spolehlivost. Dostupné terminály, v laboratoři UTKO využívající reálné služby, jsou telefony IP. K navázání komunikace mezi IP telefony je zapotřebí spojovací ústředna. Proto byl vybrán jeden počítač v laboratoři UTKO na který byl zaveden operační systém Linux a nainstalována telefonní ústředna Asterisk podporující telefony IP komunikující pomocí SIP protokolu. IP telefon připojený do experimentální sítě má přednastavenu IP adresu telefonní ústředny, kam se pomocí uživatelského jména a hesla snaží přihlásit a zaregistrovat. Potvrzení registrace zasílá ústředna až po kontrole údajů se svou místní databází uživatelů definovanou v souboru sip.conf. Autorizační a řídící informace se přenáší pomocí protokolu SIP. Každý uživatelský účet má své jedinečné telefonní číslo vedené v ústředně, neboli každý telefon se přihlašuje pod svým jménem, tudíž každý IP telefon má své telefonní číslo. IP telefon je reprezentován telefonním číslem nikoli IP adresou, čímž je dosažena přenositelnost telefonů do sítí s odlišnou IP adresací. Musí však být zachována konektivita s telefonní ústřednou. Konfigurace spojování na základě telefonního čísla je uložena v souboru extensions.conf .

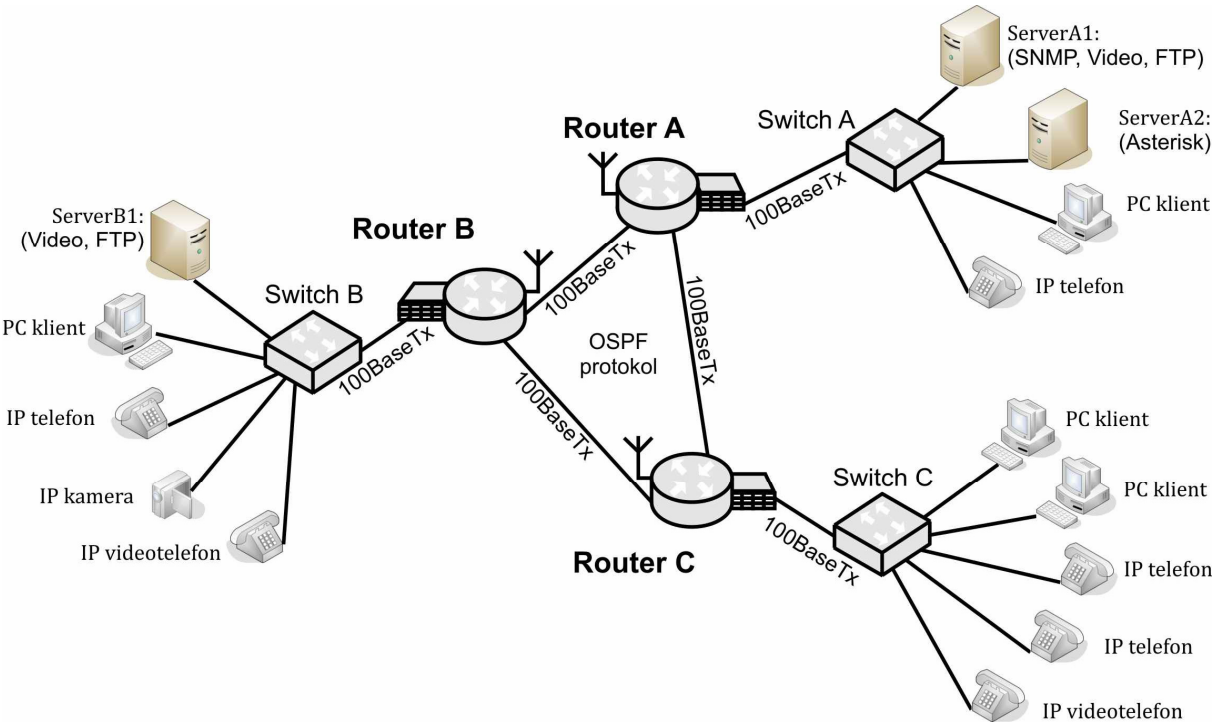


Obr. 5.15: SIP doména

IP telefony jsou výhradně určeny pro přenos hlasu. Některé modely podporují i přenos videa snímané integrovanou kamerou, označují se za videotelefony. V laboratoři UTKO byla nastavena telefonní ústředna Asterisk tak, aby bylo možné realizovat hovor mezi všemi terminály. K dispozici

bylo celkem šest terminálů. Čtyři klasické IP telefony a dva videotelefony. Lze využít i terminál v podobě aplikace spuštěné na stolním počítači. Samostatné schéma SIP domény a použitých terminálů v experimentální síti je znázorněno na obr. 5.15. Terminály nabízí možnost konfigurace pomocí webového rozhraní, kde k správné autorizaci s ústřednou stačí pouze správně vyplnit IP adresu ústředny, uživatelské jméno s heslem, které je shodné s databází v ústředně a zvolit komunikační port s ústřednou, defaultně 5060.

Jednotlivé služby provozu byly implementovány do experimentální sítě. K původní topologii byly přidány zmiňované servery, na kterých byly spuštěny serverové aplikace. Dále byly připojeny koncové stanice. Všechny koncové stanice prošly reinstalací operačního systému a následnou instalaci potřebného softwaru. Po doladění síťových ovladačů pro některé síťové karty, byly stanice připraveny k provozu. Výsledná topologie včetně koncových terminálů je znázorněna na obr. 5.16.



Obr. 5.16: Topologie experimentální sítě včetně koncových terminálů

K dosažení správného zacházení s pakety v závislosti na kvalitativní služby bylo potřeba přesně identifikovat jednotlivé pakety. S ohledem na výchozí nastavení jednotlivých serverů byly stanoveny jednotné podmínky používání komunikačních portů pro celou experimentální síť. V tab. 5.1 je stanoven seznam výhradně použitých portů za účelem testování podpory QoS. Některé služby typu přenosu dat či provozu www mají rezervovány standardní porty spolehlivého přenosu TCP 21 a 80. K datovým službám sledování více videí byly zvoleny nespolehlivé protokoly UDP 1234, 1235 a 1236. Služby v reálném čase mají též možnost výběru portu pro danou komunikaci. Definice se provádí přímo na serveru v konfiguraci ústředny Asterisk. Pro videotelefonii je použit port UDP 5006 a pro přenos hlasu byl zvolen port UDP 5004. Provoz IP kamery je hodnocen jako služba v reálném čase. K připojení na kameru je použit protokol http, ale pro sledování videa z kamery je použit nepotvrzovací protokol UDP na portu 9001.

Tab. 5.1: Vyhrazené porty pro jednotlivé datové služby v experimentální síti

Služba	Port
Přenos souborů	TCP 21
Sledování videa	UDP 1234
	UDP 1235
	UDP 1236
Provoz www	TCP 80
	TCP 8080
Video v reálném čase	UDP 9001
	UDP 5006
Hlas v reálném čase	UDP 5004

5.4 CHOVÁNÍ EXPERIMENTÁLNÍ SÍTĚ PŘI ZATÍŽENÍ DATOVÝM PROVOZEM

Po správném propojení kabeláže a instalaci všech druhů služeb v laboratoři UTKO byla experimentální síť spuštěna. Výrazným vlivem na chování sítě byl parametr využitelnosti šířky pásma. Všechna propojení mezi směrovači i koncovými účastníky byla propojena rychlostí 100Mb/s. Takové množství šířky pásma většina aplikací ani nedokáže využít. V našem případě tuto šířku pásma dokáže zcela vyčerpat pouze služba přenosu souboru pomocí FTP. Ostatní realizované služby jsou v ohledu na šířku pásma limitováni. Sledování videa pomocí aplikace VideoLAN dokáže vysílat datový tok maximálně 8Mb/s. Využitelná šířka pásma pro komunikaci IP telefonu je cca 170kb/s. Komunikace videotelefonu je také dostatečně komprimovaná a potřebuje k bezchybné komunikaci rychlost cca 400kb/s. IP telefony jsou navrženy, aby mohly být bezchybně použity i ve spojích s nízkou přenosovou rychlostí. Výrazného zatížení bylo dosaženo spuštěním stejné služby vícekrát. Například jedna koncová stanice přijímala více videí a zároveň přijímala datový tok z vzdálené IP kamery. Video server musel vysílat až několik odlišných datových toků, aby došlo k výraznému využití přenosové rychlosti. Hlasových terminálů bylo k dispozici celkem šest. K dosažení dvojnásobného datového zatížení rozhraní bylo v konfiguraci ústředny nastaveno, aby hlasová komunikace byla zasílána ústředně, a ta jej následně přesměruje k volanému terminálu. Celkový datový tok vygenerovaný všemi IP telefony i videotelefony činil 2,1Mb/s.

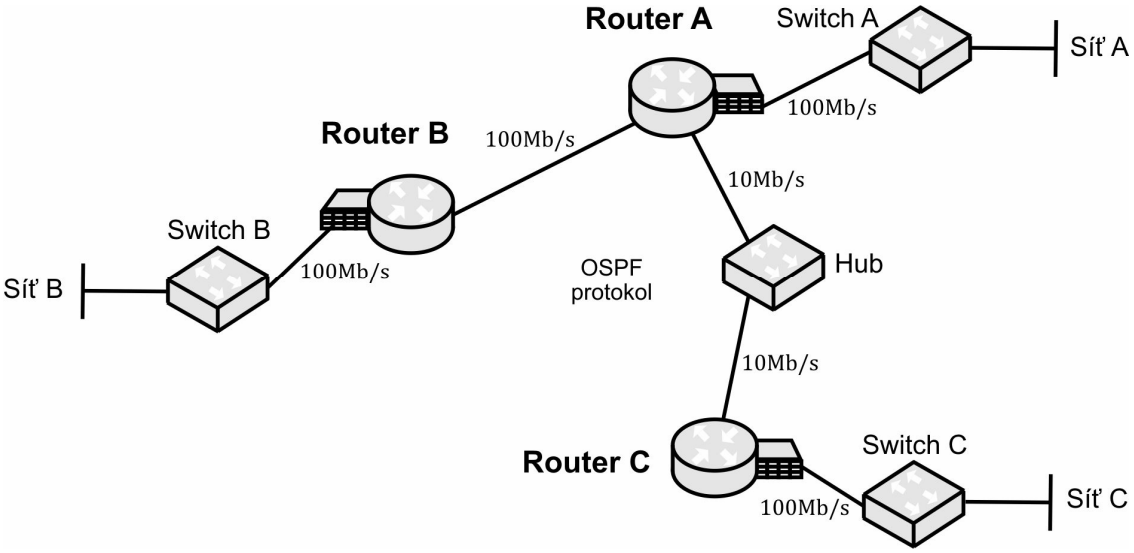
Přenosovou šířku pásma 100Mb/s v celé experimentální síti bylo poměrně složité zaplnit. Významnými generátory dat byly pouze video servery, které dokážou generovat tok s přednastavenou rychlostí. FTP přenos používá k spojení spolehlivý protokol TCP. Musí zaručit, aby žádný paket nebyl ztracen. Dle zbývající dostupné rychlosti FTP přenos vyplní zbývající pásmo a mění svou přenosovou rychlost v závislosti na četnost negativních potvrzení.

Byla snaha donutit směrovače k zahazování paketů z důvodu upřednostnění podle nastavených parametrů kvalitativních služeb. Jelikož rozhraní směrovače připojena k lokálním sítím nepodporují řazení do více front a zahazování dle QoS, byla snaha donutit zahazovat pakety na rozhraní, které více front podporují, tedy rozhraní směrovačů připojená k páteřní síti. Směrovače byly navzájem propojeny prakticky každý s každým. Tudíž provoz byl směrován podle nejlepší metriky dle směrovacího protokolu a nebylo možné prakticky přetížit výstupní rozhraní směrovače připojené k páteřní síti. Prvotní upřednostnění a využití šířky pásma bylo provedeno již na prvním síťovém prku, čímž byl přepínač. Přepínač přeposílal rámce od koncových stanic směrem k směrovači pomocí 100Mb/s rychlé linky. Tento datový tok již nebylo třeba nijak zpracovávat v směrovači, protože další přenosová cesta

linky měla kapacitu také 100Mb/s. K zahazování mohlo docházet pouze při konkrétním nastavení maximální rychlosti pro danou službu v síťovém prvku. Čímž došlo k snížení zátěže nikoli k zahození z důvodu upřednostnění jednotlivých paketů.

Abychom docílili požadovaného zahazování na rozhraní a ověřili zacházení směrovače s různým druhem provozu na základě nastavených podmínek QoS, museli být provedeny změny v topologii, viz obr. 5.17. Přerušením linky mezi směrovači B a C byl datový tok ze sítě B vždy směrován přes směrovač A. Poté veškerý provoz směrující do sítě C musí propouštět rozhraní na směrovači A. Rozhraní muselo začít řešit výstupní limity především v přenosové rychlosti. Při plném zatížení obou vstupních linek začal směrovač redukovat datový tok na jednu výstupní linku o přenosové rychlosti 100Mb/s. Směrovač začal jednotlivé datové pakety klasifikovat a upřednostňovat dle nastavené politiky QoS.

S ohledem na použité terminály v laboratoři UTKO bylo třeba vyvážit jednotlivé toky datových služeb. Reálné služby (IP telefony) byly schopny vyprodukovat celkový maximální datový tok 2,1Mb/s. S porovnáním s dostupnou šířkou pásma linky 100Mb/s by se měření muselo omezit pouze na datové služby video přenosu a stahování souborů z FTP serveru. Podmínky procentuálního využití šířky pásma pro služby v reálném čase byly vyřešeny degradací šířky pásma. Směrovače A a C byly propojeny pomocí rozbočovače s maximální šířkou pásma 10Mb/s. Kromě desetinásobného snížení přenosové rychlosti byla propustnost dále snížena z důvodu vynuceného poloduplexního způsobu přenosu na spoji namísto původního duplexního způsobu provozu. Nově vzniklá topologie k měření zacházení s různým druhem provozu je zobrazena na obr. 5.17. Vložení síťového prvku bylo zvoleno z důvodu nesprávného chování softwarového limitu nastaveného v směrovači.



Obr. 5.17: Topologie experimentální sítě se spojem se sníženou přenosovou kapacitou 10 Mb/s.

5.5 OVĚŘENÍ FUNKČNOSTI SMĚROVAČE CISCO PRO RŮZNÁ NASTAVENÍ QOS PARAMETRŮ

5.5.1 Klasifikace paketů podle datové služby

Jednotlivé realizované datové služby v experimentální síti byly seřazeny dle priority. Třídy priorit jsou definované v paketu hodnotou IP precedence v poli ToS. Navržené priority jsou uvedeny v tab. 5.2.

Tab. 5.2: Navržené třídy priorit

Třída priority	Služba	IP precedence	Hodnota DSCP	Binární vyjádření
Kritická	Hlas v reálném čase	CS 5	46	101 110
Upřednostněná	Video v reálném čase	CS 4	32	100 000
Rychlá	Provoz www	CS 3	24	011 000
Okamžitá	Sledování videa	CS 2	16	010 000
Přednostní	Přenos souborů	CS 1	8	001 000
Normální	Ostatní provoz	CS 0	0	000 000

Pomocí počítačové aplikace byly zachytávány pakety. Protokolový analyzátor Wireshark umožňuje analyzovat hlavičku IP paketu a zobrazit hodnotu bajtu ToS. Jednotlivé provozy byly úspěšně ověřeny, zda dochází ke správné klasifikaci jednotlivých paketů.

Obr. 5.18: Analýza paketu při FTP přenosu

Názorná analýza přijatého paketu pomocí programu Wireshark je znázorněna na obr. 5.18. Byl zachycen paket přenášející FTP data. Na obr. 5.18 je detailně zobrazena část paketu nesoucí informaci o prioritě reprezentující údajem DSCP. Hodnota DSCP byla 001000 (0x08). Tento údaj je i vyjádřen pomocí IP precedence CS 1 (Class Selector). Klasifikaci provedl směrovač, protože při použití analyzátoru ve vysílací stanici (Serveru FTP), údaj DSCP v stejném paketu byl původně nastaven na hodnotu 0.

Nastavení QoS pro jednotlivá koncová zařízení

Všechny pakety v síti mají svého odesílatele. Značkování paketů je možné nastavit přímo v některých terminálech. Všechny použité IP telefony nabízejí možnost nastavit prioritu na síťové i linkové vrstvě. Hodnoty DSCP byly nastaveny dle tab. 5.2. Hodnota linkové priority po IP telefony byla volena na hodnotu CoS = 5. Použitá IP kamera ASUS CX200 prioritu paketu neřeší. Možnosti nabízející koncové počítačové stanice nejsou v této práci řešeny. Klasifikace je zajištěna v směrovači dle užitých protokolů a portů.

5.5.2 Nabízející se možnosti při zahazování paketů v směrovači

Chování při vypnuté podpoře QoS

Pokud nebylo na rozhraní směrovače A aplikované žádné pravidlo QoS, směrovač nebral ohled na prioritu provozu. Dokud dostupná šířka pásma 10Mb/s nebyla značně využita, datové služby měly rychlou odezvu. Přenos hlasu byl plně dostačující pro realizaci hovoru s minimálním zpožděním.

Při dosažení zatížení linky na 80-90% začal směrovač některé pakety zahazovat. Nebral ohled na hlavičku v bajtu ToS. Služby sledování videa začaly mít lehké výpadky v obraze. Odezva na www aplikace byla zvýšena. Při komunikaci IP telefonů začínalo docházet k výpadkům v hlase a časovému zpoždění. Obraz pořízený videotelefony je místy trhaný s občasnými výpadky. Obraz pořízený vzdálenou IP kamerou začínal mít obrazové vady. Celkově jednotlivé datové služby byly dostupné s nahodilými výpadky, které bylo možné tolerovat.

K úplnému vytížení a zároveň zahlcení přenosové linky byl použit datový tok videa. K již zatíženému rozhraní z předchozího měření byla přidána datová služba zasílání videa s velkou šířkou pásma (video tok 8Mb/s). Bylo generováno úmyslně za účelem simulovat přetížení. Ethernetové

rozhraní směrovače s šířkou pásma 10Mb/s signalizovalo využití linky hodnotou 100%. Začalo docházet k velkým výpadkům všech použitých datových služeb. Po krátké době byly služby nedostupné. Přenos hlasu mezi IP telefony přestal probíhat. Obraz videotelefonu se zastavil a přestal se obnovovat. Webové služby se staly nedostupné. Přenos souborů byl z důvodu nedostupnosti serveru přerušen.

Počítačová síť, která neřeší problematiku upřednostňování datových služeb, nabízí dostupnost všem datovým službám, dokud nedojde k nadměrnému přenosu dat, který začne využívat celou dostupnou šířku pásma. Předcházet zahlcení v sítích bez podpory QoS je ve správném dimenzování přenosových spojů v závislosti na poskytované služby v počítačové síti.

Diagnostika chování při zapnuté podpoře QoS

Směrovač Cisco 1812W nabízí možnost monitorování některých QoS informací v reálném čase. Pomocí webového rozhraní a programu Cisco SDM (Security Device Manager) je možné sledovat aktuální stav směrovače. Program nabízí i sledovat aktuální chování problematiky QoS. Zobrazené hodnoty aktuálního stavu aktivity na daném rozhraní jsou vykreslena do grafu v aplikaci SDM. Prioritu obnovení hodnot lze volit mezi 5 až 30 vteřinami. Změřené a následně vynesené hodnoty v grafu jsou průměrovány s ohledem na předchozí stavy. Výsledné hodnoty se pouze přibližují s určitou setrvačností k reálnému dění. K ověření, které datové toky začne směrovač zahazovat, je toto znázornění dostačující.

Směrovač Cisco 1812W nabízí dvě varianty mechanizmů pro řazení do výstupních front. Jedná se o mechanizmy CB-WFQ a LLQ. Účelem měření bylo ověřit chování obou mechanizmů. Tyto mechanizmy jsou v zacházení s pakety velice podobné. K testování chování jednotlivých mechanizmů byl vybrán směrovač A. Klienti ze sítě C generovali žádosti k serverům v ostatních sítích. Většina provozu byla směřující přes rozhraní Fa1 připojené přes rozbočovač k směrovači C. Směrovač C musel řešit problematiku zahazování či upřednostňování.

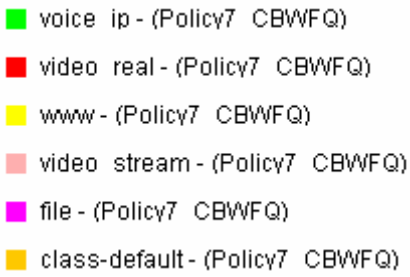
Chování mechanizmu CB-WFQ

Jednotlivé datové služby byly klasifikovány a rozřazeny do front, které obsluhoval mechanizmus CBWFQ. Rozdíl oproti mechanizmu LLQ byl znatelný při použitém nastavení parametrů CBWFQ, viz tab. 5.3. Šířka pásma se uvádí v procentuálním vyjádření k celkové šířce pásma rozhraní. Bylo sledováno chování při přesažení stanoveného limitu šířky přenosového pásma. Po zvolení 50% prostoru pro ostatní provoz byl naměřen viditelný rozdíl v chování obou mechanizmů.

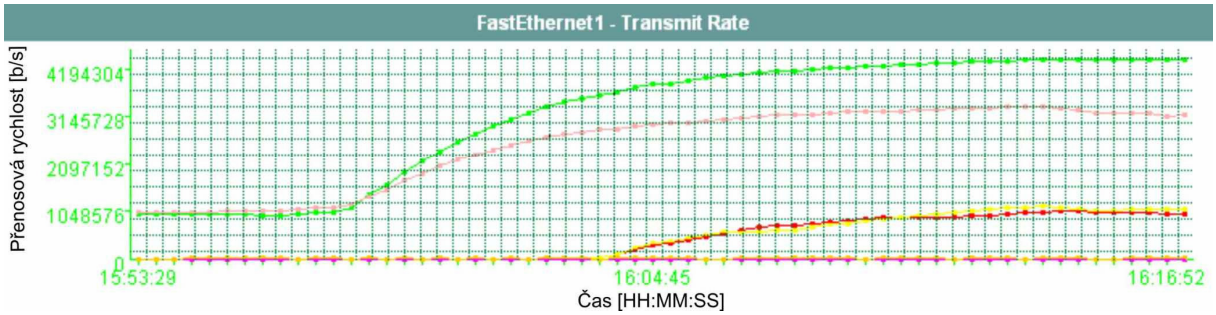
Pomocí programu SDM byly zaznamenány v paměti směrovače potřebné hodnoty a následně exportovány na jednotlivé průběhy. Šířka pásma výstupního rozhraní směrovače A byla 10Mb/s. Datový tok je rozdělen podle datových služeb, které směrovač klasifikoval. Pro názorné vyjádření jsou jednotlivé datové služby barevně rozlišeny, viz legenda obr. 5.19.

Tab. 5.3: Nastavení mechanizmu CBWFQ

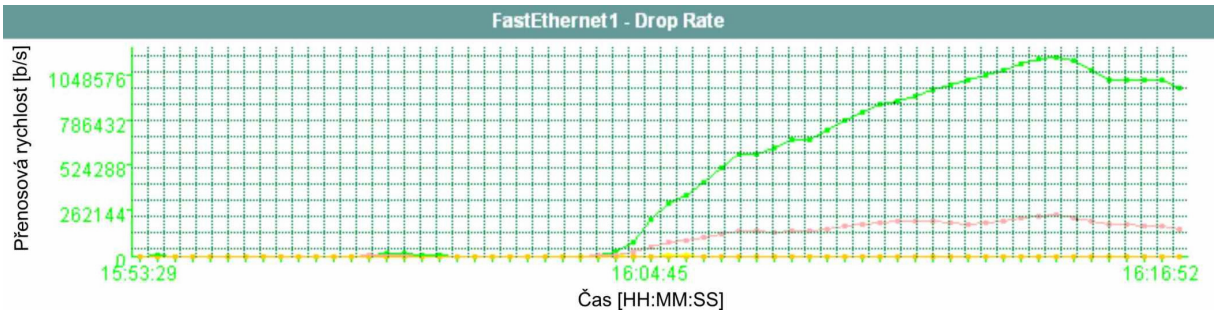
Služba	Šířka pásma
Hlas v reálném čase	10%
Video v reálném čase	10%
Provoz www	10%
Sledování videa	10%
Přenos souborů	10%



Obr. 5.19: Chování CBWFQ – legenda



Obr. 5.20: Chování CBWFQ – datový provoz



Obr. 5.21: Chování CBWFQ – zahozené pakety

Na obr. 5.20 je zobrazen průběh množství paketů proudící na rozhraní směrovače k obsloužení. Z počátku byl generován pouze datový tok VoIP a video stream, oba s přenosovou rychlostí 1Mb/s. Nebyl důvod k zahazování. Dále byly zmíněné datové toky navýšeny na nové hodnoty (VoIP 4Mb/s, Stream 3Mb/s. Celkový datový tok přes rozhraní činil 7Mb/s a žádné zahazování nebylo zpozorováno. Průběh zahozených paketů je na obr. 5.21.

Zahazování začalo až při zahájení toku dalších datových služeb (Real video 1Mb/s, www 1Mb/s). Tyto obě nově spuštěné služby mají garantované pásmo 10%. Zahazování je aplikováno pouze na datové toky převyšující limit garantované šířky pásma. Pakety služby VoIP dosahují nejvyšších hodnot převyšující limit 3Mb/s (4M/s – 1Mb/s) a v rámci dosažení maximální přenosové kapacity rozhraní jsou zahazovány. Datový tok zahazování VoIP činí cca 1Mb/s. Zahození paketů se nevyhnul ani datový tok video streamu (0,2Mb/s). Celkový datový tok zahazování činí cca 1,2Mb/s.

Mechanizmus CBWFQ má oproti předchůdcům vynikající vlastnost. Dokáže zaručit přesně definovanou šířku pásma pro konkrétní typ datového provozu. Nelze procentuelně rozdělit celou šířku pásma, vždy je třeba nechat nějaký prostor pro ostatní služby, které nejsou zahrnuty v politice QoS. V Cisco směrovači je striktně rezervováno minimálně 25%, která jsou předurčena neklasifikovanému provozu. Nevýhodou tohoto mechanizmu je nedostatek mechanizmů pro prioritní využití nerezervované šířky pásma. Na rozdíl od LLQ, které se snaží prioritně využít nerezervovanou šířku pásma.

Záruka rychlého odbavení ve směrovači je pouze při shodné velikosti datového toku s předefinovanou hodnotou v nastavení CBWFQ fronty pro danou službu. Pro dosažení ideální politiky použitím metody CBWFQ je třeba analyzovat a rezervovat potřebnou šířku pásma pro jednotlivé služby.

Chování mechanizmu LLQ

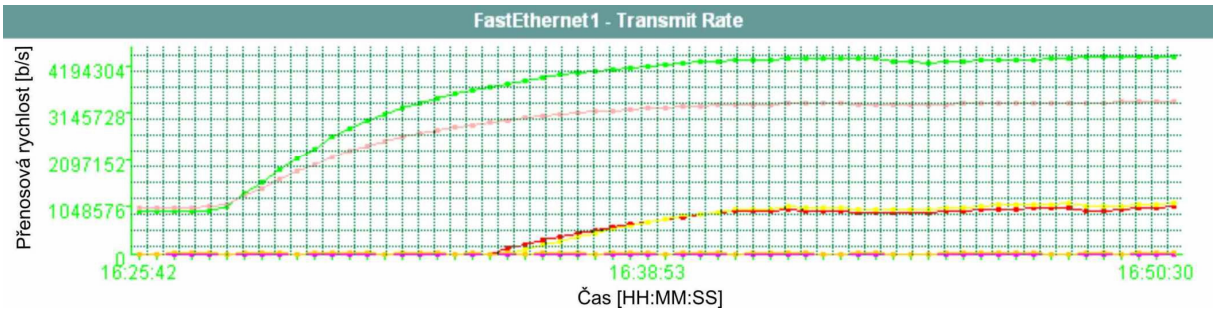
Další dostupný mechanizmus v směrovači Cisco 1812W je odbavení front pomocí LLQ. K porovnání s předchozí variantou CBWFQ bylo nastavení využití šířky pásma rozhraní pro jednotlivé datové služby shodné i pro LLQ, viz tab. 5.4. Měření probíhalo shodně jako při měření chování CBWFQ. Na výstupní směr rozhraní směrovače A byla aplikována QoS politika s obsluhou jednotlivých front pomocí LLQ. Legenda pro barevnou orientaci mezi datovými službami je znázorněna na obr. 5.22. Při měření je kladen důraz na zacházení s pakety, které přesahují garantovanou šířku pásma.

Tab. 5.4: Nastavení mechanizmu LLQ

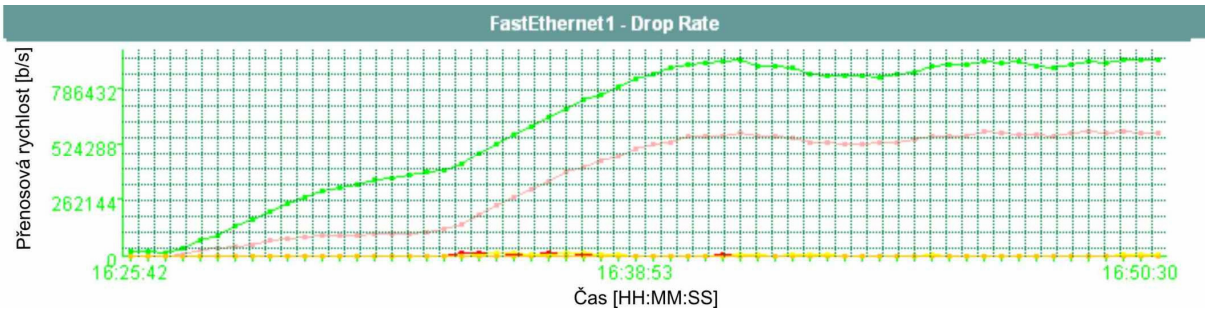
Služba	Šířka pásma
Hlas v reálném čase	10%
Video v reálném čase	10%
Provoz www	10%
Sledování videa	10%
Přenos souborů	10%

Při dodržení přenosových rychlostí dle nastavených limitů nedocházelo k zahazování. Nejprve byly generovány pouze datové toky služby VoIP a video streamu, každý s přenosovou rychlostí 1Mb/s. Průběh je na obr. 5.23. Celkový tok rozhraním činí pouze 2Mb/s. Zahazovat pakety není třeba. Závislost zahazování paketů dle provozu je na obr. 5.24. Při navýšení stávajících datových toků (VoIP 4Mb/s, stream 3Mb/s) začal mechanizmus LLQ zahazovat ačkoli nebylo zcela využito celé přenosové pásmo rozhraní směrovače. Zahazování dosahovalo nízkých hodnot (VoIP 0,3Mb/s, stream 0,1Mb/s). První rozdíl oproti CBWFQ.

Obr. 5.22: Chování LLQ - legenda



Obr. 5.23: Chování LLQ – datový provoz



Obr. 5.24: Chování LLQ – zahozené pakety

Dále byly spuštěny datové služby reálného videa a služba www. Každá služba vyžadovala přenosové pásmo 1Mb/s. Toto pásmo bylo rezervováno. Znamenalo to však zvýšení požadované obsluhy na výstupním rozhraní směrovače. Pakety datových služeb VoIP a streamu začaly být více zahazovány. Celkový datový tok zahazování činil cca 1,3Mb/s. Rozložení VoIP a video streamu je oproti CBWFQ více podřízeno IP prioritě paketů. Druhý rozdíl oproti CBWFQ. Převyšující datový tok VoIP byl vyšší než tok video streamu, proto jsou stále více zahazovány pakety služby VoIP.

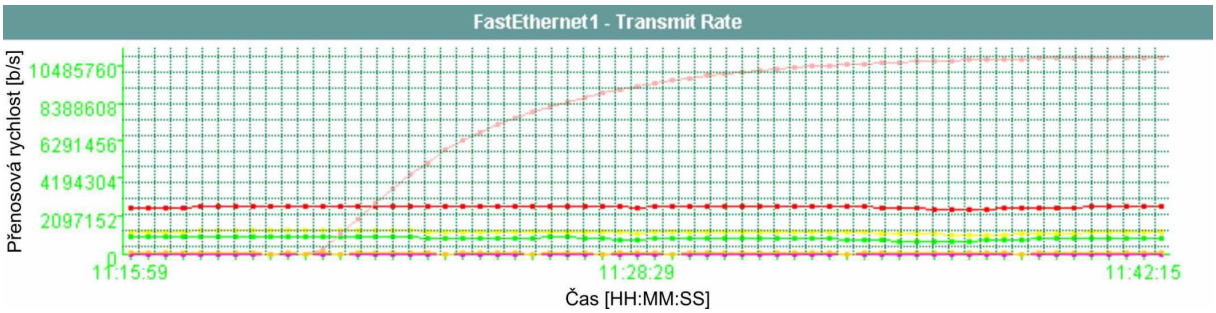
Mechanizmus LLQ zaručí minimální šířku pásma jednotlivým službám dle nastavení. Nedochází k vyhladovění žádné datové služby. K rezervaci je možné využít až 75 % šířky pásma rozhraní. 25 % je vyhrazeno jako minimum pro ostatní provoz. Velkou výhodou oproti předchozí metodě je, že nevyužitá šířka pásma je rozdělena podle priority. Při překročení velikosti toku dat nad hodnotu minimální rezervované šířky pásma pro jednotlivé služby je brán ohled na prioritu paketu.

Metoda odbavení front LLQ je pro své vynikající vlastnosti, které umožňují prioritní řazení, nejpoužívanějším mechanizmem při realizaci politiky kvalitativních služeb. Pro správné nastavení politiky je třeba analyzovat nejnižší rychlosti pro jednotlivé datové služby. Pokud dojde k překročení minimální šířky pásma je datový tok porovnán s ostatními a upřednostněn ten s nejvyšší prioritou.

Obrana před zahlcením pomocí LLQ

V experimentální síti byly realizovány některé datové služby. Byla spuštěna také služba sledování videa v reálném čase. Pomocí několika koncových stanic byl realizován přenos videa ze vzdálené IP kamery. Služba sledování videa v reálném čase zatěžovala rozhraní směrovače 2,5Mb/s. Přenos videa mezi IP kamerou a koncovými stanicemi byl rezervován v nastavení LLQ hodnotou 30%. Ostatní nastavení bylo shodné z předchozího měření LLQ.

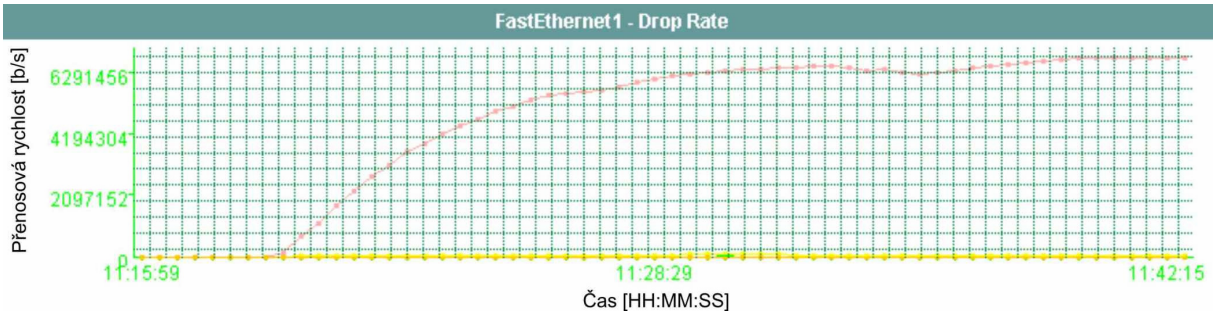
Jako simulace přetížení linky byl použit datový tok pomocí služby sledování videa. Přes rozhraní směrovače, které je limitováno propustností 10Mb/s, byl generován datový tok 10Mb/s. Naměřené hodnoty datového toku služeb jsou zobrazeny na Obr. 5.25. Barevné rozložení služeb je na obr. 5.26.



Obr. 5.25: Obrana před zahlcením pomocí LLQ – datový provoz

Obr. 5.26: Obrana před zahlcením pomocí LLQ – legenda

Z důvodu velkého zatížení výstupního rozhraní začal směrovač zahazovat pakety. Zahazování paketů v závislosti na zatížení sítě bylo změřeno a zobrazeno na obr. 5.27. Došlo k zahazování pouze paketů služby sledování videa. Pakety přenášející video z IP kamery byly dále přenášeny s nulovou ztrátovostí. Směrovač signalizoval zatížení rozhraní hodnotou 100 %. Na obraze z IP kamery nebylo poznat žádné přetížení vzniklé na rozhraní. Komunikace mezi IP telefony nebyla ovlivněna.



Obr. 5.27: Obrana před zahlcením pomocí LLQ – zahozené pakety

6 ZÁVĚR

V této práci jsem rozvedl problematiku kvalitativních služeb v síti. Prostudoval jsem, jakými možnými způsoby lze dosáhnout třídění provozu v rámci QoS pomocí různých mechanizmů, které podporuje většina novějších síťových prvků v síti. Díky vybudování vlastní fyzické experimentální sítě jsem se seznámil přímo s konfigurací konkrétních síťových prvků a s jejich kompatibilitou k podpoře kvality služeb.

Všechny metody, které se snaží o dosažení nejlepších výsledků z pohledu upřednostnění prioritního přenosu oproti méně prioritnímu, jsem se snažil popsat. Každá zmíněná politika má své výhody i nevýhody. Z dosud známých standardizovaných metod je pro kvalitu služeb nejvhodnější politika rozlišovaných služeb (Differentiated Services), která se silně rozrůstá i do menších sítí. S nárůstem aplikací vyžadující různé požadavky služeb a velké množství dat, která se v dnešní době přenáší mezi síťovými uzly, je nasazení podpory kvalitativních služeb v sítích nezbytné k dosažení konektivity předem preferovaných služeb. Následkem rozšiřování kvalitativních služeb do lokálních sítí je třeba vyšší kontrola v přístupových bodech Diffserv domény, zda nedošlo k podvržení identifikační značky v paketu či rámci.

K ověření teoretických poznatků byla vytvořena experimentální síť. Možnosti nabízející použité síťové prvky byly prostudovány a následně nastaveny k ověření činnosti. Identifikace provozu a následné přidělení priority mělo pozitivní dopad při simulaci přetížení přenosové linky. Nadměrné zahlcení nevyžádanými pakety nemělo vliv na propustnost dílčích datových provozů v síti. Při provedení stejné simulace přetížení bez použití politiky QoS na směrovači došlo k vážným výpadkům spojení, které zastavilo dostupnost užívaných datových služeb v experimentální síti.

Mechanizmus LLQ byl svými vlastnostmi k různým prioritám provozu označen za nejvhodnější variantu při výběru obsluhy front pro podporu kvalitativních služeb. Mechanizmus dokáže jednotlivým provozům zaručit minimální přenosovou rychlost a v případě překročení nastavené šířky pásma porovná paket s ostatními a upřednostní pakety s vyšší prioritou podle pole ToS v hlavičce IP paketu. Mechanizmus CB-WFQ dokáže stanovit přenosovou rychlost službě, ale nedokáže upřednostňovat jednotlivé pakety podle priorit, oproti LLQ.

Přínosem nasazení kvalitativních služeb v síti je především schopnost identifikovat prioritu přenášeného paketu v takovém stavu síťového uzlu, kdy je nutností začít zahazovat pakety z různého důvodu, nejčastěji z nadměrného vytížení rozhraní, které nezvládá obsloužit všechny pakety všech datových toků.

Na základě zpracovaných výsledků měření byla navržena laboratorní úloha. Úloha je zaměřena na seznámení se s problematikou QoS, nastavení a ověření zacházení s pakety v experimentální síti.

SEZNAM ZKRATEK

AF	Assured Forwarding
ATM	Asynchronous Transport Mode
CAC	Call Admission Control
CLI	Command Line Interface
CoS	Class of Service
CS	Class Selector
DiffServ	Differentiated Services
DS	Differentiated Services
DSCP	Differentiated Services Code-Point
EF	Expedited Forwarding
FTP	File Transfer Protocol
GB	GigaBit
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IOS	Internetwork Operating System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISL	Inter-Switch Link
LAN	Local Area Network
PHB	Per Hop Behaviours
QoS	Quality of Service
RED	Random Early Detection
RSVP	Resource Reservation Protocol
RTI	Real Time Intolerant
RTP	Real-time Transmission Protocol
RTT	Real Time Tolerant
SDM	Security Device Manager
SIP	Session Initiation Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TELNET	Telecommunication Network
ToS	Type of Service
UDP	User Datagram Protocol
UTKO	Ústav telekomunikací
UTP	Unshielded Twisted Pair

WAN	Wide Area Network
WRED	Weighted Random Early Detection
WWW	World Wide Web

POUŽITÁ LITERATURA

[1]WANG, Z. *Internet QoS : Architectures and Mechanisms for Quality of Service*. [s.l.] : Morgan Kaufman Publishers, 2001. 240 s. ISBN 1-55860-608-4.

[2]MARCHESE, M. *QoS over heterogenous network.* [s.l.] : John Wiley & Sons, 2007. 307 s. ISBN 978-0-470-01752-4.

[3]WALLACE, K. *VoIP bez předchozích znalostí*. Brno : Computer Press, 2007. 225 s. ISBN 978-80-251-1458-2.

[4]HERMAN, I. *Komunikační technologi*e. Brno, 2003. 231 s. [učební texty], Fakulta elektroniky a komunikačních technologií VUT Brno, Ústav telekomunikací.

[5]SVEN, U. *QoS a diffserv - Úvod do problematiky.* [online]. [2004] [cit. 2008-11-11]. Dostupný z WWW: <http://www.cesnet.cz/doc/techzpravy/2000-6/>.

[6]PANÁČEK, P. *QoS v IP sítích.* [online]. [2002-11] [cit. 2008-11-11]. Dostupný z WWW: <http://www.anect.com/cs/info/tiskove-centrum/clanky/qos-v-ip-sitich.html>.

[7]KACÁLEK, J. *QoS v počítačových sítích.* [online]. [2006][cit. 2008-10-30]. Dostupný z WWW: <http://amarok.cesketelekomunikace.cz/xkacal00/index.php?action=intro>.

[8]LHOTKA, L. *Internet se zaručenou kvalitou služby*. [online]. [2000] [cit. 2008-11-10]. Dostupný z WWW: <http://www.cesnet.cz/doc/seminare/ei2000liberec/lhotka.html>.

[9]HUCABY, J.; MCQUERRY, S. *Konfigurace směrovačů Cisco.* [s.l.] : Computer Press, 2004. 630 s. ISBN 80-7226-951-8.