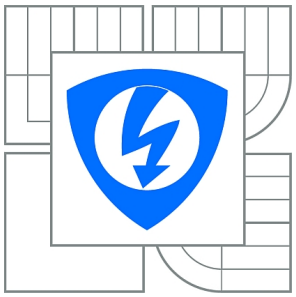
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

TESTOVÁNÍ PODPORY KVALITATIVNÍCH POŽADAVKŮ SLUŽEB V EXPERIMENTÁLNÍ DATOVÉ SÍTI

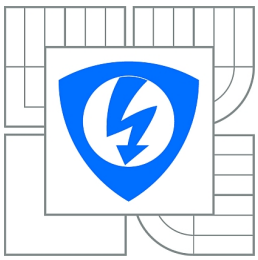
TESTING OF QOS SUPPORT IN EXPERIMENTAL DATA NETWORK

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MIROSLAV FOGL
AUTHOR

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

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Miroslav Fogl	***ID:***	73046
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Testování podpory kvalitativních požadavků služeb v experimentální datové síti

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte architektury a techniky podpory kvalitativních požadavků služeb v sítích IP. Uvažujte jak linkovou, tak i síťovou vrstvu. Seznamte se s konkrétními síťovými prvky experimentální sítě laboratoře ÚTKO a s možnostmi podpory QoS v těchto síťových prvků. Navrhněte různé scénáře konfigurací síťových prvků s ohledem na podporu QoS. V síti realizujte řadu služeb s různým typem provozu (VoIP, videokomunikace, videostreaming, FTP, HTTP apod.) a otestujte jejich chování pro různé scénáře. Zjistěte také vliv výpadku síťového prvku či spoje na průběh jednotlivých typů služeb. Výsledky vyhodnoťte, navrhněte doporučení pro konfiguraci menší podnikové sítě integrující různé služby a vytvořte dvě laboratorní úlohy.

DOPORUČENÁ LITERATURA:

[1] SZIGETI, T., HATTINGH, CH., End-to-End QoS Network Design. Cisco Press, ISBN 1-58705-176-1, Indianapolis, USA
[2] MARCHESE M. QoS over Heterogeneous Networks. John Wiley & Sons, ISBN 978-0-470-01752-4, 2007

Termín zadání:	7.2.2011	***Termín odevzdání:***	26.5.2011

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

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

UPOZORNĚNÍ:

Anotace

Práce se věnuje problematice kvalitativních požadavků služeb v IP sítích založených na technologii Ethernet. Jsou zde popsány základní způsoby nasazení řízení kvality služeb v síti. Dále jsou rozvedeny možnosti zacházení s pakety, řízení přetížení a omezování přenosové rychlosti v sítových prvcích. Pozornost je věnována síťové a linkové vrstvě. Na základě konkrétních možností síťových zařízení v laboratoři UTKO byla navržena a vytvořena experimentální síť. Síť tvořená směrovači a přepínači propojovala několik serverů s klientskými stanicemi. Byly generovány různé druhy datových přenosů (VoIP, HTTP, FTP, video). Techniky zacházení s pakety s různými prioritami byly ověřeny a porovnány. Byl naměřen značný vliv implementace podpory QoS v síti při plném zatížení spojů. Dalším praktickým měřením byla také simulace různých situací jako přetížení spoje nevyžádaným provozem či výpadek spoje mezi směrovači. Pro zajištění kvality služeb je třeba vytvořit doménu, v které jsou dodržována shodná pravidla ve všech síťových prvcích.

Abstract

This work deals with the qualitative requirements on services in IP networks based on technology Ethernet. We describe basic methods for imposing quality control mechanisms on services within networks. We elaborate on the ways, in which packets can be handled, overload controlled and transfer speed in network elements limited. Attention is given also to the Network Layer and Link Layer. Based on concrete specifications of network devices in UTKO laboratory an experimental network was designed and constructed. Network consisting of routers and switches linked several servers with client stations. Various types of data transfers (VoIP, HTTP, FTP, video) were generated. Several techniques for handling packets with different priorities were verified and compared. We observed that, in situations when connections are under full load, implementation of QoS support in the network becomes very important. This observation was confirmed by measurements. We also measured the parameters of the system during simulations of various situations, such as overload of a connection due to unsolicited operations or failure of a connection between routers. In order to guarantee the quality of services it is necessary to create a domain, in which rules are consistently observed in all network elements.

Klíčová slova

Priorita, zahazování, upřednostnění, fronta, služby, pravidla, síť, směrovač

Key words

Priority, dropping, preferred, queue, services, rules, network, router

Bibliografická citace práce

FOGL, M. *Testování podpory kvalitativních požadavků služeb v experimentální datové síti* . Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 51 s. Vedoucí diplomové práce doc. Ing. Vít Novotný, Ph.D.

Prohlášení o původnosti práce

Prohlašuji, že svou diplomovou práci na téma testování podpory kvalitativních požadavků služeb v experimentální datové síti jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a 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 diplomové práce.

V Brně dne ..... ……

podpis autora

OBSAH

ÚVOD

Komunikace mezi lidmi byla odjakživa velmi důležitá. Lidé dnes mezi sebou komunikují různými způsoby a prostředky. Pokud si své dojmy, zprávy a různé informace nemohou sdělit osobně, využijí dostupný komunikační prostředek. V dnešní době je mnoho možností jak přenést informaci k příjemci. Jedna z nejrozšířenějších možností současnosti je využití celosvětové sítě Internet, který nabízí koncovému účastníkovi řadu zajímavých prostředků komunikace a získávání informací z nepřeberného počtu informačních zdrojů.

Elektronická pošta, prohlížení internetových stránek či přenos souborů byly v devadesátých letech minulého století hlavními službami v síti Internet a zároveň i v lokálních sítích. Jelikož zmíněné služby neměly speciální požadavky na zpoždění či ztrátovost nebylo potřeba řešit podporu těchto požadavků v síti. Největší důraz byl především kladen na maximální přenosovou rychlost připojení. Postupným rozšiřováním Internetu a integrací různých služeb, jako například sledování televizního vysílání, poslech rozhlasového vysílání, hovorová služba, video konference, hraní počítačových her či stahování filmů ze serverů, dálkové řízení a dohledování či řízení systémů po síti dochází k velké pestrosti přenášených dat v síti, navíc s různými potřebami, co se týče naléhavosti na dostupnost síťových prostředků. Služby, které běží v reálném čase, jsou velmi citlivé na parametry typu zpoždění, ztrátovost a přenosová rychlost. Opakem jsou služby nevyžadující časovou dochvilnost (přenos souborů). V podnikových či komerčních sítích se setkáváme s rozmanitými druhy zároveň probíhajících služeb a je třeba vyhovět všem. Dříve byl kladen největší důraz na parametr přenosové rychlosti. Zvýšením přenosové rychlosti daného spoje bylo možné tento problém vyřešit, ale pouze lokálně. Mezi dvěma stanicemi komunikujícími přes větší síť (např. Internet) se vždy může vyskytnout spoj s nízkou přenosovou kapacitou či s vysokou úrovní provozu, a vytvořit tak tzv. úzké hrdlo na spoji v síti, kde může docházet k redukci výsledné propustnosti, a tím i k nárůstu zpoždění či dokonce k zahazování datových jednotek jako reakci na přetížení daného uzlu, spoje či obojího. Přestože podnik je napojen k poskytovateli internetového připojení spojem s vysokou rychlostí, může docházet k zahazování paketů mimo místní podnikovou síť. Tuto problematiku je třeba řešit jednak v lokálních sítích, ale mnohem více v sítích poskytovatelů připojení k Internetu, kteří si nechávají za garanci poskytnuté služby platit nemalé částky. Jestliže před deseti lety zůstávala výrazná většina datových toků uvnitř lokálních sítí, je dnes situace přesně opačná a většina toků je směřována do vyšších úrovní síťové infrastruktury a dále do prostředí Internetu.

Tradiční datové aplikace podporované mechanismy protokolu TCP jsou vcelku dobře schopny vyrovnat se s přetíženými spoji, a tedy i s případnými ztrátami (zpoždění a jeho variabilita u těchto typů služeb do jisté míry nehraje roli), horší je to však s aplikacemi multimediálními a interaktivními, které jsou velmi citlivé na zpoždění a jeho proměnlivost při přenosu digitalizovaného obrazu a zvuku, a využívajícími nespolehlivý transportní protokol UDP. Všechny služby a aplikace potřebují ke své realizaci dostatečnou přenosovou rychlost a řada z nich vyžaduje co nejmenší ztrátovost a minimální dobu zpoždění během přenosu. Současné paketové sítě jsou dnes ve většině případů nastaveny tak, že neřeší problematiku zajištění propustnosti sítě potřebné pro bezproblémový průběh služeb v reálném čase. S přibývajícím počtem a objemem datových toků v síti dochází k výpadkům důležitých služeb v rámci sítě či podniku. Především jde o to, že jednotlivé aplikace vzájemně sdílí společnou šířku pásma sdíleného kanálu, která je standardně přidělována dle mechanizmu FIFS (First In First Served). Pokud nejsou stanovena pravidla pro řízení kvality služeb, může docházet k výpadkům důležitých spojení v rozlehlých společnostech (připojení vzdálených poboček a zaměstnanců firmy přes VPN spojení) jenom proto, že někteří zaměstnanci přenášejí velké objemy dat z datových center z Internetu.

Tato práce se zabývá řešením problémů se zajištěním kvality služeb v sítích IP. Je více mechanizmů, které jsou součástí řízení kvality služeb. Budou popsány a zhodnoceny nejpoužívanější způsoby možné realizace. 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. Při reálném provozu v síti budou sledovány kvalitativní parametry jednotlivých služeb. Jednotlivé scénáře nastavení kvality služeb a jejich chování při nasazení na síťové prvky laboratorní sítě budou porovnány a následně vyhodnoceny.

1 PARAMETRY PŘENOSU

Současné integrované sítě přináší své problémy. Především jde o to, že aplikace soupeří o šířku pásma a některé z nich, např. hlasové služby, jsou méně tolerantní ke zpoždění nazývanému také jako latence, a k jeho proměnlivosti, než jiné aplikace, jako jsou například přenosy souborů. Různé typy provozu jsou různě citlivé na aktuální nedostupnost síťových prostředků. Hlasové služby potřebují konstantní šířku pásma a nízké zpoždění. Video-komunikace požaduje synchronizaci se zvukem. Služby v reálném čase vyžadují nízké a málo proměnlivé zpoždění (jitter). V Tab. 1.1 jsou uvedeny subjektivní požadavky jednotlivých služeb na přenosový spoj [14]. Hodnoty jsou závislé na velikosti odesílaných dat, použitém kódování, zabezpečení a kvality přenosové cesty. Nevyhovující parametry přenosu na spoji pro danou službu mají největší dopady na nespokojenost s kvalitou poskytované služby zákazníkovi.

Tab. 1.1: Požadavky služeb z pohledu uspokojení potřeb zákazníka

Typ provozu	Požadavky na přenos			
	rychlost spoje	ztrátovost	zpoždění	jitter
Hlas (G.711)	> 93 kb/s	< 1 %	< 150 ms	< 30 ms
Video-konference (H.263 CIF)	> 512 kb/s	< 1 %	< 150 ms	< 30 ms
VPN spojení	> 1 Mb/s	0 %	< 1 s	-
prohlížení www stránek	> 512 kb/s	0 %	< 1 s	-
přenos souborů	> 1 Mb/s	0 %	-	-
TV přenos HDTV	> 6 Mb/s	< 5 %	< 5 s	-
Poslech hudby	> 128 kb/s	< 1 %	< 5 s	-

Kvalitu konkrétního typu služby lze vyjádřit konkrétními hodnotami souboru kvalitativních atributů, z nichž nejdůležitějšími atributy závisejícími na stavu komunikační sítě jsou:

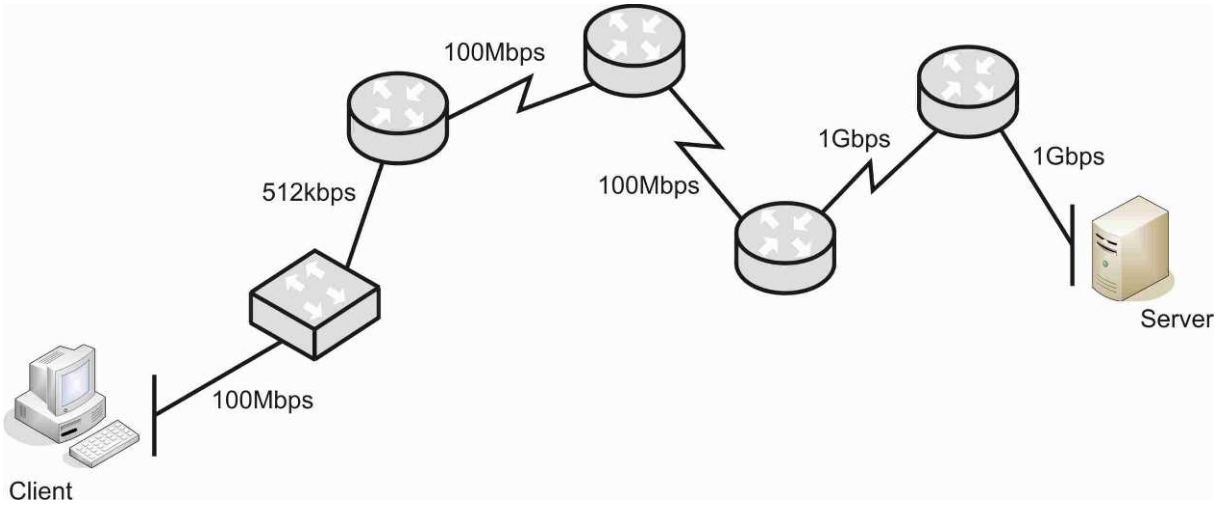
- přenosová rychlost (průměrná, maximální),
- ztrátovost paketů (maximální přijatelná hodnota),
- zpoždění (maximální přijatelná hodnota),
- proměnlivost zpoždění (jitter – maximální přijatelná hodnota).

Přenosová rychlost

Při přenosu informací je jedním z rozhodujících aspektů objem dat, který je používaný přenosový kanál schopen přenést za určitý čas. Obvykle se v této souvislosti mluví (spíše neformálně) o přenosové kapacitě či propustnosti přenosové cesty. Správným měřítkem je však přenosová rychlost (v bitech za sekundu), [8]. Dosažitelná přenosová rychlost je ale vždy dána souhrnem fyzikálních vlastností přenosového média (vodičů, optických kabelů, volného prostoru, apod.) a vlastnostmi dalších technických prostředků, které přenosový kanál spoluvytvářejí (např. modemů, multiplexorů apod.). Každý přenosový kanál je vždy schopen přenášet jen signály o kmitočtech z určitého omezeného intervalu. Šířka intervalu kmitočtů, které je přenosový kanál schopen přenést, představuje tzv. šířku pásma (bandwidth).

Přenosová kapacita je převážně závislá na šířce pásma, útlumové charakteristice kanálu, na úrovni rušení, na maximálním povoleném vysílacím výkonu a na vlastnostech přijímače signálu, [4].

Přenosová rychlost na aplikační úrovni je vždy nižší než fyzická přenosová rychlost v daném kanálu, a to podle množství režie, která závisí na konkrétní síťové technologii a protokolové sadě vyšších vrstev. Jednotlivé úseky v síti mohou být propojeny různými technologiemi s odlišnou přenosovou rychlostí. Skutečná (efektivní) přenosová rychlost je rychlost toku dat na nejpomalejším spoji v celé trase, jak je znázorněno na Obr. 1.1. Na Obr. 1.1 je naznačena situace, kdy klientský počítač komunikuje se vzdáleným serverem a je připojen k firemnímu přepínači komunikujícímu rychlostí 100 Mb/s. Efektivní využití přenosové rychlosti je však ovlivněno nejpomalejším spojem mezi přepínačem a směrovačem s přenosovou rychlostí 512 kb/s. Ve většině případů jsou limity spojů úmyslně snižovány poskytovatelem připojení z důvodu tarifování a účtování dle smluvních ujednání.



Obr. 1.1: Efektivní přenosová rychlost

Ztrátovost paketů

Ztráty paketů v síti mohou mít nejrůznější příčiny, ale většinou je důvodem přetížení a zahlcení sítě, kdy některé směrovače nebo přepínače a navazující spoje nestačí odbavovat příchozí pakety dostatečně rychle, jejich fronty (vyrovnávací paměti) se nebezpečně zaplní a další příchozí pakety pak mohou být zahozeny. V případě bezdrátových technologií může být ztrátovost spojena s nadměrnou chybovostí rádiového spoje z důvodů mnohem vyšší úrovně rušení či náhlých změn parametrů rádiového kanálu při pohybu koncového zařízení.

Různé služby jsou různě citlivé na ztrátovost paketů a se ztrátovostí paketů se vypořádávají různými způsoby závislými na typu služby, použitém kodeku a na přenosovém protokolu. U služeb v reálném čase nemohou být ztracené pakety nahrazeny jejich opakovaným vysláním zdrojem (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. Malé mezery nevadí, ale vysoká ztrátovost paketů nebo ztráta většího množství paketů následujících za sebou, vede k výraznému zhoršení kvality přenášené řeči či dokonce k ukončení služby. Na Obr. 1.2 je naznačen vliv ztráty paketu na přenášenou zvukovou stopu.

Obr. 1.2: Vliv ztráty paketů při přenosu hlasu

Zpoždění

Zpoždění (často označováno jako latence) je v případě služeb v reálném čase doba, která uplyne mezi stavem, kdy jsou aplikační data vygenerována ve zdrojovém koncovém uzlu, a stavem, kdy jsou data prezentována v cílovém koncovém uzlu. Zpoždění sestává z pevné a proměnlivé složky, [9].

- ***Pevná složka zpoždění*** – je dána převážně použitou technikou kódování, délkou trasy a rychlostí obsluhy paketu síťovými uzly (bez uvažování čekání ve frontách). V paketové síti existují tři druhy zpoždění, [4]:

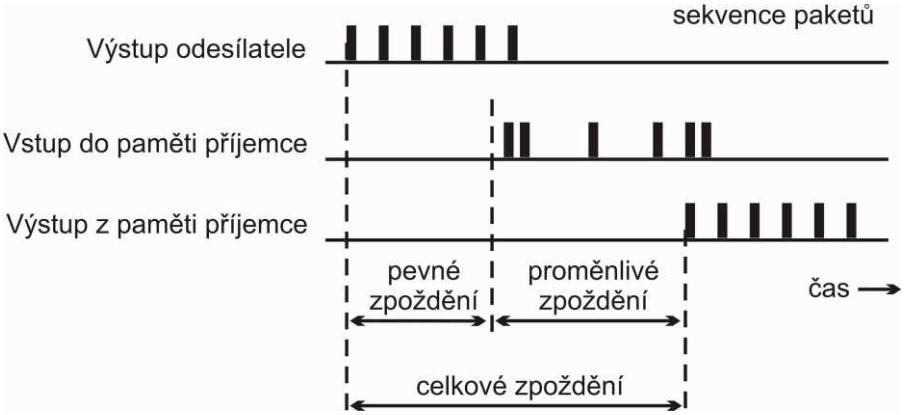
    - *Zpoždění dané šířením signálu* – čas potřebný k předání informace přímo po fyzickém přenosovém médiu. Doba mezi vysláním a přijetím signálu na daném spoji.

    - *Doba zpracování v koncových uzlech* – doba, která uplyne od přijetí signálu nesoucího dostatečné množství informace, jenž byla vyslaná zdrojem informace (paměťové médium či producent informace v reálném čase – člověk, senzor) a určené k přenosu, až po předání segmentu zprávy uloženého v paketu síťovému rozhraní dané síťové technologie (na straně odesílatele) a naopak (na straně příjemce). Tato složka zpoždění tedy zahrnuje zpoždění zdrojového kódování (dekódování), zpoždění segmentací zprávy do bloků určených k přenosu jednou datovou jednotkou a zpoždění sestavení paketu včetně vyhledání potřebných informací (a jejich vložení do záhlaví paketu) k cestě heterogenním síťovým prostředím.

    - *Zpoždění na síťovém rozhraní* – doba, která je nutná pro zpracování paketu v síťovém rozhraní uzlu při předání k vysílání a samotné vyslání nosného signálu daným komunikačním kanálem určité síťové technologie. Tzv. serializační zpoždění závislé na symbolové rychlosti kanálu je součástí této složky zpoždění.

- ***Proměnlivá složka zpoždění*** – vzniká z důvodů změn stavu sítě, například vlivem proměnlivosti zátěže v přístupové síti (sdílení přístupového kanálu) a v přepojovacích prvcích, kdy jsou pakety pozdrženy různou dobu ve frontách přepojovacích prvků, či vlivem výpadku přepojovacího uzlu či spoje v síti, kdy dojde ke změně trasy přenosu paketů. Této složce zpoždění se říká jitter. Například u hlasové služby vysílací strana posílá pakety v pravidelných intervalech. Ideálně by přijímací strana měla přijímat pakety také v pravidelných časových intervalech, v tomto případě by velikost parametru jitter byla nulová. Ale změny stavu zátěže, a také vzájemná nezávislost směrování paketů v síti mohou určité pakety v datové síti zpomalit či zrychlit, a tak některé pakety přijdou dříve a jiné mnohem později, a díky nezávislosti způsobu doručování jednotlivých paketů mohou pakety dokonce přijít i v jiném pořadí. Jestliže „zpomalené“ pakety jsou doručeny ke zpracování příliš pozdě, jsou dle použitého protokolu zahozeny, protože jejich obsah už není příjemci k užitku („časově zastaral“). Nevyrovnaný příchod datových jednotek do přijímače může díky nepřítomnosti dat pro dekodér způsobit „zamrznutí“ služby (přehrávání multimédií). Pro potlačení proměnlivosti

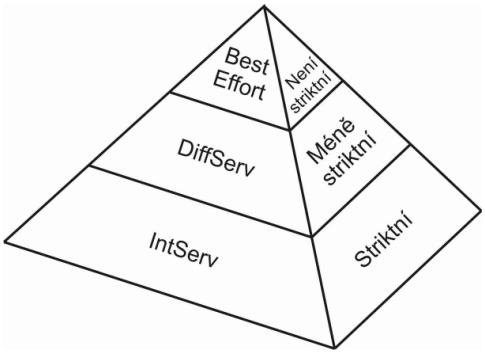
zpoždění se využívá vyrovnávací paměť, tzv. jitter buffer. Jitter buffer pozdržuje pakety na přijímací straně a předává datové segmenty dekodéru opět se správnými časovými odstupy tak, jak byly vysílány ze zdroje. Jitter paměť tedy podrží pakety po určitý čas ve vyrovnávací paměti za cenu zvýšení celkového zpoždění (Obr. 1.3).



Obr. 1.3: Celkové zpoždění sestávající ze zpoždění způsobeného vlastním přenosem (pevné) a zpoždění pozdržením ve vyrovnávající paměti (proměnlivé) pro odstranění jitteru.

2 ARCHITEKTURY PRO PODPORU POŽADAVKŮ NA QOS

V dnešních IP sítích se používají dva hlavní způsoby pro zajištění kvality služeb – architektura integrovaných služeb (Integrated Services) a rozlišovaných služeb (Differentiated Services). Případně lze jako třetí způsob řešení QoS považovat případ, kdy není nasazeno řízení QoS (Best Effort).



Obr. 2.1: Kategorie QoS a jejich striktnost k provozu.

2.1 ARCHITEKTURA INTEGROVANÝCH SLUŽEB (INTEGRATED SERVICES)

Architektura Integrovaných služeb, dále již Intserv, byla prvním modelem, který měl za úkol zajistit požadovanou kvalitu služeb v počítačových sítí protokolem IP. Tento model byl uveden v roce 1994. Model předpokládá záruku pro QoS po celé trase mezi zdrojovou a cílovou stanicí. Cílová stanice, která očekává určitá data a chce si pro ně zajistit zaručený průchod sítí, využije rezervační protokol. Protokol pak postupně signalizací zjišťuje po celé cestě sítí všemi směrovači až ke zdrojové stanici, zda vyžádaná šířka pásma může být pro daný tok přidělena (v jednom směru). Přijímač zkoumá možnost komunikace za daných podmínek. Tato funkce je označována jako řízení přístupu (admission control). Komunikující strany si mohou sdělovat své požadavky na QoS sítí přímo a pružně.

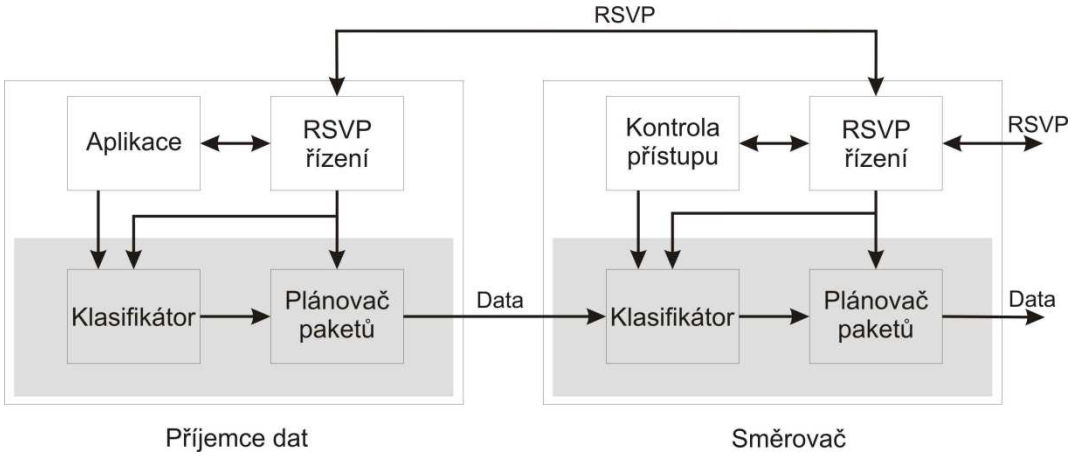
V případě, že síť nemůže požadavku vyhovět, není spojení povoleno a aplikace se může rozhodnout, zda požádá o méně náročné požadavky služeb či spojení nebude provedeno. Pokud požadavku vyhoví, musí přijímač informovat všechny komponenty, přes které bude probíhat přenos, aby pro dané spojení rezervovaly 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)[10], který je však poměrně složitý a vnáší významnou režii při řízení relací, což má za následek především větší zpoždění zahájení přenosu uživatelské informace.

Integrované služby rozlišují následující kategorie aplikací, [10]:

- **Real Time Intolerant (RTI) aplikace** – tato třída požaduje minimální odezvu (latency) a rozptyl zpoždění (jitter). Příkladem jsou hovorová služba, řízení procesů po síti, videokonference, akční hry po síti, apod.

- **Real Time Tolerant (RTT) aplikace** – požadují omezení na maximální zpoždění v síti. Občasná ztráta paketů je přijatelná. Příkladem jsou video aplikace využívající paměť buffer, která před aplikací potlačí proměnlivost zpoždění paketů.

- **Elastické aplikace** – jsou méně náročné na brzké doručování. Do této kategorie zapadají aplikace nad TCP. Jsou kladeny menší požadavky na omezení zpoždění nebo kapacitu spojení. Příkladem může být posílání el. pošty či odezva na webové stránky.



Obr. 2.2: Komponenty architektury integrovaných služeb (IntServ).

Pro správnou funkci Intserv musí být ve směrovačích a hostitelích implementovány následující komponenty, viz Obr. 2.2 na kterém je znázorněna provázanost jednotlivých komponentů pro rezervaci toku dat mezi příjemcem vysílání a směrovačem, [11]:

- **Kontrola přístupu**

Kontrola přístupu realizuje rozhodovací algoritmus, který směrovač nebo hostitelský počítač používá k určení, zdali novému toku může být udělena rezervace bez dopadu na dřívější záruky. Kontrola přístupu je spuštěna v každém uzlu sítě, aby mohlo být rozhodnuto, zda bude požadavek akceptován nebo odmítnut.

- **Klasifikátor**

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

- **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 a řešena samostatnou frontou. Plánovač řídí posílání jednotlivých paketů z front podle předem daných algoritmů.

- **Rezervační protokol**

Další součástí implementace je protokol pro rezervaci zdrojů, který je nutný k vytvoření a udržování stavů v směrovačích a koncových zařízeních podél celé cesty. Nejpoužívanějším protokolem je RSVP (Resource Reservation Protocol).

Nevýhody Integrated Services

Tento přístup má řadu nevýhod. Všechna zařízení, přes která procházejí IP pakety datových toků a pro které je potřeba zajistit určitou kvalitu služby, včetně koncových zařízení, musí podporovat

protokol RSVP. Každý směrovač v síti musí udržovat stavovou informaci pro každou rezervaci (každý datový tok s požadavkem na zajištění kvality služeb). Ve větších sítích, kde se přenáší velké množství datového toku, 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 lokálních IP sítích, kdy před ustavením komunikace probíhá kontrola volných zdrojů prostřednictvím rezervačního protokolu.

2.1.1 Protokol rezervace prostředků RSVP

Protokol RSVP (Resource Reservation Protocol) [1] je určen pro signalizaci požadavků na přenosové pásmo. Vzhledem k zátěži propojovacích zařízení způsobené sledováním stavu každé rezervace pomocí RSVP má protokol uplatnění jen v lokálních sítích. V Internetu mohou nastat problémy z důvodu, že RSVP musí podporovat všechny směrovače na cestě od odesílatele požadavku k požadovanému zdroji. Zdroj datového toku pomocí protokolu RSVP periodicky informuje uzly o přihlášených účastnících v dané multicastové skupině a o vlastnostech svého datového toku. Kterýkoli člen multicastové skupiny si pak na základě těchto informací může požádat o rezervování přenosového pásma a všechny směrovače na cestě by mu měly vyhovět. Protokol garantuje šířku pásma prostřednictvím vybudování cesty mezi koncovými uzly s dohodnutými parametry ve specifikaci toku v každém směrovači nebo přepínači na síťové vrstvě. RSVP je preferovaným mechanizmem pro signalizaci QoS zejména pro služby typu hlas po IP (VoIP) a video po IP. Protokol nabízí jedinečnou přednost v tom, že nepřipouští žádný nadbytečný paket, a pásmo je také dostupné pro jiné volání nebo spojení po stejném spoji.

Protokol RSVP není směrovací protokol, pouze využívá směrovací tabulky směrovačů k určení nejlepší cesty k doručení. Jedná se o signalizační protokol, který používá především následující dvě signalizační zprávy:

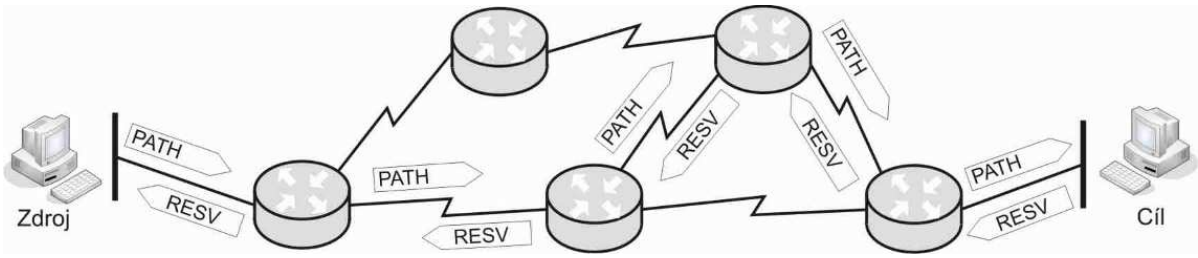
Signalizace zdroj – cíl (zpráva PATH)

Odesílatel, například server vysílající určitý video stream, stanoví hranice parametrů kvality služby požadované na jeho datový tok, speciálně šířku pásma, zpoždění a změnu zpoždění. Tyto parametry vloží do zprávy (PATH message) a pošle ji na adresu příjemce nebo ji periodicky začne zasílat na multicastovou adresu v jejíž skupině je registrován video stream. PATH message je tedy rozeslána směrem k cíli a veškeré uzly na cestě jsou tak informovány o specifikaci datového toku odesílatele.

Signalizace cíl – zdroj (zpráva RESV)

Příjemce, zaregistrovaný v dané multicastové skupině, přijme některou ze zpráv PATH a na základě jejích parametrů vytvoří rezervační požadavek. Tato RESV zpráva obsahuje požadavky na kvalitu a rychlost datového toku (obvykle stejné jako v PATH zprávě), informace o portu, na kterém příjemce naslouchá, a informace o použitém přenosovém protokolu (TCP/UDP). Zpráva RESV je poté odeslána na adresu zdroje uvedenou v PATH zprávě. Jakmile některý ze směrovačů přijme zprávu RESV, na základě požadavků uvedených v RESV zprávě rozhodne o rezervaci prostředků. Pokud se směrovač z jistých důvodů rozhodne odmítnout žádost o rezervaci, odešle žadateli upozornění o zamítnutí. Jestliže i poslední směrovač potvrdí požadavek, jsou příjemce i odesílatel uvědomeni a prostředky jsou rezervovány.

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, jak je znázorněno na Obr. 2.3. Informace a rezervace příslušející danému toku lze též zrušit explicitně pomocí zpráv typu PATHTEAR a RESVTEAR.

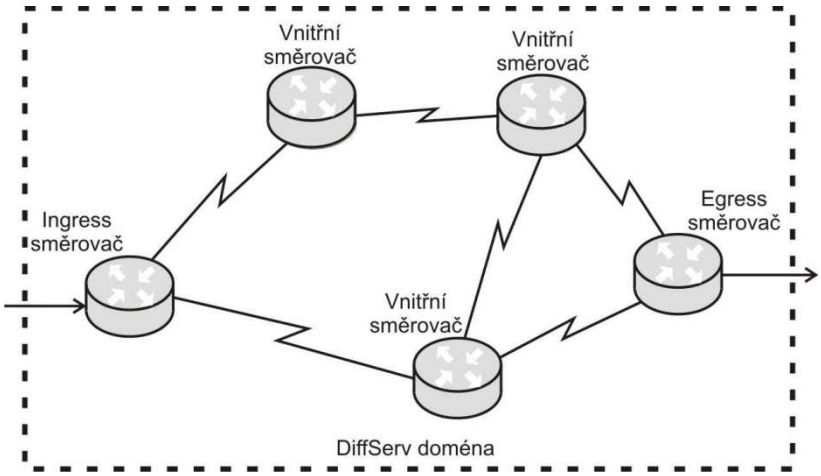


Obr. 2.3: Průběh rezervace prostředků pomocí RSVP.

2.2 ARCHITEKTURA ROZLIŠOVANÝCH SLUŽEB (DIFFERENTIATED SERVICES)

Architektura rozlišovaných služeb [2], dále již 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 neoznamují předem počítačové síti své požadavky na přenos. Použití rezervačních protokolů tedy není nutné. Jednotlivé směrovače neudržují žádnou stavovou informaci o jednotlivých spojeních.

Implementace QoS je navržena tak, že každý paket vstupující do sítě s podporou QoS je v IP hlavičce paketu označen značkou třídy priority, tzv. DSCP kódem. S tímto označením paket dále putuje přes jednotlivé uzly sítě až k příjemci. Síťové prvky zkoumají značení paketů a dle priority se k nim chovají. Pakety s kódem vyjadřujícím vyšší prioritu upřednostní před ostatními pakety čekajícími ve frontě. Všechny služby, které chce administrátor upřednostnit, musí rozdělit do upřednostňovaných tříd. V různě zaměřených počítačových sítích může být požadováno odlišné zacházení s datovými službami. Proto je priorita paketu vyjádřena v IP hlavičce každého paketu jako číselný údaj a je možné jej přeznačit dle požadavků správce sítě. Může tedy docházet k odlišným politikám se zacházením s pakety v různých počítačových sítích spravovaných jinými organizacemi. Proto jednotliví správci síti definují svá pravidla na hraničních směrovačích, kde tedy může docházet k přeznačení priority v IP paketu. 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.



Obr. 2.4: Směrovače v DiffServ doméně.

Síť je možné rozdělit na jednotlivé oblasti se samostatnou správou rozlišovaných služeb tzv. DiffServ domény. Každá doména obsahuje vnitřní a hraniční směrovače. Vnitřní směrovače zajišťují komunikaci uvnitř sítě s prioritním řízením obsluhy s využitím QoS. Hraniční směrovače mají za úkol pečlivě zkoumat příchozí provoz a na základě definovaných pravidel QoS vyhodnocovat

jednotlivé pakety a označit je patřičnou značkou priority a předávat je vnitřním směrovačům DiffServ domény. Hraniční 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 vnitřními směrovači a vystupují přes egress směrovač, jak je znázorněno na Obr. 2.4.

2.2.1 Klasifikace a značkování paketů

Klasifikace paketů

Klasifikace pouze filtruje a rozpoznává toky dle provozovaných služeb a zdrojů s případným omezením či dokonce odmítnutím daného toku. Při klasifikaci se provoz může rozdělit do více rozdílných tříd. Ke klasifikaci mohou být použity četné charakteristiky. K jednotlivým třídám se přistupuje odděleně dle výstupních front zařízení, aby mohla být zaručena různá prioritní obsluha pro jednotlivé třídy. Do třídy „REAL TIME“ by mohl být umístěn provoz protokolem RTP a aplikace v reálném čase (VoIP), zatím co provoz FTP, SMTP či POP3 by mohl být umístěn do třídy „NORMAL“. Názvy jednotlivých tříd jsou ponechány na fantazii správce sítě. Klasifikace nicméně nemění žádné bity v datovém rámci nebo paketu, [3].

Značkování paketů

Při značkování se manipuluje s bity uvnitř rámce, buňky nebo paketu, a tím je síť informována o tom, jak s tímto provozem zacházet. Samotné značkování však neovlivňuje, jak síť s paketem zachází. Na tyto značky se nicméně mohou odvolat jiné nástroje QoS (nástroje řazení do front) a na jejich základě se rozhodnou o jejich předání či zahození. Značkování je následným krokem po klasifikaci paketů do jednotlivých tříd, tudíž klasifikace a značkování na sebe úzce navazuje a v některých literaturách se tyto pojmy nerozlišují.

Včasná klasifikace a označení paketů jsou důležité procedury a je třeba je implementovat co nejblíže ke zdroji vysílání dat. Ideální případ je, pokud pakety značkuje datový zdroj, tedy pokud aplikace odesílající data přímo značí vysílané pakety. Příkladem můžou být IP telefony, které umožňují zadávat prioritu paketům se službou VoIP. Pokud terminál vysílající data do sítě neumožňuje značkování paketů, je paket označen až při vstupu do DiffServ domény v ingress směrovači. Výběr prioritní značky je nejčastěji zvolen na základě použitého portu aplikační vrstvy, případně IP adresy odesílatele či příjemce. 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 odlišným významem. Ingress směrovač může tuto značku pozměnit nebo zachovat, [2].

Způsob označení paketu závisí na zvolené technologii nebo protokolu použitém pro přenos. Nejčastější je implementace Diffserv na úrovni síťové vrstvy při použití IP protokolu. Na linkové vrstvě je též možné značkovat rámce, pokud daný přepínač tuto možnost podporuje. V případě IP protokolu se priorita provozu značkuje pomocí číselného (bitového) vyjádření v hlavičce IP paketu. Hlavička paketu dnes nejpoužívanějšího protokolu IP verze 4 (IPv4) je zobrazena na obrázku Obr. 2.5 a jeho zatím nerozšířený nástupce IP verze 6 (IPv6) na obrázku Obr. 2.6.

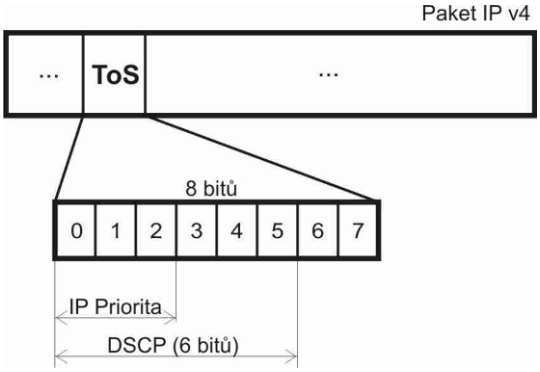
<table>
<tr><td>Ver. (4b)</td><td>IHL (4b)</td><td>Type of Service (8b)</td><td colspan="2">Total Length (16b)</td></tr>
<tr><td colspan="3">Identification (16b)</td><td>Flags (3b)</td><td>Frag. Offset (13b)</td></tr>
<tr><td colspan="2">Time to Live (8b)</td><td>Protocol (8b)</td><td colspan="2">Header Checksum (16b)</td></tr>
<tr><td colspan="5">Source Address (32b)</td></tr>
<tr><td colspan="5">Destination Address (32b)</td></tr>
<tr><td colspan="5">Options + padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Obr. 2.5: Hlavička paketu IPv4

Ver. (4b)	Traffic Class (8b)	Flow Label (20b)	
Payload length (16b)		Next Header (8b)	Hop Limit (8b)
Source Address (128b)			
Destination Address (128b)			

Obr. 2.6: Hlavička paketu IPv6

V hlavičce protokolu IPv4 se nachází bajt (tzn. 8 bitů), který se nazývá bajt ToS (Type of Service). U novějšího protokolu IPv6 je také vyčleněn jeden bajt s označením TC (Traffic Class). Struktura a značení polí ToS a TC je shodné v obou protokolech. Dále již bude popisován pouze IPv4 (tedy ToS) z důvodu návaznosti v praktické části této práce. Pakety se tedy značkují pomocí bitů uvnitř bajtu ToS, a to prostřednictvím kódu DSCP (Differentiated Service Code Point) o délce 6 bitů, případně pouze IP prioritou, jak je znázorněno na Obr. 2.7. Zbylé dva bity se nevyužívají, [3].



Obr. 2.7: Bajt ToS

Kód DSCP, který pracuje se šesti bity umístěnými zcela vlevo v bajtu ToS, zobrazuje Obr. 2.7. Šest bitů poskytuje 64 možných hodnot. Takové velké množství prioritních hodnot je třeba zorganizovat. Důležité síťové informace, které si předávají směrovače mezi sebou k udržování sítě, také využívají tento prioritní bajt k upřednostnění při vytížení. Bylo by nežádoucí upřednostnit jakýkoliv provoz nad řízení sítě. Implementace DifServ se označuje jako Per Hop Behaviours (PHB), protože každý směrovač pracuje s pakety nezávisle na ostatních. Oproti implementaci IntServ, kde všechny směrovače vyhrazují danému toku stejné prostředky (Per-Flow Behaviour).

2.2.1.1 Technika podpory QoS typu Per Hop Behaviour

V poli DSCP je možné pomocí šesti bitů docílit až 64 úrovní, které mohou značit prioritu daného paketu. 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 s pakety, u kterých není známa hodnota PHB, mapují právě také na hodnotu nula. Každý směrovač nebo přepínač na třetí vrstvě má definované chování (PHB), pokud se objeví více požadavků na jeho zdroje, jako vyrovnávací paměť nebo šířka pásma.

V rámci DSCP se specifikovaly čtyři kategorie chování PHB, [1]:

- Selektor třídy (Class Selector – CS)
- Zajištěné předávání (Assured Forwarding – AF)
- Urychlené předávání (Expedited Forwarding – EF)
- Základní služba (Best Effort – BE)

Selektor třídy (CS-PHB)

Paketový provoz je rozdělen do osmi základních úrovní pro určení priority přenosu. Kategorie CS-PHB zajišťuje kompletní zpětnou kompatibilitu s hodnotami IP Priority (IP Precedence), protože stejně jako IP priorita mají CS-PBH nuly ve čtvrtém, pátém a šestém bitu bajtu ToS, jak je znázorněno v Tab. 2.1. K zajištění kompatibility priorit s dalšími metodami využívá CS-PHB právě první tři bity MSB v poli DSCP.

Tab. 2.1: Selektor třídy PHB

Selektor třídy PHB		
PHB	**DSCP**	**Název**
CS0	**000** 000	Routine
CS1	**001** 000	Priority
CS2	**010** 000	Immediate
CS3	**011** 000	Flash
CS4	**100** 000	Flash Override
CS5	**101** 000	Critical
CS6	**110** 000	Internetwork control
CS7	**111** 000	Network control

Zajištěné předávání (AF-PHB)

Kategorie AF chování PHB představuje nejširší kategorii a konkrétně představuje 12 rozdílných hodnot chování PHB. Umožňuje zařadit pakety do jedné ze čtyř tříd. Každé třídě je ve směrovačích přidělen určitý objem prostředků, například velikost vyrovnávací paměti nebo kapacita výstupního spoje. V rámci každé třídy pak může být každému paketu přiřazena jedna ze tří priorit zahození paketu (drop precedence). 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 pro jednotlivé třídy jsou uvedeny v Tab. 2.2.

Tab. 2.2: Zajištěné předávání PHB

Priorita AF PBH	Třída 1	Třída 2	Třída 3	Třída 4
Nízká	001 010	010 010	011 010	100 010
Střední	001 100	010 100	011 100	100 100
Vysoká	001 110	010 110	011 110	100 110

Urychlené předávání (EF-PHB)

Kategorie EF (Expedited Forwarding) poskytuje nástroje pro zajištění nízké ztrátovosti, malého zpoždění a zajištění šířky pásma pro koncové služby přes Diffserv doménu. EF PHB chování PBH má pole DSCP přesně stanovené na hodnotu 46 (101 110), která odpovídá úrovni CS5 v CS-PHB. V porovnání s předchozími kategoriemi je hodnota DSCP vyšší, z čehož vyplývá, že EF má vyšší prioritu. Například přenos hlasu (VoIP) je typický pro označení EF-PHB.

Základní služba (BE-PHB)

Pouze provoz, který vyžaduje zacházení na nejnižší úrovni, je označen kategorií BE (Best Effort) chování PHB, což znamená, že všech šest bitů v části MSB bajtu ToS jsou nuly. Hodnota DSCP je 0.

Hodnoty DSCP pro všechny typy chování jsou uvedeny v tabulce Tab. 2.3. Třídy jsou vzájemně kompatibilní, protože všechna chování vycházejí z binární hodnoty v poli ToS IP paketu.

Tab. 2.3: Kódy DSCP pro PHB

Per hop behaviour	Označení třídy	DSCP (bin)	DSCP (dec)
Expedited forwarding	EF	**101** 110	46
Assured forwarding	AF		
Class Selector 4 (CS4)	AF43 (high drop preference)	**100** 110	38
	AF42 (medium drop preference)	**100** 100	36
	AF41 (low drop preference)	**100** 010	34
Class Selector 3 (CS3)	AF33 (high drop preference)	**011** 110	30
	AF32 (medium drop preference)	**011** 100	28
	AF31 (low drop preference)	**011** 010	26
Class Selector 2 (CS2)	AF23 (high drop preference)	**010** 110	22
	AF22 (medium drop preference)	**010** 100	20
	AF21 (low drop preference)	**010** 010	18
Class Selector 1 (CS1)	AF13 (high drop preference)	**001** 110	14
	AF12 (medium drop preference)	**001** 100	12
	AF11 (low drop preference)	**001** 010	10
Best Effort	Default	**000** 000	0

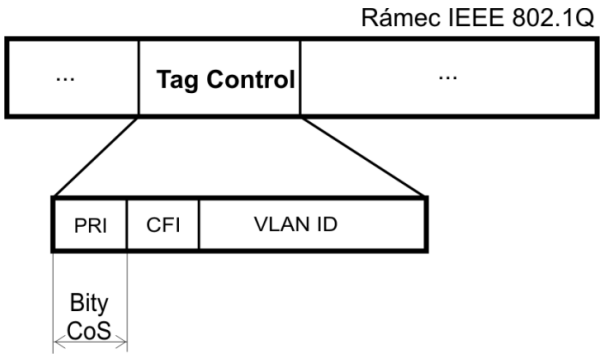
2.3 KLASIFIKACE RÁMCŮ

Až dosud jsme zkoumali značení paketů za pomocí bajtu ToS v hlavičce protokolu IP. Nicméně je také možné provoz značit na druhé vrstvě modelu OSI (tj. na linkové vrstvě), kde se datová jednotka nazývá rámec. Dříve než se objevily zmíněné modely IntServ a DiffServ pro zajištění QoS na 3. vrstvě modelu OSI, existovala také podpora pro QoS na 2. vrstvě modelu OSI.

Podmínkami pro dosažení opravdové end-to-end podpory QoS jsou nezávislost implementace na médiu resp. na technologii 2. vrstvy OSI a vzájemné mapování klasifikátorů QoS na 2. a 3. vrstvě modelu OSI [1].

Rámce proudící po ethernetovém spoji je možné označit hodnotou třídy služby CoS (Class of Service) druhé vrstvy, jak je znázorněno na Obr. 2.8. Rámec IEEE 802.1Q má vyhrazeny 3 bity v bajtu Tag Control k označení hodnoty CoS. Pomocí bitů CoS je tedy možno definovat až osm prioritních hodnot (0–7), ačkoliv společnost Cisco doporučuje nepoužívat hodnoty 6 a 7, protože tyto hodnoty jsou vyhrazeny pro řízení v síti, obdobně jako je tomu u tříd služeb PHB na síťové vrstvě. Vkládání IP paketu do rámce včetně bitů pro určení priority na síťové i linkové vrstvě je zobrazen na Obr. 2.10.

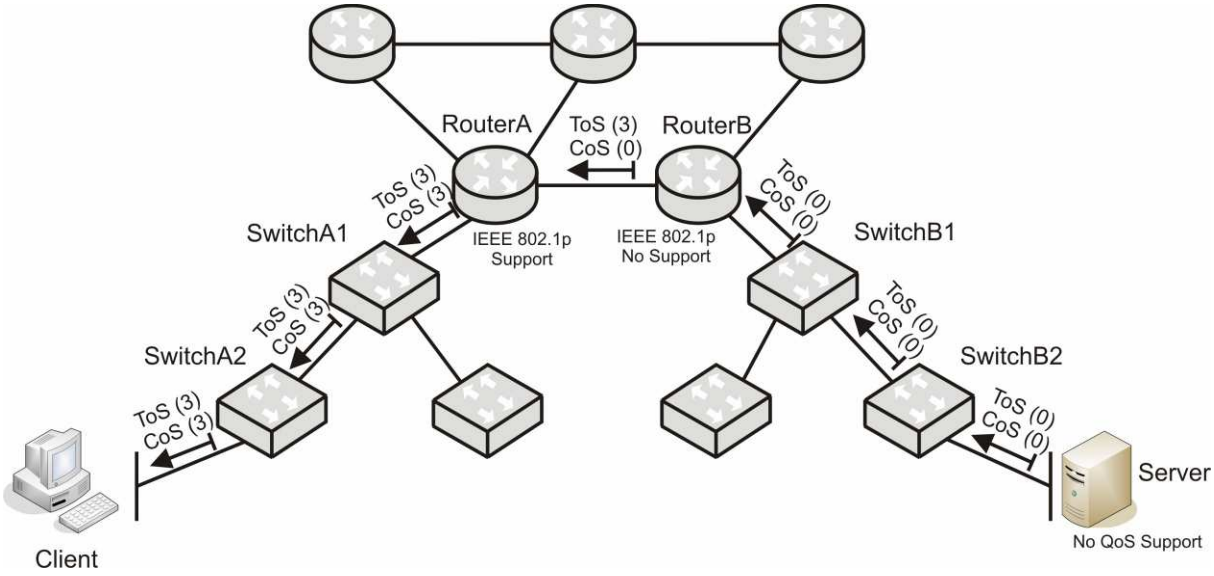
Rámce IEEE 802.1.Q jsou definována pro přenos pomocí VLAN sítí. To znamená, že pokud chceme aplikovat QoS i na linkové vrstvě je žádoucí vytvořit virtuální sítě.



Obr. 2.8: Značení třídy služby na linkové vrstvě

Vazba priorit mezi síťovou a linkovou vrstvou

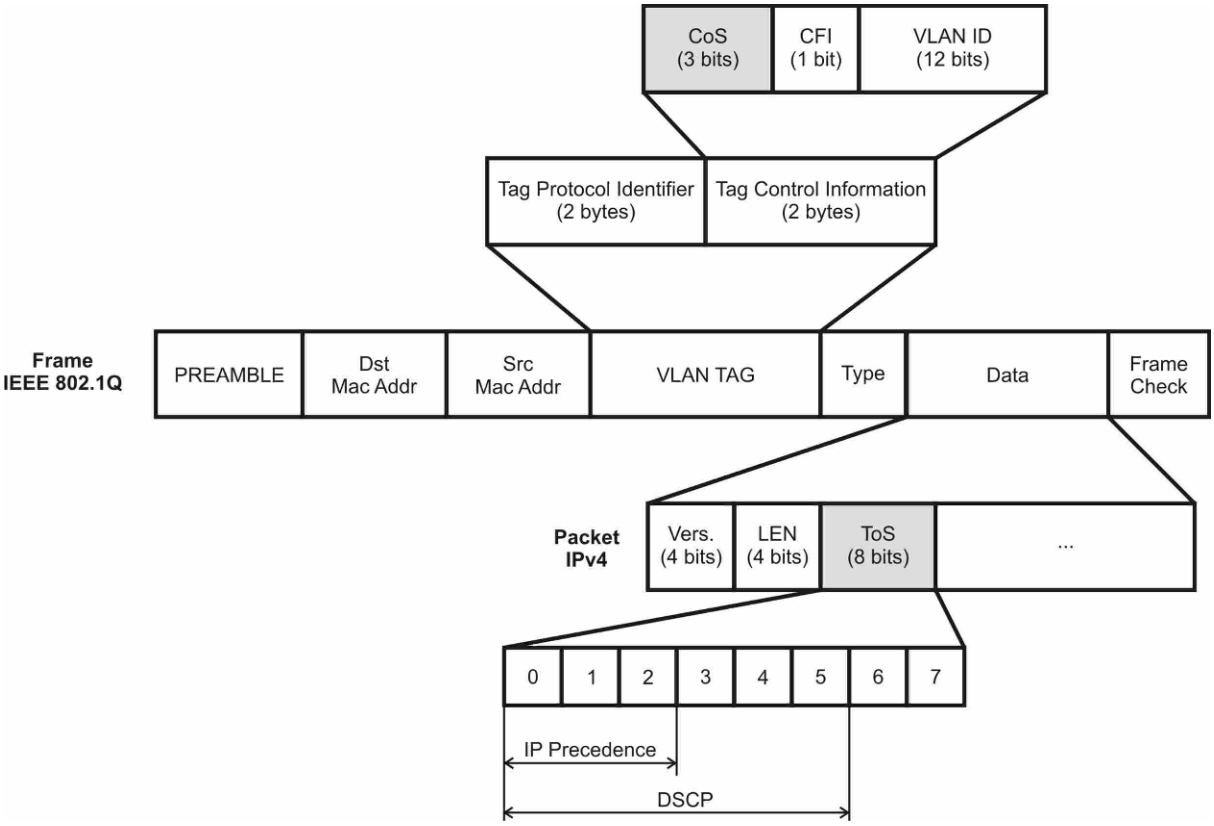
Důležitá věc, kterou je třeba mít při plánování na paměti je, že značku CoS většina směrovačů ignoruje a sleduje pouze značky v bajtu ToS na síťové vrstvě. To znamená, že pokud identifikujeme priority provozu pouze pomocí značky CoS, musí být tato značka při průchodu směrovačem přeznačena na značku třetí vrstvy, jelikož samotný směrovač nemusí brát zřetel na označení na linkové vrstvě. V opačném případě je situace podobná. Je třeba zajistit, aby paket označen vysokou prioritou ToS byl zároveň přeznačen vysokou hodnotou CoS na linkové vrstvě, čímž docílíme plnohodnotného zajištění kvality služeb jak na síťové vrstvě, tak i na vrstvě linkové. Implementace vyšších priorit do značek rámce proudící přes ethernetový spoj dle IEEE 802.1Q se označuje jako IEEE 802.1p [2]. Ne každý směrovač podporuje přeznačení priority rámců podle paketů. Na Obr. 2.9 je uveden příklad, kdy server posílá klientovi důležitá data s prioritou „3“ a nepodporuje žádný způsob značení QoS. K přeznačení dochází až na hraničním směrovači (RouterB), kde je IP paket klasifikován. Protože směrovač nepodporuje přeznačení na linkovou vrstvu, dále odesílá rámec s nulovou prioritou oproti směrovači, který přeznačení IEE 802.1p podporuje.



Obr. 2.9: Vliv podpory přeznačení rámců - IEEE 802.1p

I když společnost Cisco doporučuje značit provoz co nejblíže u zdroje, většinou poskytovatel připojení k Internetu nebude chtít, aby si koncoví uživatelé nastavovali vlastní značku priority, respektive jim nebude věřit. 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 na IP telefon.



Obr. 2.10: Důležité prioritní bity v paketu a rámci pro QoS.

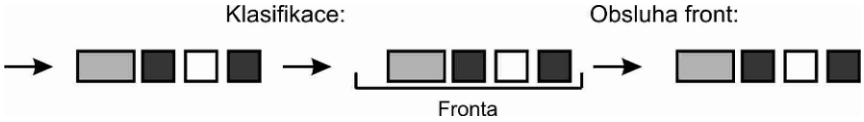
3 OBSLUHA FRONT

Pokud zařízení, jako je přepínač nebo směrovač, přijímá provoz rychleji, než dokáže obsloužit či odeslat, pak se zařízení pokusí tento nadměrný provoz uložit do vyrovnávacích pamětí, dokud nejsou dostupné prostředky pro jeho zpracování. Tento proces ukládání do paměti se nazývá řazení do front. Řízení přetížení je činnost dohledu nad úrovní zaplňování front a činnost řízení při zaplnění fronty. Směrovače obsahují jak hardwarové, tak softwarové fronty. První paket, který vstoupí do hardwarové fronty, je také prvním, jenž ji opustí. Jakmile se však kapacita hardwarové fronty zaplní, uloží směrovač další pakety do softwarové fronty, u které můžeme použít různé mechanizmy řazení fronty k ovlivnění pořadí, ve kterém různé typy provozu opouští tuto frontu. Mechanizmů řazení fronty je spousty, a proto zde budou zmíněny pouze ty nejpoužívanější. (FIFO, CBWFQ a LLQ), [3].

K přetížení částí sítě může docházet jak v páteřních sítích WAN, tak i v lokálních sítích LAN, a to především v důsledku nesprávně navržené topologie a nesprávného dimenzování spojů a přepojovacích schopností jednotlivých síťových uzlů (přepínačů a směrovačů. K přetížení spoje dochází na síťových uzlech, kde dochází ke sloučení více příchozích spojů do jednoho výstupního toku; např.: když se k přepínači při rychlosti Ethernet (10Mb/s) připojí mnoho pracovních stanic a současně provádí přenos na shodný server, který je připojen ke stejnému přepínači opět prostřednictvím 10Mb/s spoje.

Řazení FIFO

Metoda řazení FIFO používá pouze jednu frontu. Metoda ve skutečnosti neprovádí žádné operace spojené s QoS. Jak již název napovídá, první paket, který přijde do fronty, je také první paket, jenž ji opustí, jak je naznačeno na Obr. 3.1. Směrovače používají metodu FIFO ve svých hardwarových frontách. Metoda FIFO v softwarové frontě pracuje stejně jako v hardwarové frontě. Fronta má omezenou délku, a pokud je zaplněna, dojde k zahazování všech dalších příchozích paketů bez ohledu na jejich hodnotu DSCP. Způsob řazení z pohledu kvality služeb neřeší prioritu toků a ani nezaručuje minimální propustnost k zabránění tzv. vyhladovění provozu. 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 výpadek v přenosu telefonního hovoru.

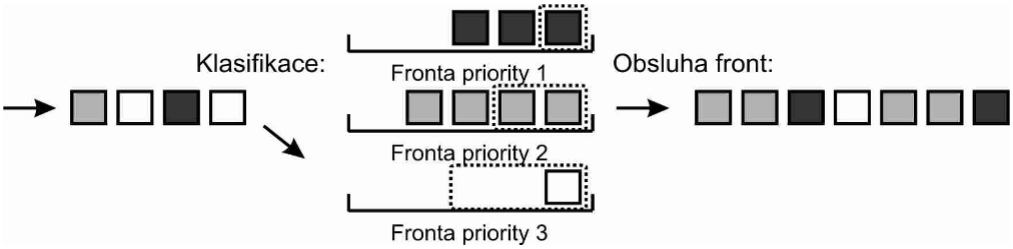


Obr. 3.1: Obsluha fronty metodou FIFO.

Řazení CBWFQ (Class-Based Weighted Fair Queuing)

Mechanizmus CBWFQ rozděluje vstupní tok paketů do více samostatných tříd. Každé třídě je přiřazena váhová hodnota. Součet všech váhových hodnot odpovídá celkovému součtu šířce pásma. Váhová hodnota udává velikost okna pro obsluhu. Velikost okna se volí podle priority paketu. Pakety v třídě s vyšší prioritou jsou obslouženy s větším odbavovacím oknem, čímž je dosažena rychlejší obsluha a přenos dat. Princip obsluhy paketů je naznačen na Obr. 3.2. Mechanizmus také zajišťuje, že žádný definovaný provoz nevyhladoví, čili není opomíjen. Pomocí mechanismu CBWFQ můžeme přesně určit minimální šířku pásma, která bude pro různé typy provozu dostupná. Provoz pro každou třídu vstupuje do samostatné fronty. Může se stát, že jedna fronta bude přetékat, zatímco jiné fronty stále přijímají pakety.

Nevýhodou tohoto mechanizmu je nedostatek mechanizmů pro prioritní využití šířky pásma. Tento problém dokáže vyřešit drobná úprava řazení CBWFQ, která se nazývá LLQ.



Obr. 3.2: Obsluha front metodou CBWFQ.

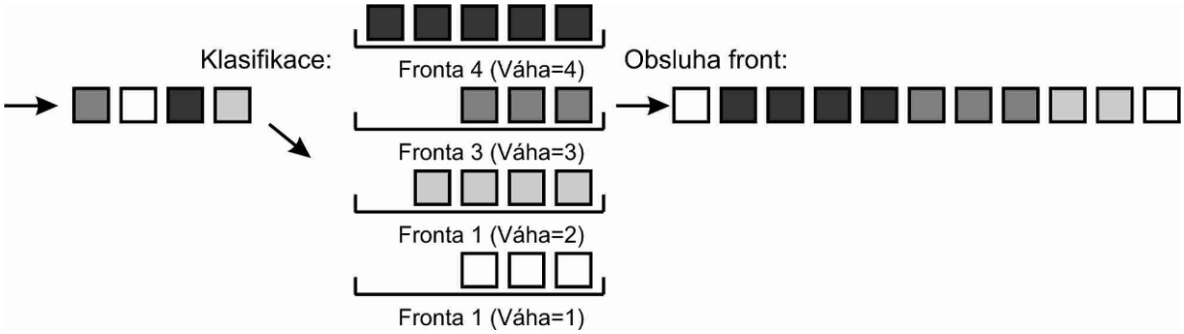
Řazení LLQ (Low Latency Queuing)

LLQ vytváří striktně prioritní frontu. Pakety v této frontě mají vždy přednost před ostatními. Řazení je ve své konfiguraci téměř identické s řazením CBWFQ. Mechanizmus zaručí minimální šířku pásma jednotlivým frontám podle nastavení. Nedochází k vyhladovění žádné datové služby.

Řazení WRR (Weighted Round Robin)

Výše zmíněné mechanizmy pracují s pakety na síťové vrstvě. Metoda obsluhy řazení WRR se používá na vrstvě linkové, tedy k řazení rámců. K prioritnímu rozdělení rámců do front je nejčastěji použita hodnota v hlavičce rámce CoS. V podstatě jde o obdobný přístup jako při obsluze paketů mechanizmem CB-WFQ.

Frontám mohou být přiděleny váhy, které ovlivní, jakou šířku pásma rámce s různým značením dostanou. Princip metody řazení WRR [3] je znázorněn na obrázku Obr. 3.3. 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.



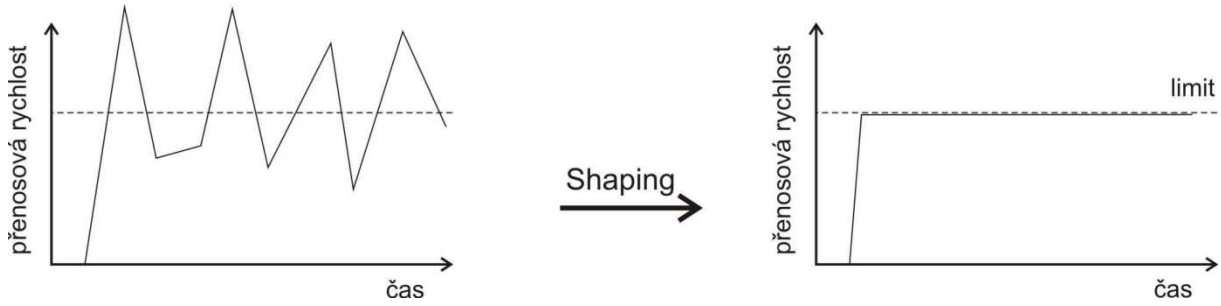
Obr. 3.3: Obsluha front metodou WRR.

4 OMEZOVÁNÍ RYCHLOSTI

V určitých případech je potřeba místo přidělování minimální šířky pásma datovým tokům omezit maximální dostupnou šířku pásma pro určitý provoz. Mechanizmy QoS, které limitují šířku pásma, se nazývají usměrňovače provozu. Jejich účelem je omezit šířku pásma pro určitý datový provoz, tedy nastavit maximální datový tok, který provoz nemůže překročit. Minimální pásmo pro datový provoz ale nijak negarantují. Základní dvě kategorie usměrňovačů jsou shaping a policing [3]. Přestože oba tyto způsoby limitují šířku pásma, jejich činnost je odlišná.

Shaping

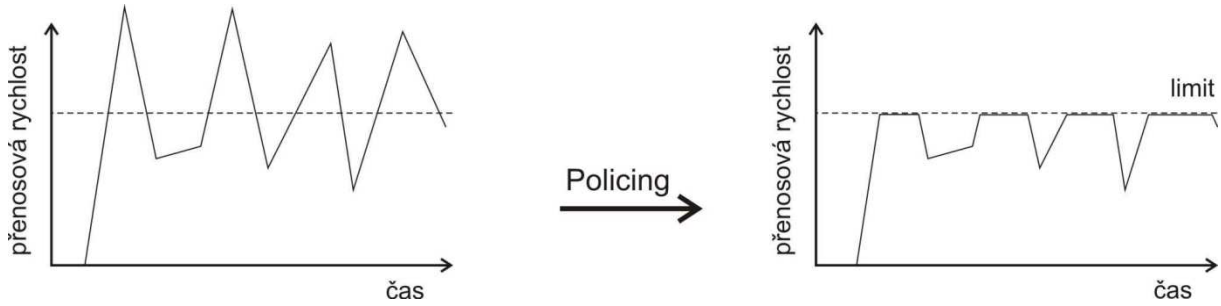
Shaping omezuje nadměrný provoz ukládáním do vyrovnávací paměti nikoliv jeho zahazováním. Následně jej v dalším časovém kroku odešle tak, aby celkově nepřekročil nastavenou limitní rychlost odesílání. Shaping potlačuje ztrátu paketů, používá se tedy především při propojování síťových uzlů s odlišnými rychlostmi. Tímto ukládáním nadměrného provozu do paměti síťového uzlu se zvyšuje zpoždění pro přenášené pakety. Průběh omezování rychlosti je zobrazen na Obr. 4.1.



Obr. 4.1: Omezení rychlosti mechanizmem shaping

Policing

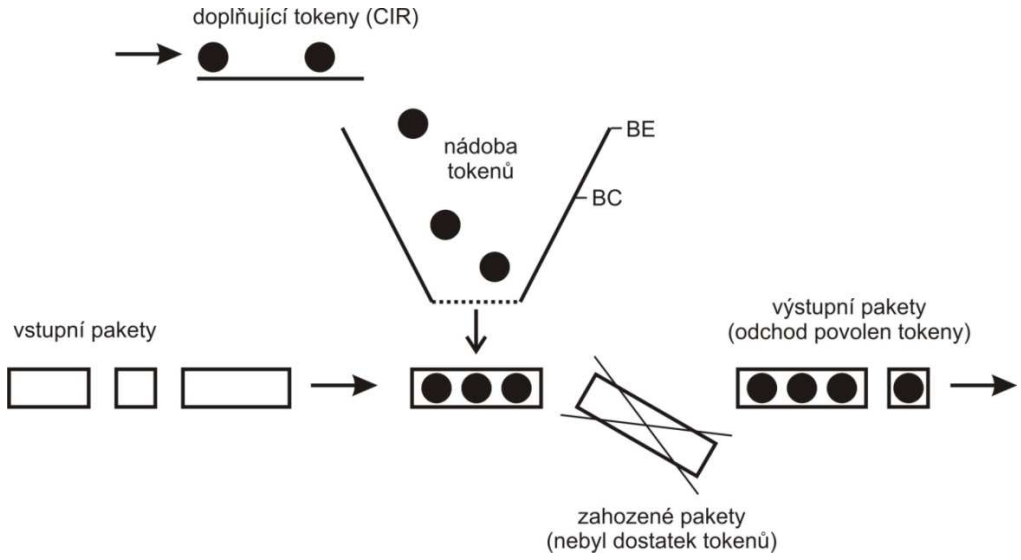
Policing typicky omezuje šířku pásma tím, že zahazuje jakýkoliv provoz, který převyšuje danou limitní rychlost. Policing však také dokáže přeznačit provoz, který převyšuje danou rychlost, a pokusí se pakety poslat do fronty s nižší prioritou. Metoda obvykle představuje jednoduché zahazování přicházejících paketů (paket je směrovačem ignorován a není posílána žádná zpráva o zahození ke zdroji dat), což má za následek opakované vysílání paketů při spojení nad protokolem TCP. Názorný příklad je uveden na Obr. 4.2, kde převyšující rychlost odesílání je striktně zahazována. V rozšířeném nastavení je možné povolit krátkodobé překročení limitní hodnoty.



Obr. 4.2: Omezení rychlosti mechanizmem policing.

Nejvíce využívanou metodou pro řízení toku dat je metoda token bucket, [5]. Tento přístup slouží k vyrovnávání různě velkého objemu dat přicházejícího nepravidelnými rychlostmi na vstupní porty směrovače v síti tak, aby nemohlo dojít k překročení výstupní kapacity linky.

Pro ilustraci činnosti usměrňovačů provozu si představme přirovnání s nádobou pověření (token bucket). Směrovač stálou rychlostí CIR (Commited Information Rate) doplňuje tolik pověření, kolik odpovídá hodnotě BC (Committed Burst). Do nádoby se celkem vejde BE (Excess Burst) pověření. V konfiguraci policing se provoz, který nevyžaduje odeslání většího počtu bitů než BC, nazývá vyhovující (Conform) provoz. O provozu, který vyžaduje větší počet bajtů než BC, se říká, že jde o nadměrný (Excess) provoz. Dlouhodobý průměr rychlosti přenášených dat nesmí překročit rychlost doplňování tokenů CIR a krátkodobé špičky nesmí překročit velikost nádoby BE, jinak dojde k zahození paketu. Jedná se o usměrňovač s jednou nádobou. Princip policing s jednou nádobou je naznačen na Obr. 4.3.



Obr. 4.3: Metoda token bucket s jednou nádobou

Metoda token bucket má i svá rozšíření v podobě zavedení dvou nádob s dvourychlostním policingem, kde má každá nádoba odlišnou rychlost doplňování tokenů (CIR a PIR).

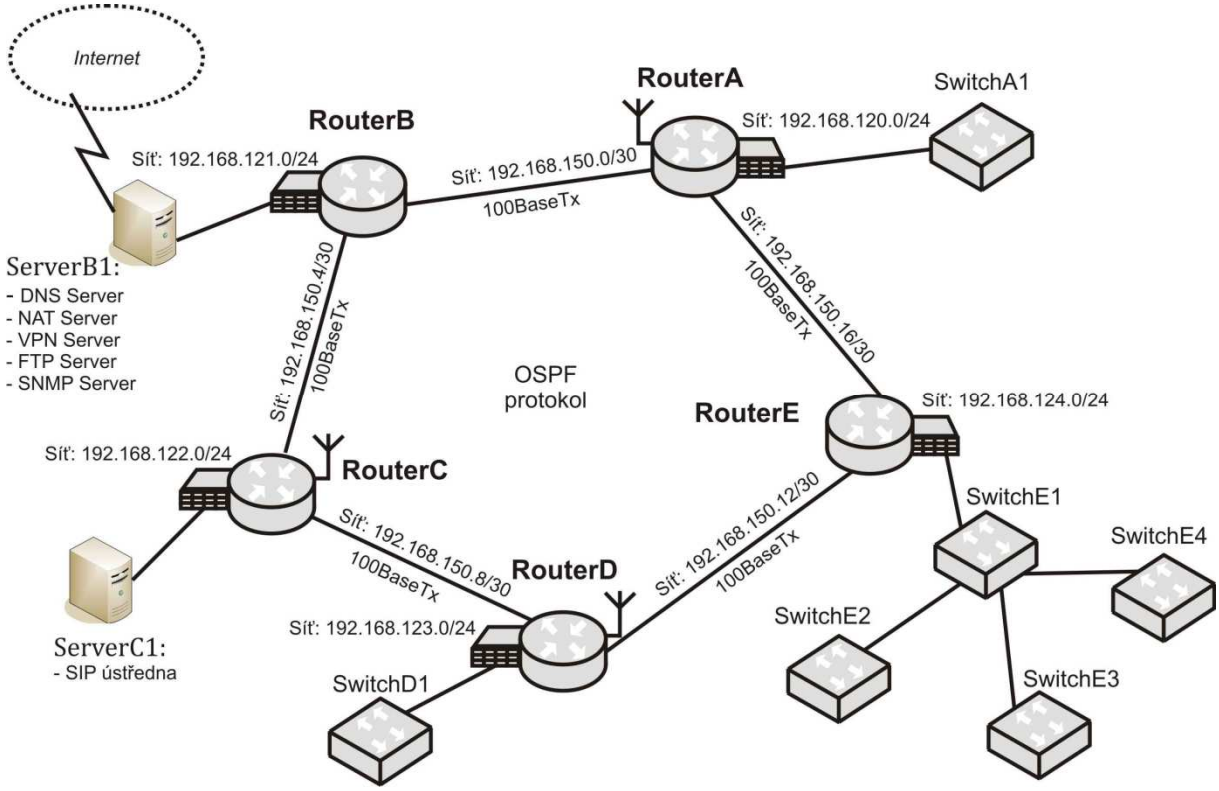
Pokud zpracovávaný paket vyprázdní tokeny z první nádoby, je možné využít tokeny z druhé nádoby. Není-li možné paket přesměrovat pomocí bajtů z první nádoby, ale lze ho přesměrovat pomocí bajtů z nádoby druhé, říká se, že jde o nadměrný (Excess) provoz. V případě, že paket nelze přesměrovat pomocí žádné ze dvou nádob, jedná se o porušující (Violating) provoz.

Hlavní parametry, které se nastavují u algoritmu token bucket, [13]:

- CIR – průměrná přenosová rychlost, provoz klasifikován jako vyhovující – Conform.
- BC - počet bitů, o které je možno jednorázově překročit rychlost CIR, provoz klasifikován jako nadměrný – Excess.
- BE - počet bitů, o které je možné jednorázově překročit rychlost CIR, provoz klasifikován jako porušující – Violating.

5 EXPERIMENTÁLNÍ SÍŤ

K ověření skutečného zacházení a přístupu k paketům a rámcům v ethernetové síti z pohledu QoS byla v laboratoři UTKO navržena a sestavena experimentální síť. Je navržena nejen za účelem testování kvalitativních parametrů služeb v síti, ale i pro realizaci dalších činností spojených s provozem služeb či dohledem nad sítí jako takovou (těmito aktivitami se tato práce nezabývá). Z dostupných síťových prvků v laboratoři byla navržena a realizována síť s topologií zobrazenou na Obr. 5.1. Všechna použitá zařízení v síti byla nainstalována a postupně nastavena. Některá stávající zařízení bylo třeba resetovat do továrního nastavení.



Obr. 5.1: Topologie experimentální sítě

Experimentální síť je rozčleněna na pět jednotlivých podsítí, které jsou navzájem propojeny směrovači v kruhové topologii. O konektivitu mezi podsítěmi se stará směrovací protokol OSPF. Každá podsíť je připojena k páteřní síti jedním směrovačem, který je výchozí bránou pro danou podsíť, tudíž je veškerý provoz přenášen a z pohledu QoS klasifikován a značkován v daném směrovači. Pomocí serveru, který je druhou síťovou kartou připojen do veřejné sítě Internet, je možné zpřístupnit všem klientům experimentální sítě připojení k Internetu za použití role NAT (Network Address Translation). Adresování všech sítí je pomocí IP adres z rozsahu třídy C. Adresní prostor pro zařízení v jednotlivých přístupových sítích je 8 bitů (253 možných IP rozhraní), například síť, připojena k směrovači E, je 192.168.124.0/24. V případě páteřních sítí je pro naznačení šetření rozsahů IP adres použito VLSM (Variable Length Subnet Mask) adresování. Například spojení mezi směrovači C a D používá adresní prostor 2 bity (dvě možné IP rozhraní) s označením 192.168.150.8/30, viz Obr. 5.1.

5.1 DATOVÉ SLUŽBY

Počítačová síť Internet nabízí velkou škálu datových služeb, které je možné přenášet. Přenášená data mají vždy svého příjemce a odesílatele, tudíž druh datové služby je převážně spojen s možnostmi odesílatele – serverem. I obyčejný koncový počítač nebo notebook připojený k podnikové síti se též

může stát odesílatelem (serverem) dat a odesílat data jinému počítači – klientovi. Existují však i služby peer-to-peer, kde jsou si komunikující strany rovny.

Datové služby se převážně liší podle svých požadavků na přenos. Problematikou parametrů jednotlivých typů služeb se zabývá kapitola 1. S ohledem na dostupnost hardwarového a softwarového vybavení byly v experimentální síti realizovány tyto služby datového přenosu:

- hlasové služby (VoIP),
- video služby (Streaming),
- prohlížení webových stránek (www),
- přenos souborů (FTP).

Hlasové služby (Voice over Internet Protocol)

K realizaci hlasové služby (VoIP) jsou zapotřebí hlasové terminály v podobě IP telefonů a síť telefonních ústředen, případně i hlasové a signalizační brány pro propojení různých architektur.

V experimentální síti byla nainstalována telefonní ústředna Asterisk. Jde o kompletní open-source softwarovou PBX (Private Branch eXchange), běžící na platformách unixového typu. Propojení mezi ústřednou a terminály využívá protokol SIP, který standardně naslouchá na portu TCP 5060.

K ústředně bylo přihlášeno celkem šest telefonů. Dva softwarové a čtyři hardwarové IP telefony různých výrobců. Použité hardwarové IP telefony jsou na Obr. 5.2. Telefony disponují mnoha telefonními a síťovými službami. Některé nabízí i video-telefonii. Z pohledu QoS podporují značkování paketů podle chování EF-PHB dle specifikace DiffServ. Hlavičky všech hlasových paketů je možné již v telefonech značit hodnotou EF v bajtu ToS.

Obr. 5.2: IP telefony v experimentální síti (INTERBELL IB-402, Huawei Viewpoint 8220, Grandstream GXV-3000 a INTERBELL IB-402)

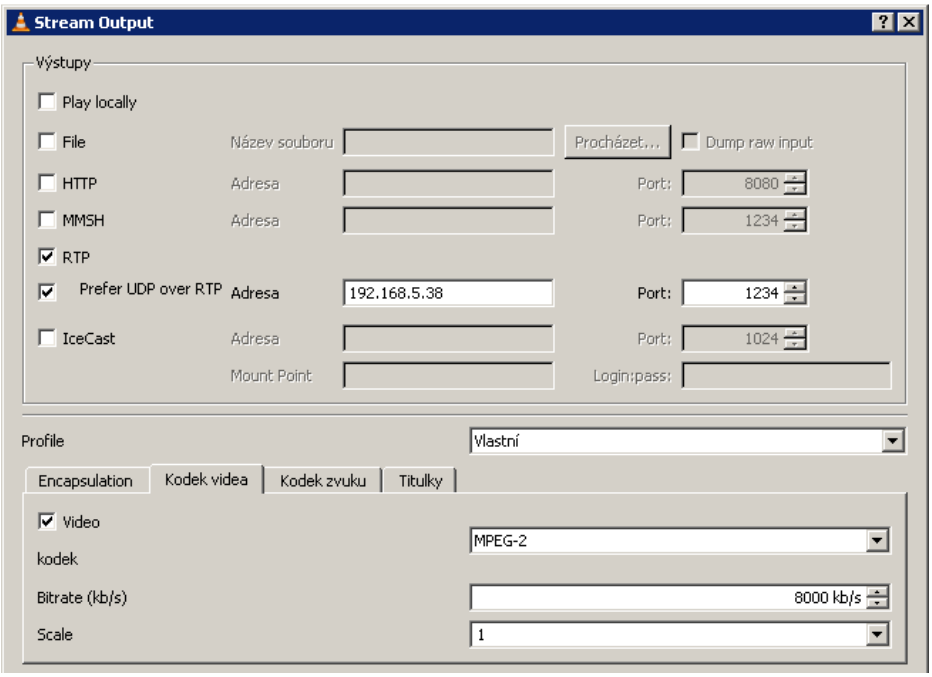
Pro hlasové a videokomunikační služby v experimentální síti byly zvoleny parametry:

- signalizační protokol SIP (port 5060) – signalizační informace,
- transportní protokol RTP Audio – přenos hlasových dat (kodek G.711),
- transportní protokol RTP Video – přenos videodat (kodek H.263).

Video služby (Streaming)

Streamování videa je možné realizovat mnoha způsoby. Nejpoužívanější způsob je pomocí multicastové adresy. Jednodušší varianta je generovat video tok jako službu na serveru na daném portu a na straně přijímací stanice se k serveru připojit pomocí klientské přehrávací aplikace. 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 i jako klient pro přehrávání videa byl použit volně stažitelný software VideoLAN VLC media player, 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. 5.3. K streamování videa je použit port 1234 a protokol UDP. Video-přenos je možné definovat průměrnou přenosovou rychlostí mezi hodnotami 700kb/s až 8Mb/s pro jeden datový tok pro kodek videa MPEG-2.



Obr. 5.3: Možnosti nastavení výstupního videa pomocí aplikace VideoLAN.

Video služba v experimentální síti je charakterizována:

- protokol UDP (port 1234),
- formát videa MPEG-2 (datový tok 8000 kb/s),
- formát zvuku MPEG Audio (datový tok 128 kb/s).

Prohlížení webových stránek (www)

Služba prohlížení webových stránek je jedna z nejpoužívanějších služeb v síti Internet. Klienti pomocí webového prohlížeče mohou zobrazovat mnohé informace uložené na vzdáleném webovém serveru. Experimentální síť je připojena k síti Internet, a tudíž klienti připojení v experimentální síti mohou komunikovat s webovými servery z veřejné sítě Internet. Tímto přenosem vzniká datový tok paketů označovaný jako datová služba www.

Prohlížení webových stránek v experimentální síti je charakterizováno:

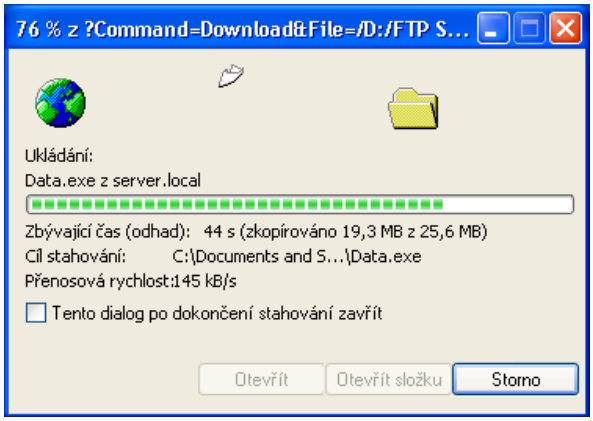
- protokolem http

Přenos souborů (FTP)

Pro přenos souborů v síti se používá protokol k tomu určený – File Transfer Protocol. Jedná se o spolehlivý přenos, který využívá transportní protokol TCP. Komunikující strany server a klient se

pomocí protokolu informují o možnostech spojení, využívají maximální propustnost sítě a jsou schopny měnit rychlost odesílání podle vytížení spoje.

V experimentální síti byl nainstalován OpenSource FTP server FileZilla Server. Registrovaní uživatelé mohou po přihlášení neomezeně stahovat data ze serveru a tím síť zatíží potřebným datovým provozem. Příklad přenosu z FTP serveru je zobrazen na Obr. 5.4.



Obr. 5.4: Přenos souboru z FTP serveru.

5.2 SÍŤOVÉ PRVKY V EXPERIMENTÁLNÍ SÍTI

Pro vytvoření sítě plně podporující kvalitu služeb (QoS) je třeba klasifikovat a značkovat přenášené pakety co nejblíže od zdroje vysílání. Některé zdroje služeb nepodporují značkování a vysílají pakety se základním nastavením priority QoS (Best Effort). Tyto pakety musí být přeznačeny na hranici DiffServ domény v ingress směrovači.

DiffServ doménu v experimentální síti tvoří páteřní směrovače. Každý směrovač je jedním fyzickým rozhraním připojen k síti, která leží mimo DiffServ doménu, a tudíž všechny směrovače pracují i jako brána do domény DiffServ (Ingress a Egress směrovač), viz kapitola 2.2.

5.2.1 Směrovače

Všech pět použitých směrovačů je od společnosti Cisco, jedná se o modely ze série 1800 lišících se pouze v podpoře dostupných fyzických rozhraních, které však nejsou v navržené experimentální síti využívány (ISDN, Wifi).

Směrovač Cisco 1800 série

Směrovače Cisco používají ke své činnosti operační systém IOS. Cisco IOS má charakteristický příkazový řádek (CLI – Command Line Interface), jehož styl se rozšířil do dalších síťových produktů nejen od společnosti Cisco. Pomocí CLI lze dosáhnout plného nastavení směrovače přes konzolový vstup. Pro přístup lze využít i grafické rozhraní nástroje SDM (Security Device Manager), který využívá webového přístupu. Pomocí prostředí SDM je možné zobrazovat i aktuální hodnoty v grafech.

Obr. 5.5: Směrovač Cisco 1800 série

Použité modely Cisco 1811 a 1812W v experimentální síti pracují s IOS verzí 12.4. Tyto směrovače podporují řadu protokolů či mechanizmů pro optimální nastavení sítě včetně zabezpečení a podpory různých rozhraní. Směrovače disponují dvěma FastEthernetovými (100Mb/s) rozhraními a jedním integrovaným osmi-portovým přepínačem, jak je vidět na Obr. 5.6. Model 1811 má navíc podporu ISDN rozhraní oproti 1812W modelu, který má navíc zabudovaný přístupový bod technologie WLAN dle IEEE 802.11b/g.

Obr. 5.6: Směrovač Cisco 1811

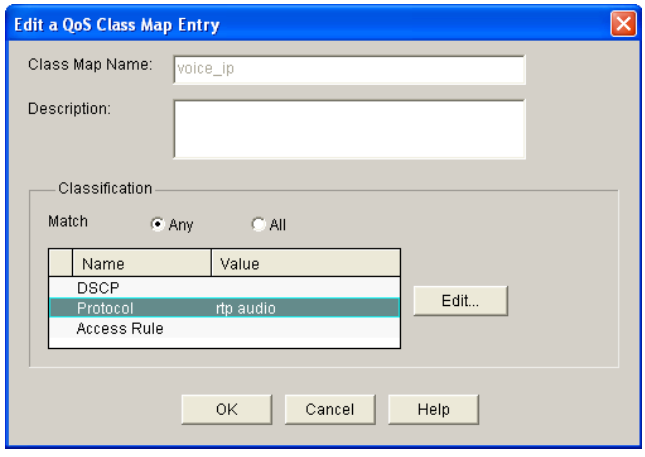
Použité směrovače mají podporu kvalitativních požadavků služeb. Pro správnou funkčnost jsou v Cisco směrovačích zavedeny mapy tříd a mapy politik [7]. K nastavení QoS je zapotřebí provést následující kroky:

- klasifikovat provoz do jednotlivých map tříd,
- uplatnit mapy tříd v mapách politik,
- přiřadit mapu politik k fyzickému rozhraní.

Jako příklad lze uvést situaci, kdy jsou realizovány současně služby přenosu souborů a přenos hlasu. Služba přenosu hlasu (VoIP) je nejdříve na základě mapy tříd klasifikována podle použitého protokolu RTP audio a přidělena do třídy „přenos hlasu“ (voice ip). Podobně jsou i pakety přenosu souborů klasifikovány a přiřazeny do třídy přenosu souborů (FTP). Mapa politik definuje zacházení s jednotlivými mapami třídy navzájem. V případě přenosu hlasu mapa tříd definuje, že třída voice ip bude upřednostněna před třídou přenos souborů FTP. Každému nastavitelnému fyzickému rozhraní je možné přiřadit politiku v příchozím i odchozím směru.

Klasifikace v směrovači

Klasifikace paketu v směrovači Cisco 1811 do mapy třídy QoS (QoS Class Map) je možné přiřadit na základě použitého protokolu, DSCP hodnoty nebo dle přístupového pravidla (Access list). Příklad nastavení klasifikace hlasové služby je na Obr. 5.7, kde hlasové pakety jsou klasifikovány podle protokolu RTP audio.



Obr. 5.7: Příklad klasifikace hlasových paketů

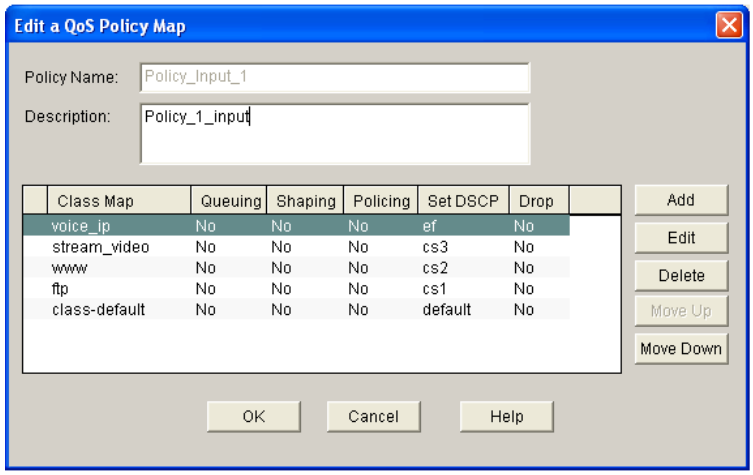
Uplatnění map tříd

Jednotlivé třídy map je možné vložit do konkrétní mapy politiky, kde se definují možnosti jak s pakety bude zacházeno. Nabízející možnosti směrovače Cisco 1811 jsou obsluha prioritní frontou, shaping, policing, značkování nebo přímé zahození. Jelikož vstupní fronty oproti výstupním frontám směrovače nepodporují řazení do front a shaping (viz Tab. 5.1), je třeba vytvářet samostatně vstupní politiku a výstupní politiku. V Diffserv doméně je vhodné definovat vstupní politiku map na vstupním rozhraní hraničního směrovače domény a výstupní politiku map aplikovat na rozhraní mezi směrovači uvnitř domény. Politika ve směru opouštějící doménu není pro chod domény důležitá a závisí na domluvě s protější stranou (např. jinou Diffserv doménou či koncovým uživatelem).

Tab. 5.1: Srovnání možností vstupní a výstupní fronty v směrovači

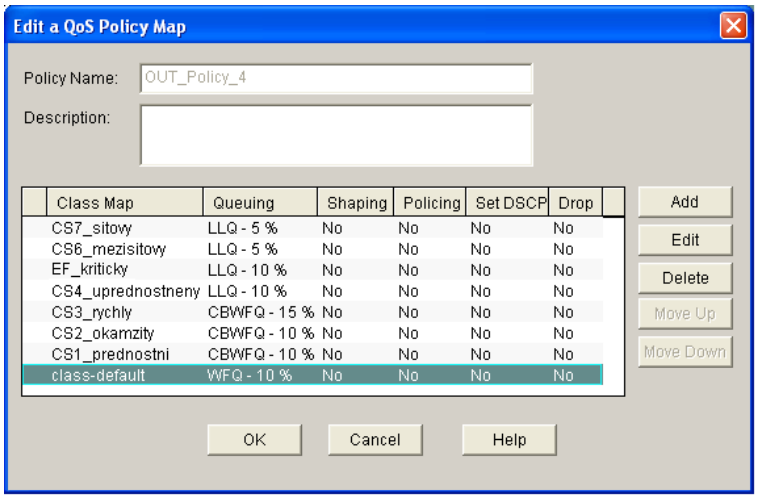
	Vstupní fronta	**Výstupní fronta**
Řazení do front	Ne	Ano
Shaping	Ne	Ano
Policing	Ano	Ano
Značkování	Ano	Ano
Zahození	Ano	Ano

Vstupní politika map obsahuje nejčastěji pouze parametry definující značkování paketů. V politice map je uveden seznam dostupných tříd a jejich zacházení s nimi. Na Obr. 5.8 je patrné, že směrovač bude pakety v třídě přenosu hlasu (voice_ip) značkovat podle DSCP v hlavičce paketu hodnotou EF. Ostatní možnosti zacházení jako řazení do front či policing nejsou definovány, protože se jedná o vstupní politiku map.



Obr. 5.8: Příklad konfigurace vstupní politiky map

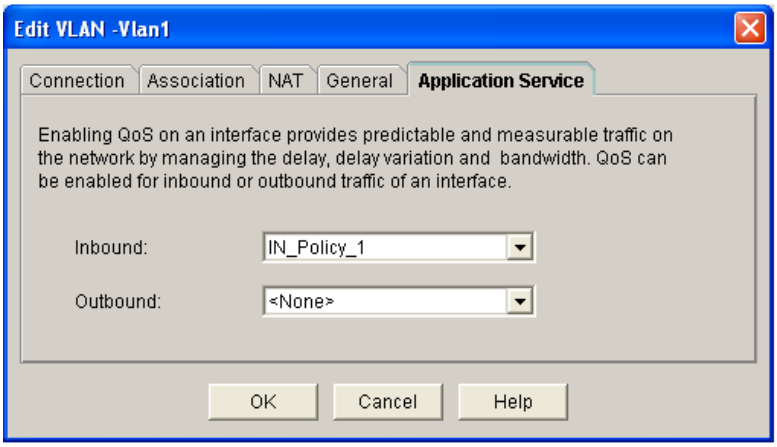
Výstupní politika map se aplikuje mezi směrovači uvnitř Diffserv domény k zaručení kvalitativních parametru QoS. Není žádoucí, aby výstupní politika map klasifikovala provoz podle použitého protokolu, jako to činila vstupní politika map. Již se předpokládá, že všechny pakety přeposílané uvnitř domény jsou správně označeny prioritní značkou v hlavičce IP paketu. V praxi to znamená mít také vytvořené mapy tříd, kde jsou pakety filtrovány pouze podle hodnot DSCP. Příklad nastavení výstupní politiky map je zobrazen na Obr. 5.9. Potřeba je neopomenout prioritní skupinu pro síťové a mezisíťové řízení sítě. V tomto příkladu jsou jednotlivé datové služby obsluhovány různými mechanizmy (LLQ, CBWFQ a WFQ).



Obr. 5.9: Příklad konfigurace výstupní politiky map

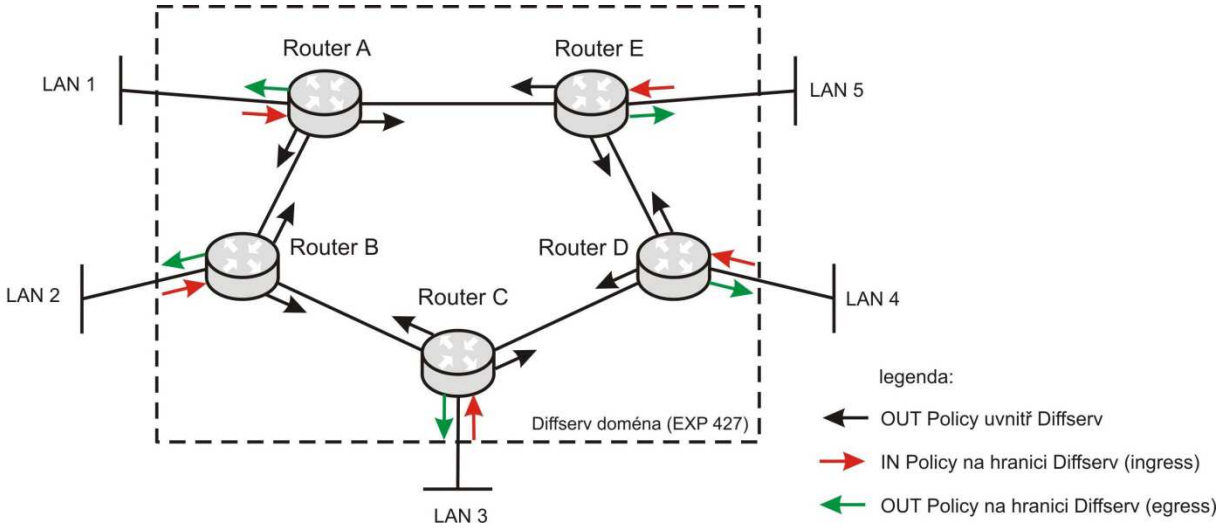
Přiřazení politiky map k rozhraní

Vytvořenou mapu politiky je třeba aplikovat na vstupní nebo výstupní frontu fyzického rozhraní. Vstupní fronta má omezené možnosti oproti výstupní frontě, která podporuje veškeré zacházení, kterým směrovač disponuje v politice QoS. Předdefinované politiky je možné manuálně přepínat, ale aplikovaná může být pouze jedna mapa politik jak pro příchozí tak pro odchozí směr, viz Obr. 5.10.



Obr. 5.10: Příklad přiřazení mapy politik k fyzickému rozhraní

Během vytváření politik map v směrovači se setkáváme s více politikami lišících se v nastavení, pro který směr jsou určeny. Druhým kritériem pro vytváření politiky je umístění směrovače zdali se jedná o hraniční směrovač či směrovač uvnitř Diffserv domény. V případě hraničního směrovače je důležité zabývat se hlavně klasifikací a značkováním příchozího provozu, a proto je na fyzický port připojený k okolní síť aplikována právě vstupní politika, která řeší převážně značkování paketů. Rozdílem jsou porty směrovače propojující síť uvnitř Diffserv domény, kde se aplikuje pouze výstupní politika, která je zaměřena na prioritní obsluhu. V některých případech mohou mít zákazníci domluveny individuální zacházení s pakety směrem k jejich síti. V takových případech je vhodné použít na hranici Diffserv výstupní politiku směrem k zákazníkovi. Výše zmíněné politiky a jejich směry přiřazení k portům směrovačů v Diffserv doméně jsou zobrazeny na Obr. 5.11.



Obr. 5.11: Využití vstupních a výstupních politik v Diffserv doméně.

Rozdíl mezi nastavením vstupní a výstupní politiky je v odkazech na různé mapy tříd. V případě vstupních politik je třeba se odkazovat na mapu třídy klasifikující provoz na základě použitých aplikačních protokolů. Výstupní politika je tvořena mapami tříd, které se klasifikují na základě DSCP značek, které odpovídají síťové vrstvě.

5.2.2 Přepínače

Přepínače jsou především síťová zařízení pracující na linkové vrstvě. Jejich úkolem je přepínat příchozí rámce na odpovídající výstupní port zařízení. Přepínací tabulka, obsahující pouze MAC adresy vázané na port zařízení, je automaticky doplňována a není potřeba po připojení žádný konfigurační zásah správce sítě. V případě levnějších přepínačů jsou už zařízení předem naprogramovaná z výroby, a není možné je jakkoli dále nastavovat.

V případě nastavitelných přepínačů je možné přepínače rozdělit na dvě základní kategorie:

- L2 přepínače a
- L3 přepínače.

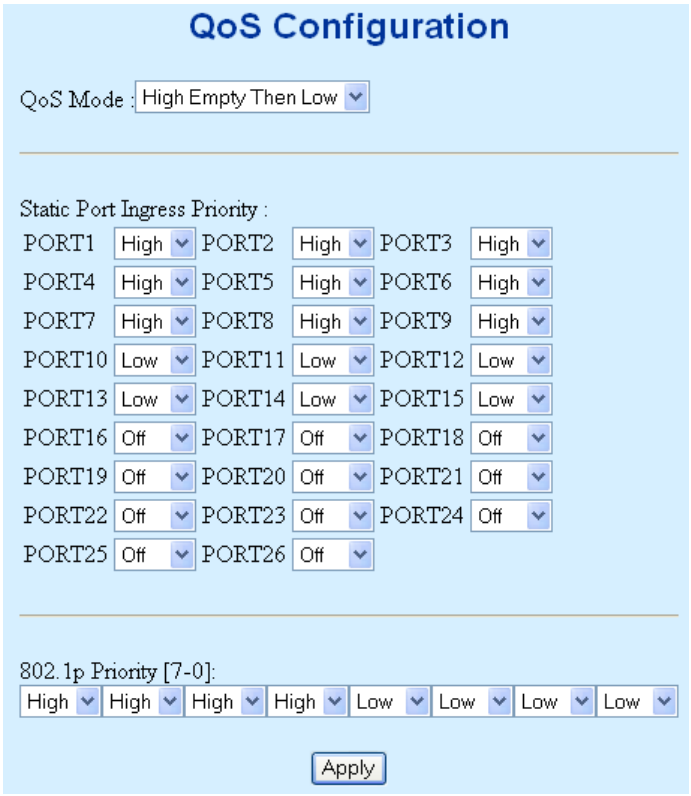
L2 přepínače

Označení L2 říká, že nejvyšší úroveň, na které je přepínač schopen pracovat, je linková vrstva. Tyto přepínače jsou vybaveny rozšiřujícími funkcemi na linkové vrstvě, jako podpora agregace portů, podpora VLAN, vytváření a správy záložních spojů, a tedy správce sítě může provádět některá dostupná nastavení věnující se pouze možnostem linkové vrstvy.

Z pohledu kvality služeb tyto přepínače umožňují prioritní obsluhu fronty podle parametru CoS (Class of Service) v rozšíření hlavičky rámce dle standardu IEEE 802.1p/Q. Využívají k zpracování rámců více obslužných front (maximálně osm) s prioritním přístupem. Na Obr. 5.12 jsou znázorněny L2 přepínače použité v experimentální síti, jejichž nastavení QoS je velmi podobné.

Obr. 5.12: L2 přepínače zapojené v experimentální síti.
(Planet FGSW 2620, Alied Telesyn 8326GB)

Jako příklad nastavení QoS jsou vybrány možnosti nabízené přepínačem od společnosti Planet, viz Obr. 5.13. Přepínač vlastní dvě fronty (High a Low), do kterých mohou být rámce přiřazeny na základě hodnoty CoS (802.1p Priority) nebo podle zapojeného fyzického rozhraní v přepínači.



Obr. 5.13: Nastavení QoS v L2 přepínači Planet FGSW 2620

L3 přepínače

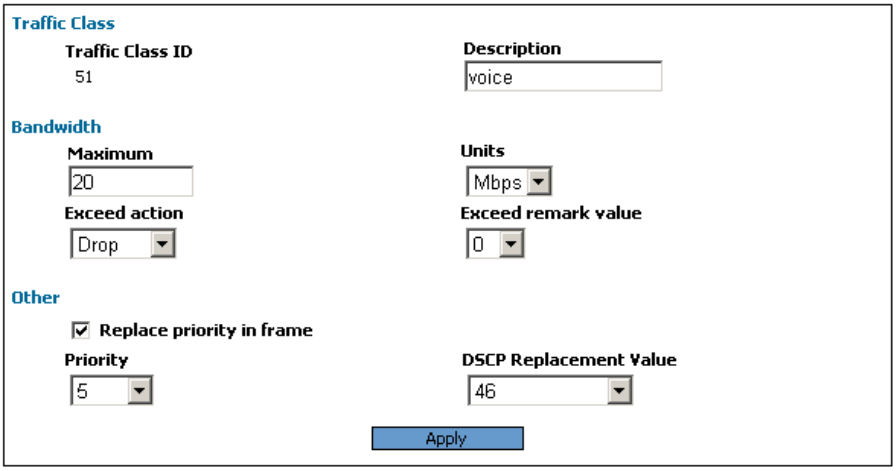
Přepínače s označením L3 dokáží pracovat na úrovni síťové vrstvy, tedy s pakety. Původní L3 přepínače byly velmi rychlé a jednoduché. Typicky měly jen velmi omezenou podporu směrovacích protokolů a veškerých pokročilých funkcí. Postupem času se jejich schopnosti rozšiřovaly a v současnosti se pojem L3 přepínač používá víceméně jako synonymum pro směrovač.

Přepínače dokáží přečíst hodnotu DSCP v hlavičce paketu. Výhodou z pohledu kvality služeb je, že většina L3 přepínačů podporuje přeznačení priority mezi síťovou a linkovou vrstvou (IEEE 802.1p). Zařízení disponují různým počtem výstupních front, přičemž oproti L2 přepínačům při rozhodování o upřednostnění berou ohled i na hodnotu DSCP v hlavičce paketu. Použité přepínače v experimentální síti jsou zobrazeny na Obr. 5.14.

Obr. 5.14: L3 přepínače použité v experimentální síti.
(HP ProCurve 2626, AT-2624t-2m, Linksys SRW2008P)

Příklad nastavení QoS na L3 přepínači Allied Telesyn je zobrazen na Obr. 5.15. Předem klasifikovaný provoz s označením „voice“ je možné přeznačit, jak na úrovni síťové (DSCP), tak i na úrovni linkové vrstvy (CoS). Tento model dále nabízí možnost přiřadit datové službě maximální

přenosovou rychlost a definuje, jestli při překročení hodnoty budou pakety zahazovány nebo přeřazeny do jiné prioritní skupiny.

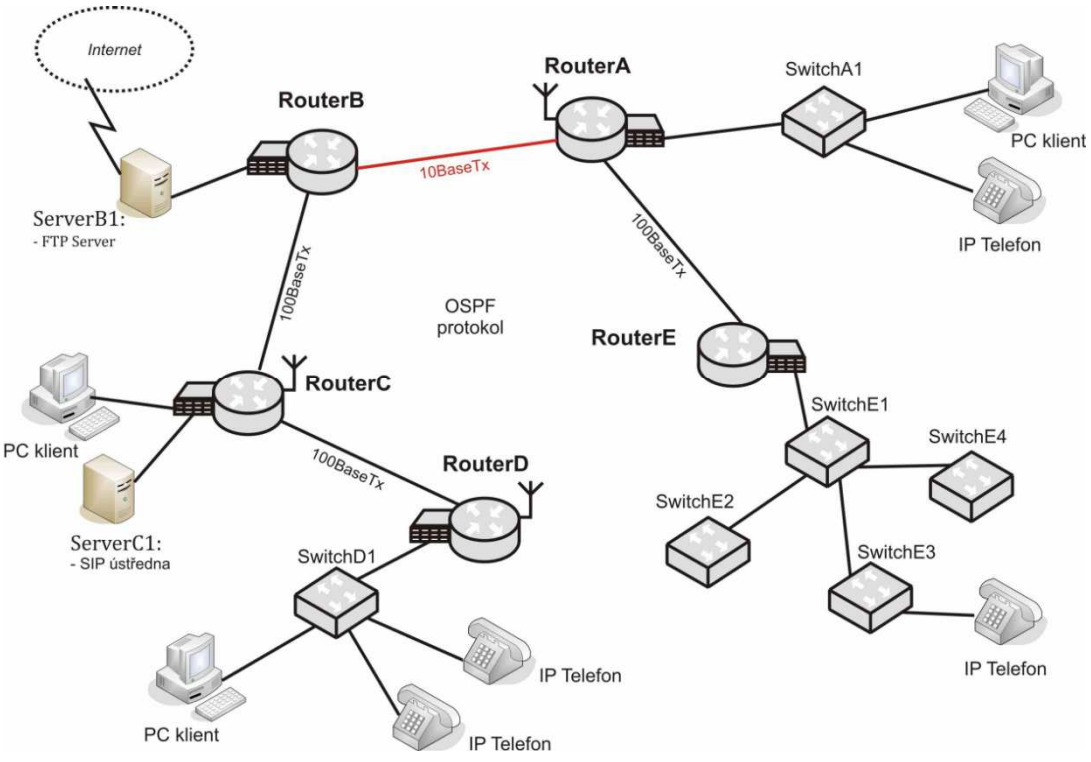


Obr. 5.15: Zacházení s pakety v L3 přepínači Allied Telesyn 2624t-2m

5.3 SIMULACE ZAHLCENÍ SPOJE BEZ POUŽITÍ QOS

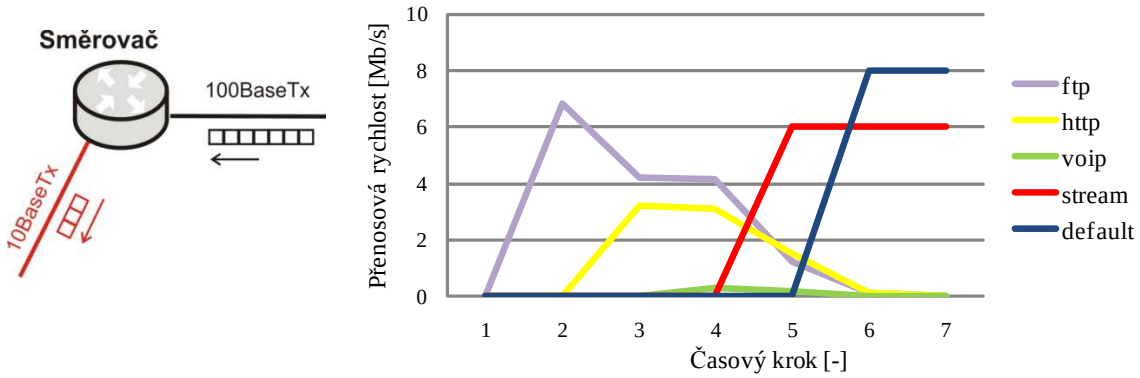
V páteřních sítích se mnohdy stává, že dojde k zahlcení spoje datovým tokem a síťový prvek musí začít zahazovat datové rámce, které není schopen obsloužit. Jaké příznaky mohou vzniknout v případě zahlcení spoje na datové služby, jsou náplní této kapitoly.

Pro vytvoření slabého místa, kde by mohlo dojít k přetížení spoje v experimentální síti, byla přenosová rychlost spoje mezi směrovačem A a B nastavena na přenosovou rychlost 10 Mb/s. Ostatní přenosové spoje v síti mají rychlost 100 Mb/s. Nově vzniklá topologie s vyznačenými rychlostmi spojů je zobrazena na Obr. 5.16.



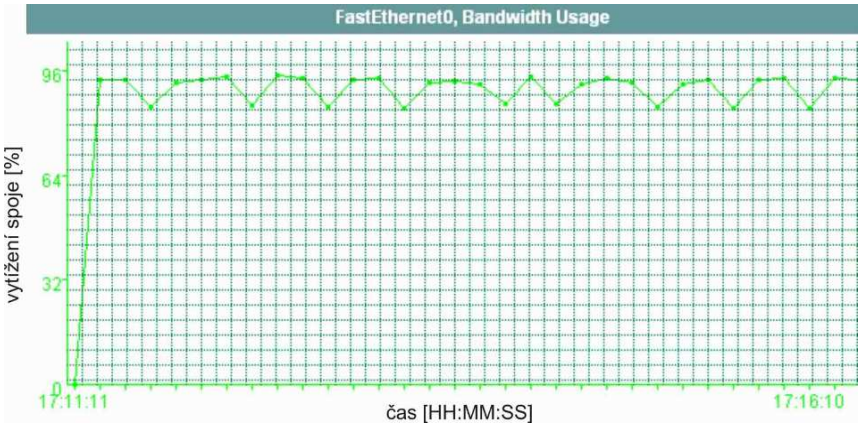
Obr. 5.16: Topologie experimentální sítě pro testování simulace přetížení spoje mezi směrovači.

Byly realizovány různé datové služby (VoIP, HTTP, FTP, video) s odlišnými požadavky na přenosové pásmo. Byla snaha přesáhnout nejvyšší možnou přenosovou rychlost pomalého 10 Mb/s rozhraní mezi směrovači a sledovat reakci jednotlivých služeb. Podpora QoS na směrovačích nebyla nastavena. Datové služby FTP a HTTP jsou provozovány nad protokolem TCP, který řídí datový tok podle stavu cesty mezi serverem a klientem, a proto byly při simulaci spuštěny nejdříve. Přenosová rychlost při začátku stahování souboru byla 6,7 Mb/s. Jednotlivé po sobě jdoucí kroky simulace přetížení spoje jsou graficky naznačeny na Obr. 5.17. Po zahájení stahování dat pomocí HTTP protokolu došlo ke snížení rychlosti FTP stahování a spoj byl plně využit pouze FTP a HTTP daty. Vysoké vytížení vzniklo při zahájení video streamu o datovém toku 6 Mb/s, kdy propustnosti předešlých služeb poklesly právě z důvodu, že využívají TCP řízení.



Obr. 5.17: Datové toky vyžadující obsluhu směrovače při simulaci zahlcení spoje 10 Mb/s.

Obr. 5.17 zobrazuje nevyřízené požadavky pro obsluhu směrovače, množství paketů přicházejících po 100 Mb/s rychlostním spoji. V časovém kroku číslo 5 na Obr. 5.17 je spuštěn pro směrovač neznámý UDP datový tok simulující zahlcení spoje. Neznámý datový tok využívající šířku pásma 8 Mb/s značně přeplnil výstupní frontu směrovače se spojem o rychlosti pouze 10 Mb/s. Směrovač informoval o vytížení spoje mezi směrovačem A a B hodnotami cca 95 %. Zaznamenaný průběh vytížení spoje je zobrazen na Obr. 5.18.

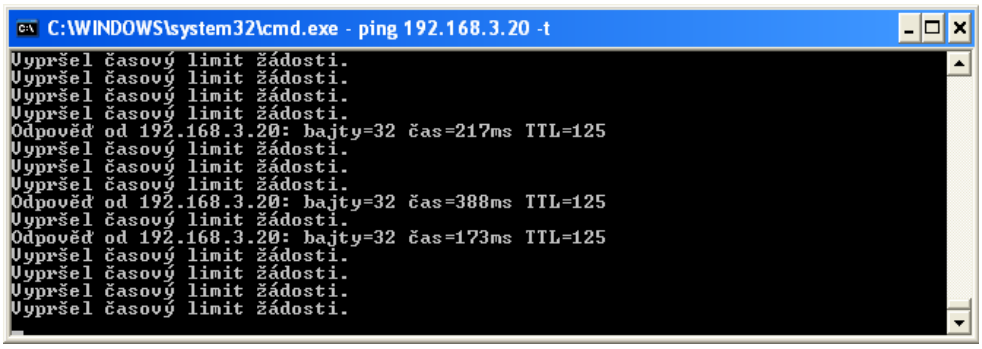


Obr. 5.18: Vytížení spoje mezi směrovači při simulaci zahlcení

Výsledky a dopady při zahlcení spoje

Směrovač musel začít zahazovat pakety, a protože nebyla zapnuta žádná podpora QoS, ztracené pakety měly značný vliv na předchozí spuštěné datové služby. Aplikace komunikující pomocí TCP protokolu (HTTP a FTP) začala rychle snižovat přenosovou rychlost, až došlo k přerušení spojení z důvodu nedosažitelnosti serveru. Opětovné spojení s datovým i webovým serverem nebylo možné

z důvodu nedostupnosti. Byla změřena konektivita a doba odezvy mezi stanicemi komunikujícími přes zahlcený spoj pomocí příkazu ping. Průběh příkazu ping je zobrazen na Obr. 5.19. Odezva dosahovala průměrně 300ms se ztrátovostí až 80%. Tyto parametry ukazují na nemožnost navázat nové spojení.



Obr. 5.19: Měření konektivity stanic přes zahlcený spoj příkazem ping

Negativní dopady byly znatelné na službě VoIP. Přenos hlasu začal být silně trhaný a s velkým časovým zpožděním. Po ukončení hovoru a opětovném požadavku na spojení přes úzké hrdlo v síti, byla komunikace po nezvykle dlouhé době (cca 10 vteřin) inicializována vyzváněním, ale následný přenášený hovor byl opět velmi nekvalitní, a tedy pro hlasovou službu zcela nevyhovující.

Vysoká ztrátovost během přenosu destruktivně poznamenala i přenos videa. Použitý kodek MPEG-2 s datovým tokem 6 Mb/s už nedokázal opravit zpožděné a ztracené pakety a výsledný obraz je zachycen na Obr. 5.20.

Obr. 5.20: Snímek přenášeného videa při zahlceném spoji

Z výše uvedených dopadů je patrné, že v případě vzniku úzkého hrdla v síti nebo nevyžádaného toku dat může docházet k zahlcení front v síťových prvcích a následně dochází k zahlcení a zahazování paketů preferovaných služeb.

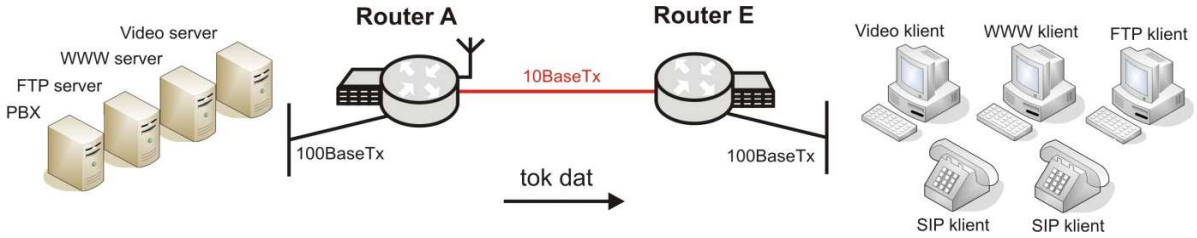
5.4 MĚŘENÍ CHOVÁNÍ PRIORITNÍCH ŘAZENÍ

Nasazením podpory kvalitativních požadavků služeb (QoS) dojde k prioritnímu přístupu síťových prvků k paketům či rámcům. Pomocí obsluhy výstupních front mohou být datové služby s vyšší prioritou upřednostněny a odbaveny s vyšší rychlostí. Dostupná šířka pásma může být rozdělena jednotlivým službám dle stanovených pravidel, a tím se zabrání nedostupnosti především u služeb, které jsou citlivé na zpoždění a ztrátovost.

Směrovače Cisco 1812 disponují dvěma hlavními mechanizmy pro obsluhu prioritních front:

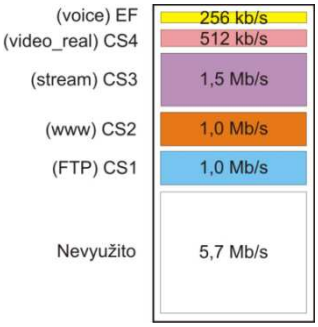
- LLQ a
- CBWFQ.

Měřením je snaha porovnat mechanizmy za použití shodných provozních podmínek a následně vytvořit kombinaci obou mechanizmů. Byla vytvořena parametrově shodná výstupní mapa politiky pouze s odlišným mechanizmem řazení. Měřený spoj byl především mezi směrovačem A a E, kterému byla nastavena přenosová kapacita na 10 Mb/s. Názorné schéma zapojení sítě je na Obr. 5.21.



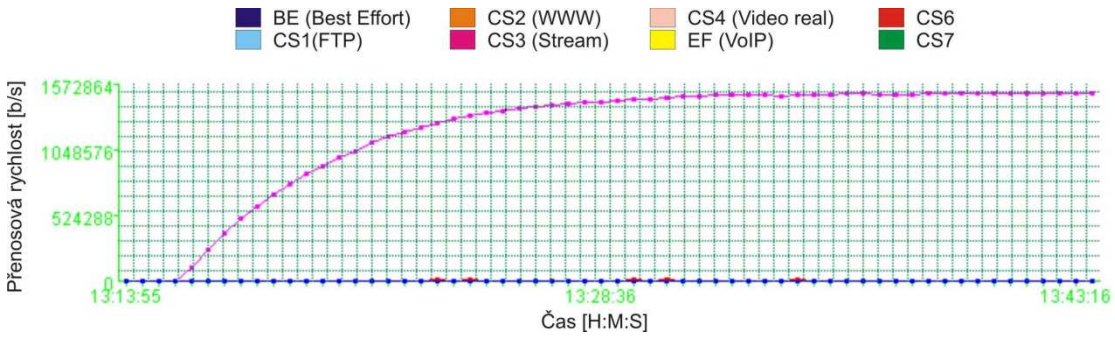
Obr. 5.21: Schéma zapojení sítě při měření prioritních front

Vždy při zahájení měření již byly spuštěny datové služby s malým vytížením spoje tak, aby směrovač nemusel řešit případné zahazování nadměrných paketů. Konkrétní hodnoty generovaných datových toků jsou zobrazeny na Obr. 5.22. Součet využití šířky pásma spoje činil cca 4 Mb/s. Zbývajících cca 6 Mb/s bylo nevyužito.



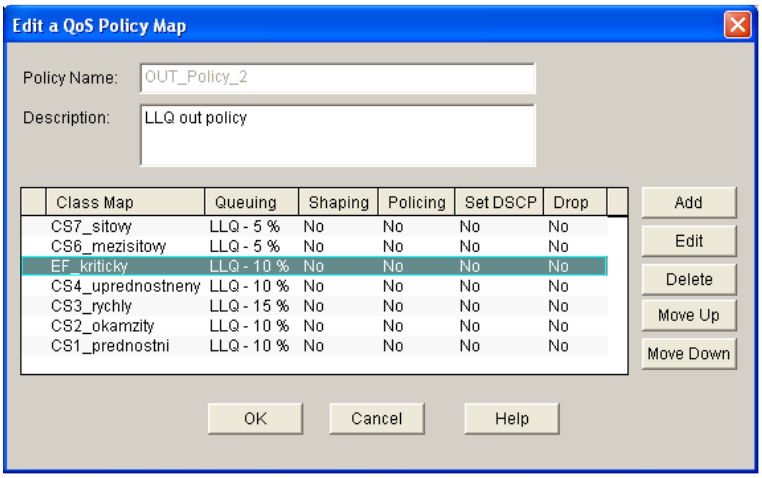
Obr. 5.22: Počáteční využití 10 Mb/s spoje při měření

V určitý okamžik bylo zahájeno stahování z FTP serveru a vytvořen datový tok označený značkou priority CS1. Dále pro případ zahlcení neznámým provozem byl generován datový tok až 8 Mb/s, který byl značen jako Best Effort. Šířky pásem pro služby vyčleněné v politice map byly téměř shodné s původním vytížením sítě. Průběhy jsou zaznamenány pomocí grafické podpory (SDM) v směrovači Cisco. Prostředí SDM měří hodnoty s velkou hysterezí, tudíž v případě zahájení vysílání danou rychlostí se zobrazené hodnoty křivky postupně přibližují s časovým odstupem (až 10min) k hodnotám skutečného přenosu. Obdobné zkreslení vzniká při okamžitém ukončení přenosu, křivka postupně klesá a zobrazené hodnoty neodpovídají skutečným. Příklad hystereze je na Obr. 5.23, kde byl spuštěn datový tok videa rychlostí 1,5 Mb/s. Křivka se ustálila na skutečné hodnotě cca po 15 minutách přenosu. V případě sledování jednotlivých služeb a ovlivňování mezi sebou není zkreslení znehodnocující měření.



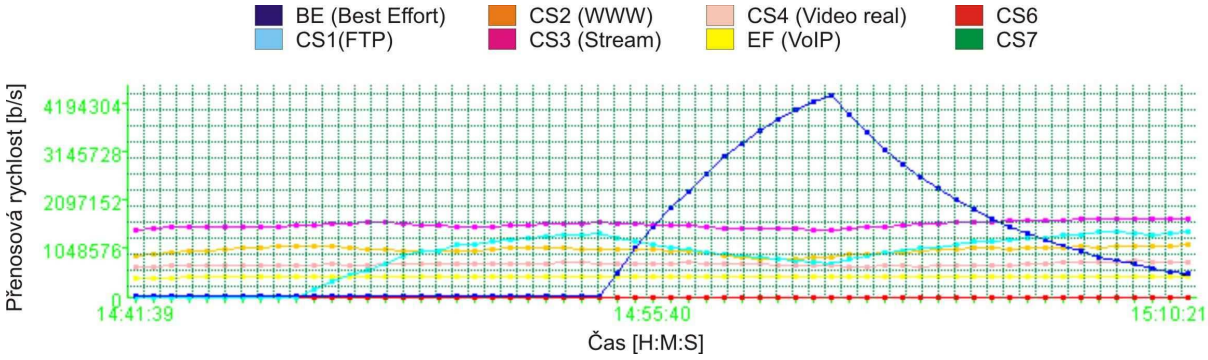
Obr. 5.23: Hystereze měření v prostředí SDM

Průběhy měření při obsluze pouze mechanizmem LLQ



Obr. 5.24: Nastavení výstupní politiky při měření fronty LLQ

Nastavení prioritního zacházení pomocí mechanizmu LLQ bylo definováno ve výstupní politice map na směrovači A. Konkrétní nastavené hodnoty jsou zobrazeny na Obr. 5.24. Všechny generované služby měly v politice nadefinovanou minimální přenosovou rychlost v procentuálním vyjádření k šířce pásma spoje. Operační systém IOS na směrovačích Cisco požaduje ponechat minimálně 25% pro nedefinované služby v politice. V našem případě bylo pro ostatní služby ponecháno 35% mimo pravidel politiky. Je třeba mít na mysli, že aktuálně nevyužité rezervované pásmo mohou využít ostatní služby v politice nebo nedefinované služby. Při měření nebylo využito veškeré rezervované pásmo v politice map pro všechny třídy (např. CS6 a CS7), tudíž dostupné volné pásmo pro služby činilo až 57%, což odpovídá rychlosti 5,7 Mb/s.

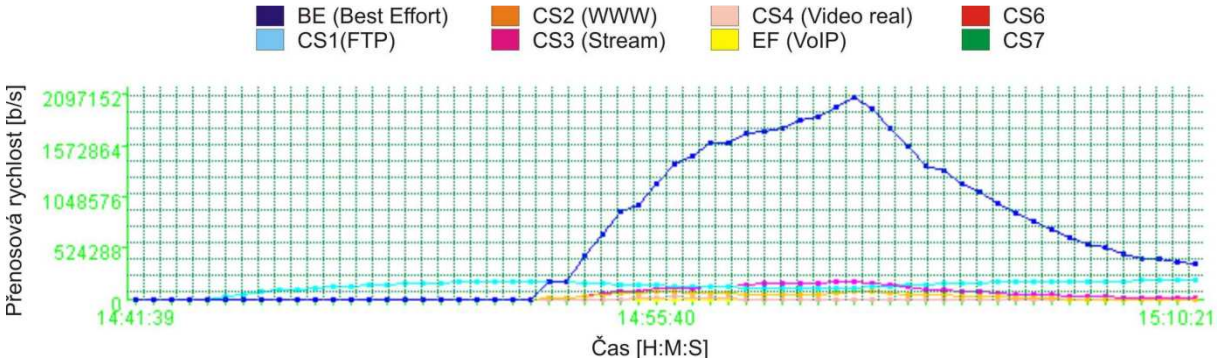


Obr. 5.25: Průběh obsloužených paketů frontou LLQ

Na Obr. 5.25 jsou zobrazeny průběhy obsloužených paketů z front, kde byl nastaven prioritní mechanizmus LLQ. Z průběhů je patrné, že po zahájení stahování dat z FTP serveru bylo paketům se značkou CS1 dovoleno mírně překročit hranici nastavenou v politice (1 Mb/s). Služba FTP nebyla nijak limitovaná kromě zmíněné politiky na směrovači A, a přesto ji směrovač nedovolil využít volné pásmo na daném spoji. Naměřená rychlost FTP spojení činila průměrně 1,7 Mb/s. Během obsluhy, pro směrovač neznámého provozu (8 Mb/s), byla rychlost paketů CS1 snížena. Hodnota snížené rychlosti byla dána nastavenou minimální rychlostí třídě CS1 v politice map.

Na Obr. 5.26 je výsledek měření zahozených paketů jednotlivých tříd služeb. V průběhu měření bylo nejdříve zaznamenáno zahazování třídy CS1, kterou tvořily převážně pakety se službou přenosu souborů. Služba FTP využívá protokol TCP, který si sám reguluje přenosovou rychlost podle úspěšně doručených datagramů. Zahazováním paketů třídy CS1 bylo způsobeno regulováním rychlosti, kterou mechanizmus LLQ povolil paketům využít. Dále je patrné zahazování paketů z třídy Best Effort.

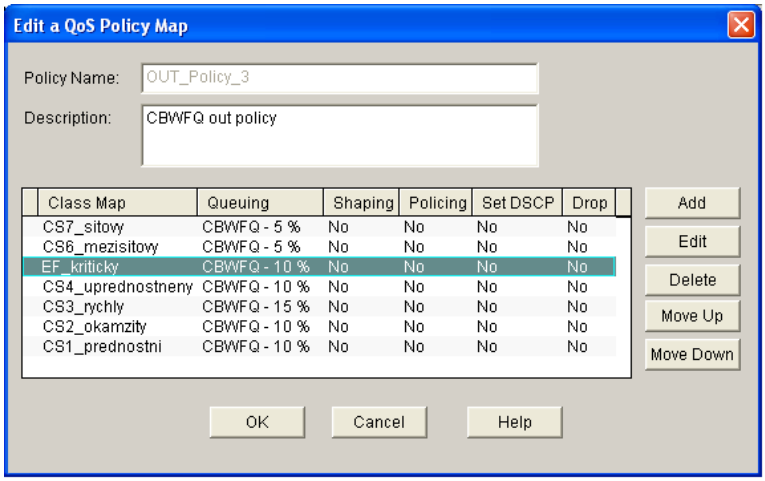
Kapacita spoje nestačila pojmout všechny požadavky a směrovač začal zahazovat. Zahazovány byly převážně pakety BE, které překročily volnou šířku pásma. Důležité je také si všimnout, že zahazovány začaly být i pakety ostatních tříd. To mělo za následek malé nedostatky v chodu ostatních datových služeb. Především na přenášených video-přenosech začaly vznikat artefakty. Služba VoIP a použitý rekonstrukční kodér drobné výpadky odstranil a pro lidské vnímání se jevil přenos bez problémů.



Obr. 5.26: Průběh zahozených paketů ve frontě LLQ

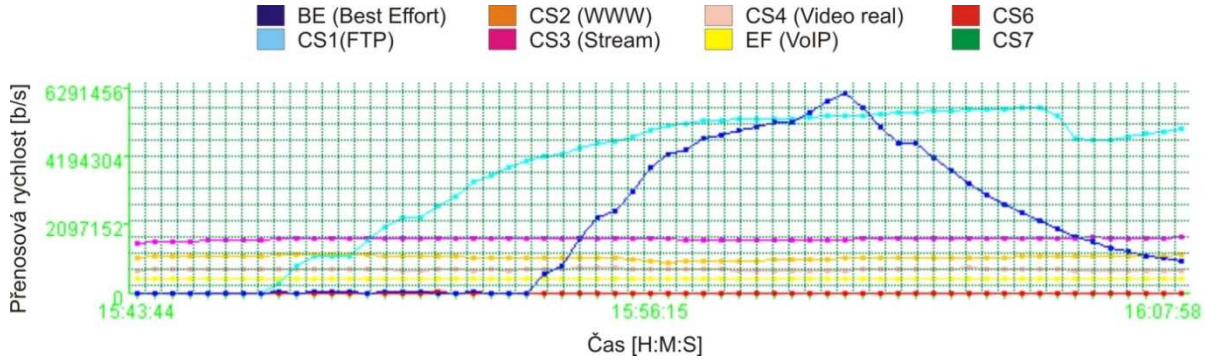
Při použití obsluhy třídy mechanizmem LLQ je třeba brát v potaz jeho ohleduplnost ke všem ostatním službám. V případě třídy CS1 (FTP) měla třída definovanou minimální rychlost 1 Mb/s, přestože bylo dostupné volné pásmo spoje, mechanizmus jej nedovolil zcela využít. Naopak služba BE, která nebyla definována v politice map, mohla využít volný prostor. Třída BE měla za následek malé zahazování v ostatních třídách. Při použití pouze mechanizmu LLQ je potřeba počítat, že pokud dojde k zahlcení celé kapacity spoje, začne mírně zahazovat z fronty. Chování LLQ zaručuje nevyhladovění třídy s nízkou prioritou.

Průběhy měření při obsluze pouze mechanizmem CBWFQ



Obr. 5.27: Nastavení výstupní politiky při měření fronty LLQ

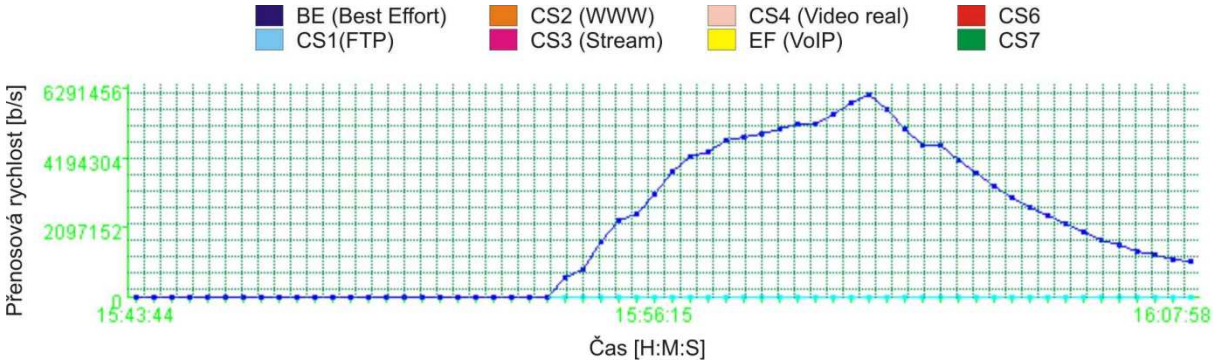
Mechanizmus CBWFQ využívá také ke garantování rychlosti procentuální vyjádření šířky pásma. Nastavení výstupní politiky směrovače je zobrazeno na Obr. 5.27. V politice bylo uplatněno pouze prioritní řazení. Stejně jako při měření LLQ byl zpočátku generován datový provoz, který nevyužil celou šířku pásma spoje mezi směrovači. Schéma zapojení sítě bylo shodné s Obr. 5.21.



Obr. 5.28: Průběh požadavků k obsluze při měření mechanizmu CBWFQ

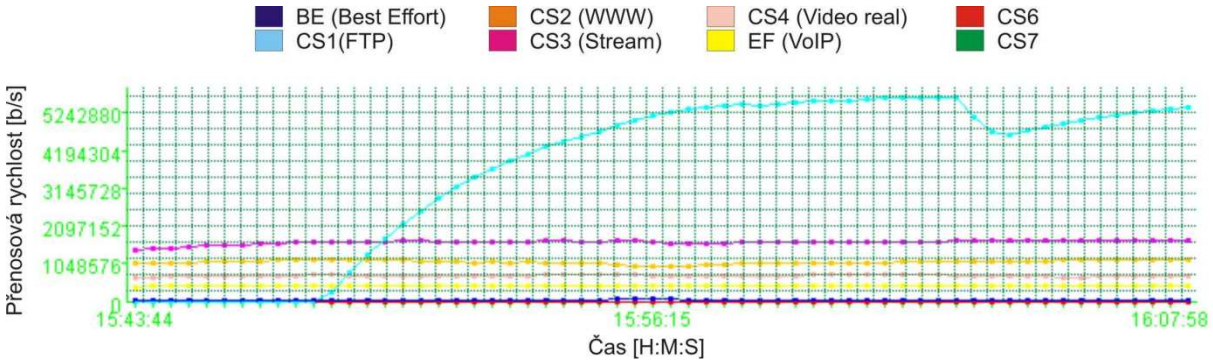
Na Obr. 5.28 jsou zobrazeny požadavky jednotlivých tříd, jejichž pakety vstupovaly do směrovače A a směrovač měl na starosti obsloužit jednotlivé pakety za pomoci mechanizmu CBWFQ. Jsou to datové toky na vstupu směrovače. V první fázi bylo navázáno FTP spojení a směrovač umožnil využít veškeré volné pásmo právě přenosu řízeno TCP protokolem. Naměřená rychlost FTP spojení byla 5,2 Mb/s. V druhé fázi byl generován pro směrovač neznámý datový tok (8 Mb/s), který tvořily UDP datagramy. Jelikož UDP nemá zpětné řízení rychlosti, směrovač byl nucen sám řešit snížení rychlosti – zahazováním. Celková rychlost požadavků činila cca 16 Mb/s.

Pakety, které byly zahazovány, jsou zobrazeny na Obr. 5.29. Z průběhu měření je patrné, že směrovač začal zahazovat téměř všechny pakety z třídy Best Effort. Ostatní třídy nepocítily žádnou ztrátovost. Přenosy jednotlivých služeb nezaznamenaly žádné výpadky či zhoršení kvality přenosu.



Obr. 5.29: Průběh zahozených paketů při obsluze pouze mechanizmem CBWFQ

Pokud odečteme ztracené pakety od vstupních požadavků z předešlého průběhu, dostaneme průběh, který znázorňuje jednotlivé třídy paketů přenesených na spoji mezi směrovači A a E, viz Obr. 5.30.



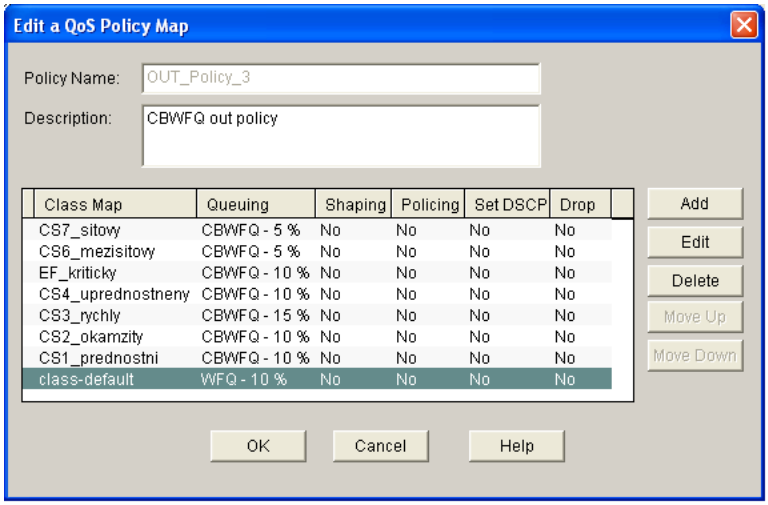
Obr. 5.30: Průběh přenesených paketů mezi směrovači při obsluze pouze CBWFQ

Jednotlivé datové třídy měly plně dostupnou nastavenou rychlost v politice map. Zahazování se jich nedotklo. Mechanizmus se choval tak, že přenos s vyšší prioritou byl ponechán využívat volné pásmo na úkor provozu s nedefinovanou prioritou (BE). Pakety FTP spojení mohly využívat celou volnou šířku pásma i přesto, že přicházely požadavky paketů s nižší prioritou.

Mechanizmus CBWFQ plně garantuje šířku pásma definovanou v politice. Provozy, které nejsou definovány v politice map, budou první, koho mechanizmus zahodí. Při použití pouze mechanizmu CBWFQ je třeba počítat, že datový provoz nedefinovaný v politice může být zcela vyhladověn. Třídy definované v politice mají zaručenou minimální přenosovou kapacitu spoje.

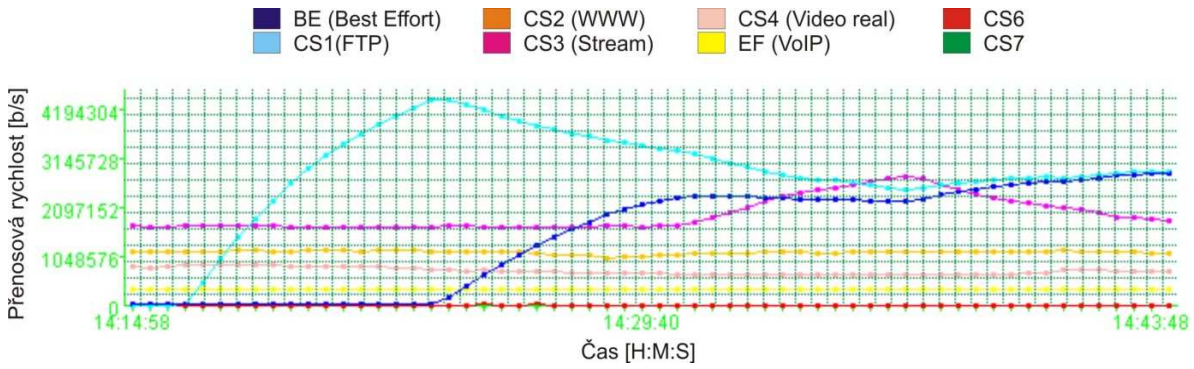
Průběhy měření při obsluze mechanizmem CBWFQ a třídou class-default

Zmíněný problém s vyhladověním nedefinovaného provozu mechanizmem CBWFQ je možné řešit přidáním do politiky třídu s názvem class-default, která zastupuje neznámý provoz. Upravené nastavení politiky map je na Obr. 5.31. Směrovač Cisco 1811 umí prioritně obsloužit třídu class-default pouze mechanizmem WFQ (Weighted Fair Queuing) [12]. Pro korektní nastavení je třeba určit, kolik šířky pásma bude pro tento provoz rezervováno. Při měření bylo nastaveno 10% pro třídu class-default.

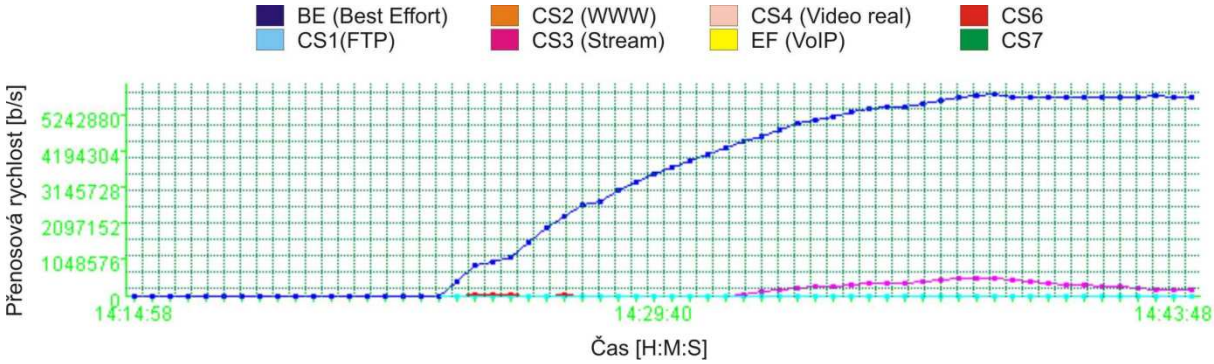


Obr. 5.31: Nastavení výstupní politiky při měření CBWFQ s třídou class-default

V rámci jednotlivých kroků měření bylo nejdříve spuštěno stahování dat. Dále generován neznámý datový tok s přenosovou rychlostí 8 Mb/s. V poslední fázi byl zvýšen video-stream na hodnotu 3,5 Mb/s. Časové průběhy přenesených paketů mezi směrovači A a E jsou zobrazeny na Obr. 5.32. Průběhy zahazování paketů ve směrovači A při přetížení spoje je zobrazen na Obr. 5.33.



Obr. 5.32: Průběh přenesených paketů při obsluze CBWFQ a třídy class-default



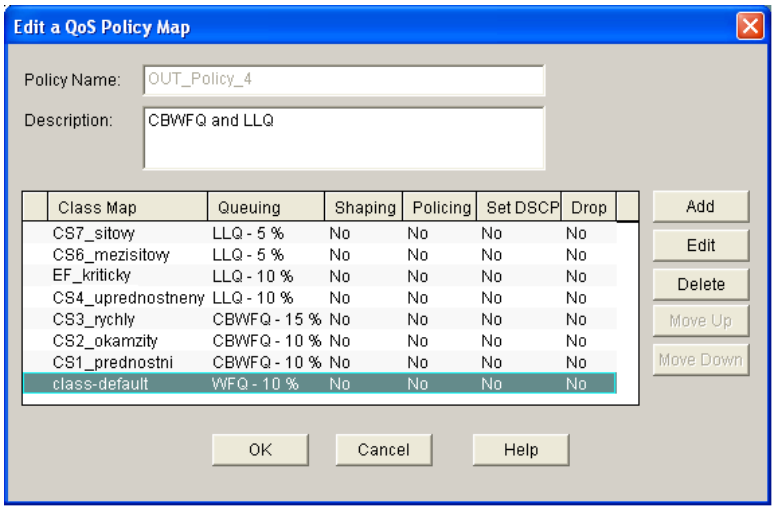
Obr. 5.33 : Průběh zahozených paketů při obsluze CBWFQ s třídou class-default

Z průběhů je patrné, že zahájená FTP komunikace dosahovala rychlosti až 5 Mb/s. Spoj mezi směrovači byl plně vytížen. Rozdíl oproti předchozímu měření vznikl při generování toku dat třídy BE. Byla snížena rychlost přenosu FTP na 2,8Mb/s. Rychlost třídy BE dosahovala rychlosti 2,5Mb/s. Převyšující datový tok BE byl směrovačem zahazován. Ostatní služby nebyly postihnuty zahazováním. V případě výrazného zvýšení toku dat v generátoru video-streamu na hodnotu 3,5 Mb/s, která přesahuje garantovanou hodnotu v politice o 2 Mb/s, začal mechanizmus malé množství paketů zahazovat (500kb/s). Video-stream je značkován s vyšší prioritou než FTP pakety či pakety BE. Všechny tři zmíněné třídy, které překročily svou minimální garantovanou hodnotu v politice (CS1, CS3 a BE), dosahovaly shodných rychlostí pouze s malými rozdíly dané značkou priority.

Problém s vyhladověním Best-Effort provozu při použití CBWFQ je možné řešit právě zavedením minimální rychlosti pro třídu class-default a zároveň použít obslužný mechanizmus např. WFQ.

Průběhy měření při obsluze mechanizmy CBWFQ a LLQ v jedné politice map

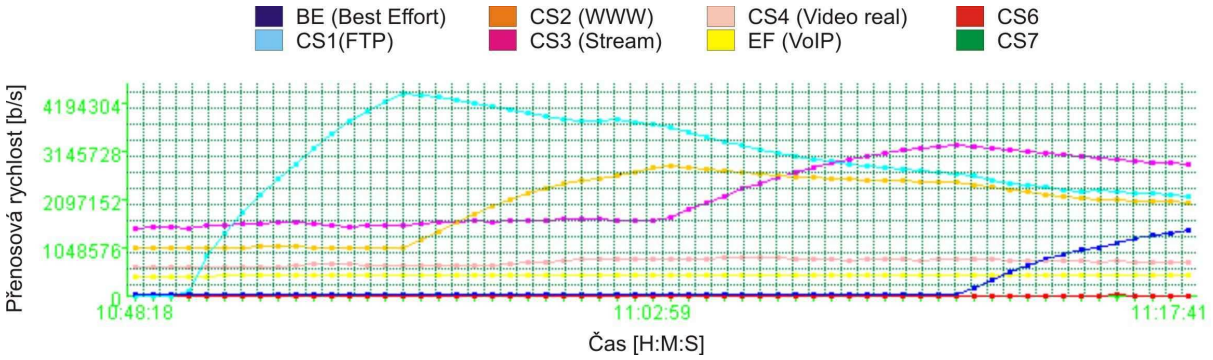
Při vytváření politiky map je možné zvolit jednotlivým třídám mechanizmus obsluhy. V jedné politice map je možné kombinovat různé prioritní mechanizmy. V případě směrovače Cisco 1811 lze vybírat pouze ze dvou mechanizmů pro vytvořené třídy. Pro obsluhu třídy class-default je možné zvolit pouze mechanizmus WFQ nebo FIFO. Příklad vytvořené politiky map je na Obr. 5.34.



Obr. 5.34: Výstupní politika map s použitím více mechanizmů obsluhy

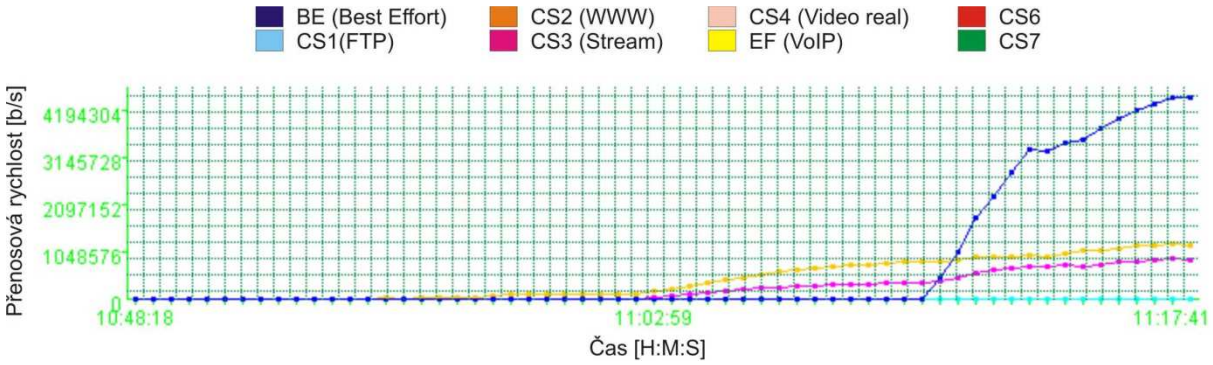
Mechanizmus LLQ se vyznačuje svými nízkými hodnotami zpoždění přenosu při obsluze a proto byl zvolen pro datové třídy citlivé na časové zpoždění. Zbývající třídy využívající větší šířku pásma byly obsluhovány mechanizmem CBWFQ a ostatní provoz (Best Effort) mechanizmem WFQ.

Průběhy obsloužených paketů jsou zobrazeny na Obr. 5.35. Měření bylo realizováno mezi směrovačem A a E na spoji 10 Mb/s.



Obr. 5.35: Průběh přenesených paketů mezi směrovači s různými mechanizmy obsluhy

V klidovém vytížení všech puštěných služeb nebylo zaznamenáno žádné zahazování či omezení. První změna přišla při zahájení stahování z FTP serveru. Pakety s FTP daty dosahovaly rychlosti 5,2 Mb/s. Druhým krokem měření bylo zvýšení toku třídy CS2 na celkové 3 Mb/s. Nastal pokles rychlosti CS1 na 4 Mb/s. V třetí fázi měření došlo ke zvýšení rychlosti toku dat na 3,5 Mb/s třídě CS3. Reakce byla v poklesu třídy CS2 i třídy CS1. FTP server snížil rychlost odesílání na 2,5 Mb/s. V čtvrté poslední fázi měření byl generován pro směrovač neznámý provoz o rychlosti 8 Mb/s. Došlo k plnému zatížení spoje a jednotlivé rychlosti byly lehce sníženy. Snižování rychlosti docházelo pouze u tříd, které překročily minimální rychlost definovanou v politice map.



Obr. 5.36: Průběh zahozených paketů při obsluze kombinací mechanizmů

Během celého měření nedošlo k žádnému zahození paketů z vyšších prioritních tříd. Zahazovány byly pouze třídy, které využívaly volné pásmo. Na Obr. 5.36 jsou zaznamenány zahozené pakety jednotlivých tříd. K prvnímu malému zahazování došlo v druhé fázi měření. Datový tok s pakety CS2 překročily hodnotu 1Mb/s a dělily se s FTP provozem. Číselně hodnotnější začalo být zahazování po třetím kroku měření. Zahazována byla třída CS2 rychlostí – až 1 Mb/s. V posledním kroku je znatelný nárůst zahozených paketů třídy Best-Effort, který měl za následek lehké zvýšení zahazování tříd CS2 a CS3.

V tomto nastavení politiky map byly služby v reálném čase obsluhovány mechanizmem LLQ. Služby méně náročné na časovou odezvu byly obsluhovány mechanizmem CBWFQ. Je zde vidět garance minimální rychlosti a zároveň větší zahazování provozu s nižší prioritou.

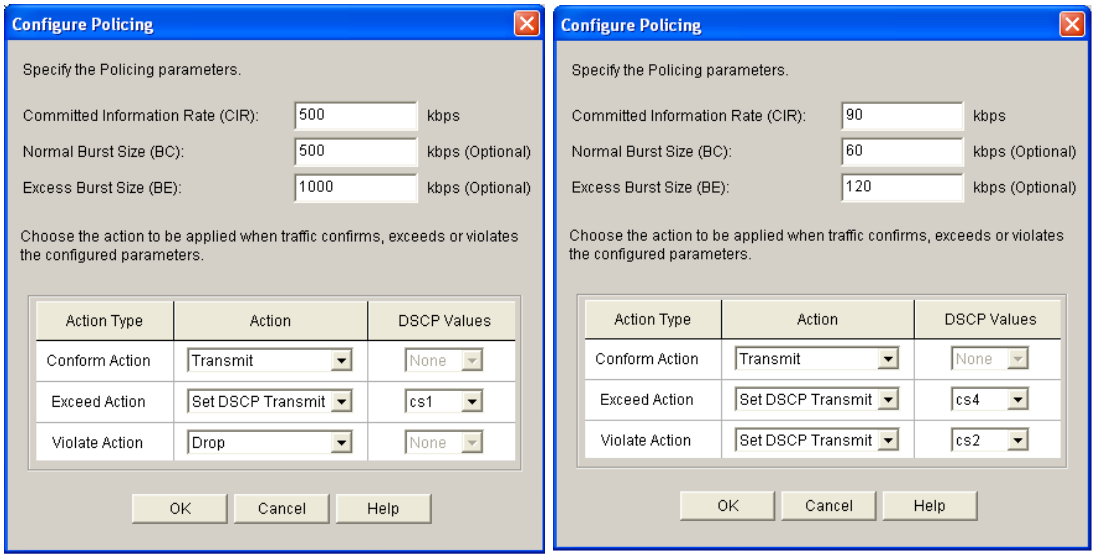
Shrnutí

Na základě provedených měření je vhodné kombinovat více mechanizmů obsluhy v jedné politice map. Mechanizmy typu LLQ přiřadit třídám provozu se striktní obsluhou, která se vyznačuje

nízkým zpožděním. Služby v reálném čase je vhodné přiřadit k mechanizmu LLQ. Zbývající třídy přiřadit k mechanizmu zaručující minimální přenosovou rychlost, například CBWFQ. Aby nedocházelo k vyhladovění nedefinovaného provozu v politice map, je třeba přidat tzv. výchozí třídu (Class-default) do politiky map, aby ostatní datové toky (Best Effort) měly vyčleněnou alespoň nějakou šířku pásma a nebyly vyhladověny při přetížení spoje.

5.5 OVĚŘENÍ NASTAVENÍ POLICINGU

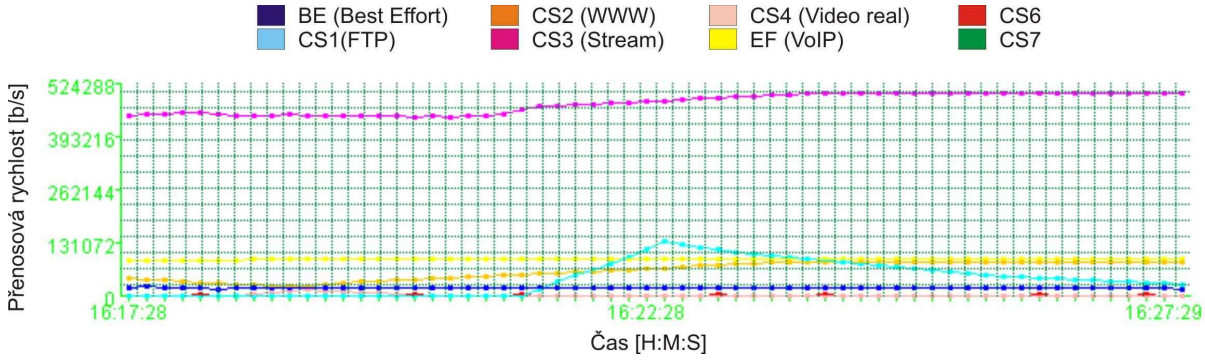
Policing slouží k omezení maximální rychlosti přenosu. Definujeme tím limitní hodnotu rychlosti, kterou je směrovač ochotný obsloužit pakety. V případě většího množství požadavků začne směrovač pakety zahazovat, případně využije princip obsluhy pomocí tokenů. Příklad nastavení policingu u datových tříd CS3 a EF jsou na Obr. 5.37.



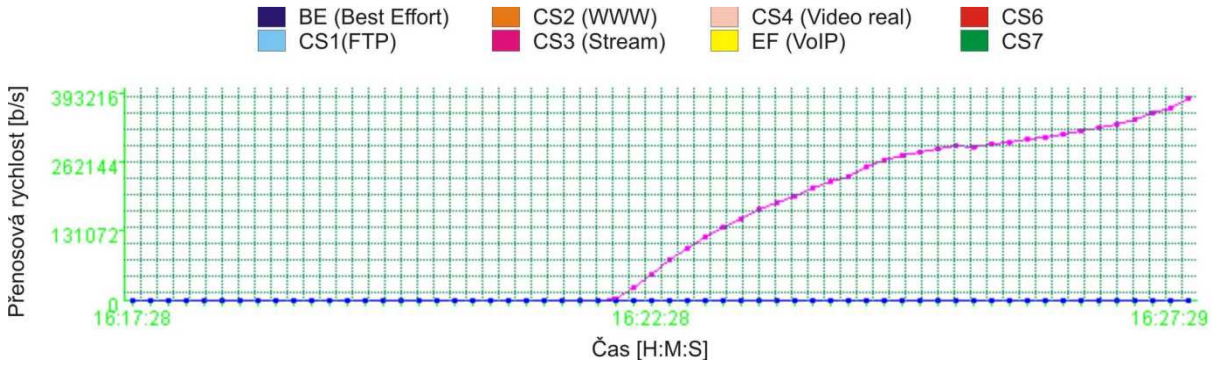
Obr. 5.37: Nastavení policingu pro třídu CS3 (vlevo) a EF (vpravo)

Při nastavení policingu je důležitá položka CIR, která stanovuje povolenou hranici maximální rychlosti. Další parametr BC definuje, o kolik je možné překročit rychlost CIR. Položka BE definuje velikost zásobníku tokenů pro nadměrný provoz, dle doporučení by měla dosahovat dvojnásobku hodnoty BC [17]. Další možnosti jsou volby zacházení s typem provozu. Pro zacházení bylo vyhrazeno 500 kb/s pro třídu CS3. Pakety převyšující 500 kb/s, tedy mezi 500 – 1000 kb/s byly přeznačeny do třídy CS1 do doby než byla vyprázdněna nádoba s tokeny. U nastavení třídy EF je rozdíl v zacházení. Pakety převyšující o 60 kb/s byly nejprve přeznačovány do třídy CS4 a po vyčerpání tokenů byly přeznačovány do třídy CS2. V případě EF nebylo nastaveno zahazování, pouze přeznačení.

Měření probíhalo tak, že nejprve byl generován provoz tak aby vyhovoval limitům policingu. Dále byl vždy zvýšen datový tok jedné třídy na cca dvojnásobek, což znamenalo překročení policingu a projevu zacházení s nadlimitním provozem. Průběh měření chování policingu je zaznamenán na Obr. 5.38. Na Obr. 5.39 jsou zobrazeny zahozené pakety při řízení rychlosti.



Obr. 5.38: Průběhy datových tříd při měření policingu

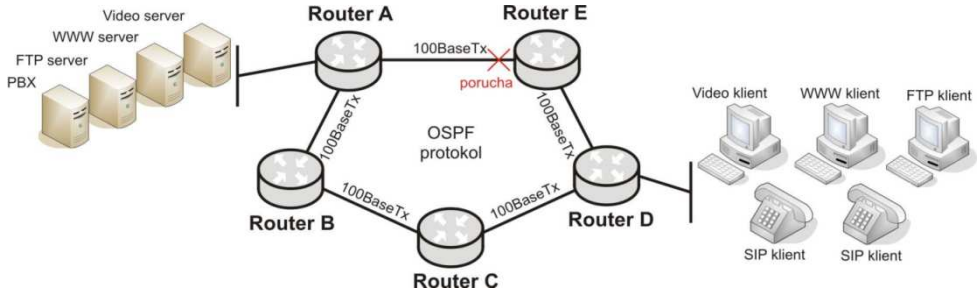


Obr. 5.39: Průběh zahozených tříd během policingu

Z výsledků měření je vidět, že nastavené hodnoty policingu byly dodrženy. Nastavená maximální hodnota CIR nebyla překročena. Nadlimitní pakety videostreamu byly zahozeny (Obr. 5.39). Využití třídy CS2 je způsobeno přeznačením nadlimitních paketů EF. Značný nárůst provozu třídy CS1 způsobil nadlimitní provoz CS3 dokud nedošlo k vyčerpání volných tokenů.

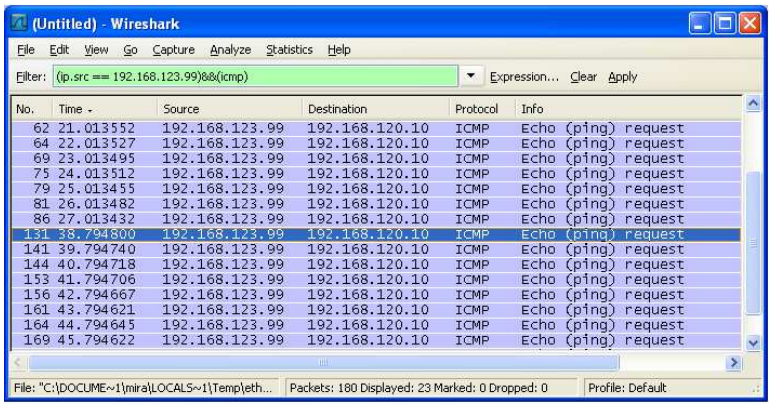
5.6 VLIV VÝPADKU SÍŤOVÉHO SPOJE NA PRŮBĚH SLUŽEB

Cílem této kapitoly a měření je realizovat výpadek spoje mezi směrovači v experimentální síti a vyhodnotit průběh jednotlivých typů služeb po výpadku. Vytvořená experimentální síť obsahuje redundantní spoje. Mezi dvěma směrovači v síti existují vždy dvě cesty. Pro směrování v síti byl používán směrovací protokol OSPF, který mapuje celou topologii a vypočítává nejlepší cestu sítí pro každý směrovač. V případě výpadku nějakého spoje se automaticky rozešle zpráva o změně topologie a směrovače si přepočítají směrovací tabulku. Schéma propojení směrovačů v páteřní síti je na Obr. 5.40. Servery jednotlivých služeb byly připojeny k směrovači A. Všichni klienti byli připojeny k páteřní síti přes směrovač D. Nejvhodnější cesta toku dat mezi servery a klienty byla směrována přes směrovač E. Výpadek či porucha spojení byly simulovány odpojením konektoru ze směrovače E.



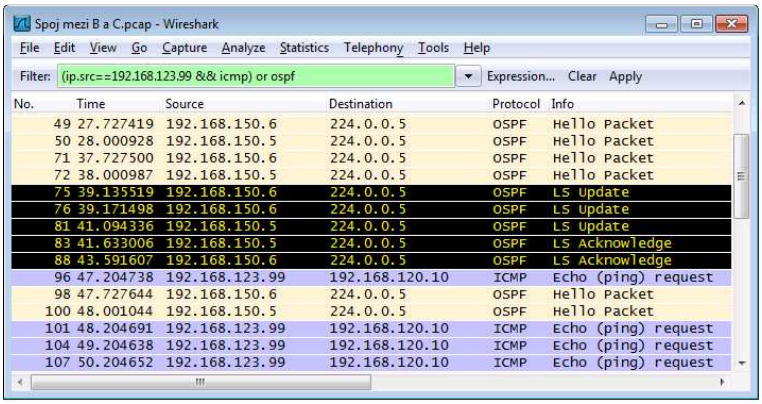
Obr. 5.40: Propojení směrovačů při výpadku spoje

Pro určení délky doby přerušení mezi výpadkem a přepnutím na záložní spoj byl využit program ping využívající icmp echo zprávy. Na klientském počítači byla dotazována dostupnost serveru FTP (IP adresa 192.168.120.10) v pravidelných vteřinových intervalech. Pomocí programu Wireshark byly zachyceny a filtrovány pouze pakety, které se dotazovaly na dostupnost FTP serveru. Zachycené pakety jsou na Obr. 5.41.



Obr. 5.41: Zachycené pakety dotazující se na dostupnost FTP serveru

Doba přerušení dostupnosti FTP serveru způsobená přerušením aktivního spoje činila cca 11 vteřin, viz Obr. 5.41. Při opakovaném měření dosahovaly hodnoty přerušení 10 až 11 vteřin. Zda došlo k přesměrování, bylo ověřeno hodnotou TTL v hlavičce paketu programem Wireshark. Jakmile některý směrovač zjistí, že došlo k přerušení spoje neboli k změně topologie, vyšle zprávu o opravě – Link State Update (LSU). Sítí se šíří tato zpráva a směrovače ji přeposílají dále. LSU paket je nutno vždy potvrdit paketem Link State Acknowledgement (LSA). Jakmile směrovače obdrží potvrzení, opraví si směrovací tabulku a nově příchozí datové pakety jsou již směrovány správně. Zprávy si směrovače předávají pomocí multicastové adresy 224.0.0.5. Časová posloupnost OSPF zpráv zachycená na náhradním spoji v experimentální síti následně po výpadku je zobrazena na Obr. 5.42. Pomocí filtru byly filtrovány pakety OSPF a icmp dotazy, které tímto spojem začaly být nově směrovány.



Obr. 5.42: Zachycené pakety v síti po výpadku spoje

Důsledky výpadku spoje

Doba přerušení dostupnosti vzdáleného serveru či stanice při výpadku činila 10 vteřin. Návaznost dostupnosti datových služeb realizovaných v experimentální síti během výpadku spojení byla pozitivní. Přenosy paketů provozu VoIP, streamu a FTP se během výpadku (10 vteřin) zastavily, ale poté automaticky navázaly přerušené spojení a pokračovaly dále v přenosu. Pouze služba http musela být ručně aktualizována.

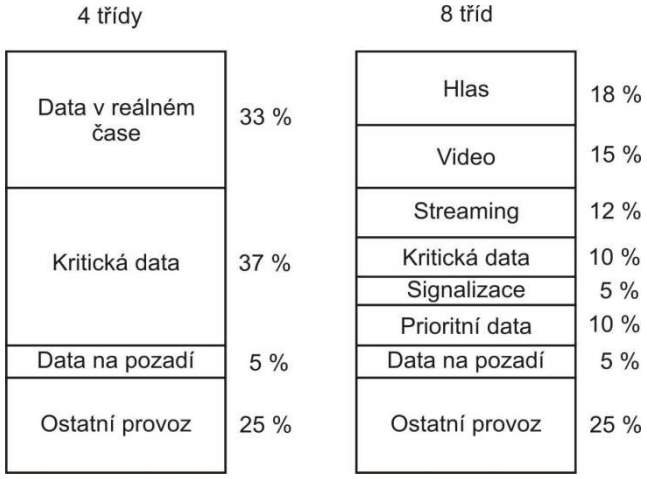
6 NÁVRH PRO MENŠÍ PODNIKOVOU SÍŤ

V případě nasazení kvality služeb v podnikové síti je vždy třeba vycházet z požadavků, které jsou kladeny na síťovou infrastrukturu. Každý podnik klade různé požadavky na svou dostupnost služeb. Společnost pro poskytnutí hostingu pro web či emailové servery bude garantovat konektivitu protokolu HTTP či IMAP oproti společnosti zabývající se „horkou“ telefonní linkou pro své zákazníky, kde bude preferován převážně VoIP. Obecně platí, že služby v reálném čase (např. VoIP) je třeba upřednostňovat. Při návrhu kvality služeb se můžeme zabývat i ostatními službami a jejich upřednostňováním mezi sebou.

Při návrhu je třeba brát v potaz následující základní otázky:

- Je účelem upřednostnit pouze VoIP komunikaci?
- Je třeba uvažovat i video přenos (stream nebo realtime)?
- Jsou nějaké aplikace vyžadující kritické parametry pro přenos?
- Existují v síti služby s nízkou prioritou?

Nejjednodušší rozdělení prioritního rozsahu je pomocí čtyř základních datových tříd. V případě podrobnějšího nastavení kvality služeb je vhodné volit více tříd. Ideálně pro každý druh služby vlastní třídu. Příklad rozdělení rozsahu pásma na 4 a více základních tříd podle doporučení společnosti Cisco [16] je uveden na Obr. 6.1. Použitím více tříd je možné blíže specifikovat vzájemné prioritní vztahy mezi jednotlivými třídami. Další výhodou je možnost konkrétní datové třídě rezervovat šířku pásma.



Obr. 6.1: Základní nastavení prioritních tříd podle doporučení Cisco

Dalším krokem je přiřazení značky priority všem třídám. Základní doporučení Cisco klasifikace je uvedeno v Tab. 6.1 [16]. Uvedené doporučené hodnoty se mohou lišit v jednotlivých případech. Vždy záleží na správci podnikové sítě či domény. Důležité je seřadit jednotlivé třídy podle priority a označit třídy odpovídající značkou priority (DSCP).

Důležitým krokem k dokončení nastavení QoS je vhodná volba obslužných mechanizmů. Mechanizmů pro obsluhu je více a každé zařízení disponuje odlišnými mechanizmy. Moderní síťové prvky podporují mechanizmus zajišťující rychlé odbavení s minimálním zpožděním, např LLQ. Služby v reálném čase je vhodné obsluhovat právě mechanizmem LLQ (VoIP, videotelefonie).

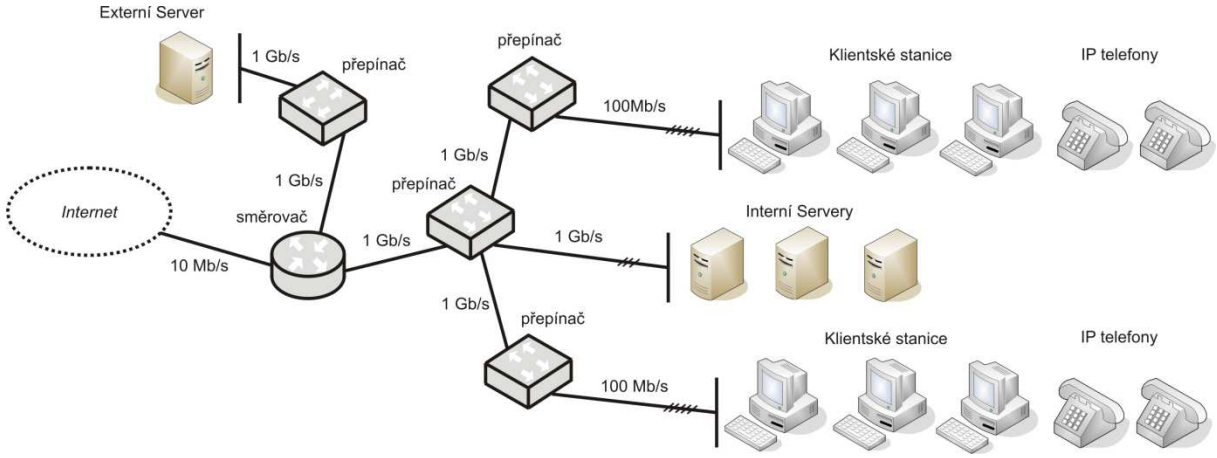
Dále jsou síťové prvky vybaveny mechanizmy zaručující nevyhladovění tříd, zaručující kvalitativní prostředky pro prioritní obsluhu jednotlivých třídy, např. CBWFQ.

Tab. 6.1: Základní klasifikace tříd podle doporučení Cisco

Služba	Klasifikace		Příklad
	PHB	DSCP	
Směrování	CS 6	48	RIP, OSPF, SNMP
Hlas v reálném čase	EF	46	RTP audio
Video v reálném čase	AF 41	34	RTP video
Streaming video	CS 4	32	UDP (porty)
Kritická data	AF 31	26	RDP, VPN
Signalizace	CS 3	24	SIP, DNS
Prioritní data	AF 21	18	HTTP, SSH
Data na pozadí	AF 11	10	FTP, SMTP
Ostatní provoz	Best Effort	0	ostatní

Konkrétní případ podnikové sítě

Schéma zapojení jednotlivých síťových prvků v podniku je naznačeno na Obr. 6.2. V takto situovaném zapojení podnikové sítě je třeba se věnovat kvalitě služeb jak na hranici firmy (připojení k internetu), tak i uvnitř podnikové sítě (interní provoz).



Obr. 6.2: Topologie podnikové sítě

V případě implementace QoS do stávající počítačové sítě je třeba vhodně analyzovat stávající datový provoz, určit více i méně prioritní data, navrhnout omezení pro nevyžádaná spojení a zachovat stávající bezpečnostní politiku společnosti. V případě propojení více poboček přes veřejnou síť internet je třeba počítat s rychlostním omezením poskytovatele připojení k internetu.

Při návrhu scénáře kvality služeb v síti, je třeba se zabývat následujícími body:

- Definovat žádoucí datové služby a spojení (min. šířka pásma, max. zpoždění apod.)
- Uvažovat, případně zvýšit rychlosti spojů síťové infrastruktuře
- Rozmístit síťové prvky, dle podpory QoS, v podnikové síti
- Nastavit omezení jednotlivým datovým službám

Příklad požadavků společnosti pro návrh QoS v menší podnikové síti je uveden v Tab. 6.2, kde podniková síť musí zajistit uvedené požadavky. Nejvyšší prioritu má služba VoIP. Druhá preferovaná služba je VPN spojení pro udržení komunikace se vzdálenou pobočkou a VPN klienty využívající služeb firemního serveru. Společnost vyžaduje i garantovaný přenos videa. Klasické služby HTTP a FTP jsou samozřejmostí. Z mravních účelů je však požadováno omezení rychlosti stahování dat. Společnost je připojena k veřejné síti internet. Poskytovatel internetového připojení garantuje rychlost 10 Mb/s.

Tab. 6.2: Požadavky pro návrh podnikové sítě

Priorita	Služba	Min. rychlost [Mb/s]	Max. rychlost [Mb/s]
1.	VoIP	0,5	2
2.	VPN	2	Neomezeno
3.	IP TV	4	4,5
4.	HTTP	0,5	Neomezeno
5.	FTP	0,5	1
6.	Ostatní	2,5	Neomezeno

Směrovač připojený k internetu by měl mít aplikovanou politiku QoS dle Tab. 6.2. V rámci svých možností by měl být schopen rozlišit jednotlivé provozy (provést klasifikaci) a upřednostnit jednotlivé datové služby. Pro služby VoIP je žádoucí vyhradit prioritní frontu, nejčastěji mechanizmem obsluhy LLQ, a ostatní provozy upřednostnit například mechanizmem CBWFQ. Omezení maximální rychlosti se aplikuje nastavením policingu k dané službě. Příklad nastavení politiky na směrovači je uveden v Tab. 6.3.

Tab. 6.3: Řešení politiky QoS na směrovači v podnikové síti

Klasifikace	Značkování	Fronta	Policing
VoIP	DSCP EF	LLQ 5%	CIR 2 Mb/s
VPN	DSCP AF 41	CBWFQ 20%	-
IP TV	DSCP AF 31	CBWFQ 40%	CIR 4,5 Mb/s
HTTP	DSCP AF 21	CBWFQ 5%	-
FTP	DSCP AF 11	CBWFQ 5%	CIR 1 Mb/s
Default	Best Effort	WFQ 25%	CIR 4 Mb/s

Implementace kvality služeb do lokální sítě je možná pouze pokud přepínače podporují QoS. Dle možností je žádoucí alespoň upřednostnit VoIP komunikaci od ostatního provozu. Přepínače podporu QoS převážně řeší přiřazením daných rámců do front. Dle množství front je možné roztřídit jednotlivé provozy. Nejčastější metoda obsluhy je WRR.

K přiřazení rámce do fronty je několik možností. Nejjednodušší je přiřazení fyzického portu přepínače. V takovém případě je třeba zajistit, aby k danému prioritnímu portu byl opravdu připojen např. IP telefon. Další možností je klasifikovat podle informací v hlavičce rámce, podle MAC adresy zdrojové či cílové. Pokud jsou v síti zavedeny virtuální sítě VLAN, je možné využít v hlavičce rámce hodnotu CoS. V tomto případě je třeba zajistit správné mapování nejlépe přímo u zdroje vysílání.

Řešením pro podnikovou síť uvedenou na Obr. 6.2 k zajištění kvality služeb v lokální síti by bylo zavedení virtuální sítě VLAN. I v případě nevyužití možností virtuálních sítí je žádoucí, aby mezi přepínači byly přenášeny tagované rámce (IEEE 802.1Q), které obsahují hodnotu CoS. Jednotlivým

službám bude přidělena patřičná prioritní hodnota CoS. Dále by bylo vhodné přiřadit konkrétní fyzický port na přepínači, kam budou následně připojovány pouze IP telefony, případně další porty pro stanice využívající IP TV. Na směrovači je třeba nastavit mapování priority ze síťové na linkovou vrstvu.

ZÁVĚR

Obsahem práce byl rozbor a testování technologií pro nasazení podpory kvalitativních požadavků služeb v datových sítích IP. Se zaváděním nových a nových aplikací do prostředí IP sítí s různými požadavky na síť ohledně dodržení kvalitativních parametrů služeb a s nárůstem objemu dat, který je zapotřebí sítí přenést, je nasazení podpory kvalitativních parametrů služeb v sítích nezbytné k dosažení přijatelné úrovně kvality služeb při vynaložení akceptovatelného množství finančních prostředků na její zajištění. Přínos nasazení se projevuje především při vysokých úrovních vytížení síťových uzlů a spojů, kdy hrozí nebezpečí velkého zpoždění či dokonce ztráty přenášených dat. Kvalita služeb QoS umožňuje obranu před nežádoucími jevy, jako jsou velmi nízká kvalita či dokonce nedostupnost důležitých služeb v datové síti právě v době velkého zatížení sítě službami typu přenosů velkých objemů dat.

V práci byly rozebrány základní dvě technologie pro nasazení QoS v IP sítích, a to technologie integrovaných služeb (IntServ) a technologie diferencovaných služeb (DiffServ), a uvedeny jejich výhody a nevýhody v případě nasazení. Způsob značení a zacházení s datovými jednotkami byl popsán na síťové i linkové vrstvě. Parametry přenosu, které jsou důležité pro chod aplikací, byly detailně rozvedeny.

Pro praktické ověření teoretických poznatků byla z dostupných síťových prvků v laboratoři UTKO navržena a následně vytvořena laboratorní experimentální síť. Možnosti, které nabízejí použité síťové prvky, byly prostudovány a následně nastaveny k ověření činnosti. Síť byla sestavena z řady zařízení od různých výrobců, a to z přepojovacích prvků (směrovače a přepínače; největší zastoupení tvoří síťové prvky od společnosti Cisco) a koncových uzlů (osobní počítače, servery, IP telefony, aj.). V síti byla realizována řada služeb s různým typem provozu (VoIP, FTP, HTTP, Video). Provoz se liší nejen obsahově, ale především v nárocích na síťové prostředky. Některé služby (hlas a video v reálném čase) jsou citlivé na zpoždění a jeho proměnlivost, a proto vyžadují prioritní obsluhu, oproti službám, které vyžadují primárně vysokou spolehlivost přenosu (FTP, HTTP). S technickými a programovými prostředky pro zprovoznění jednotlivých služeb bylo třeba se detailně seznámit a poté služby v experimentální síti laboratoře zprovoznit. V přepojovacích prvcích (přepínačích a především směrovačích) byly konfigurovány různé úrovně a způsoby podpory kvalitativních požadavků služeb a byla realizována řada měření. Ve směrovačích byla použita technologie diferencovaných služeb (Differentiated Services), jenž pro uplatnění priorit využívá značku v záhlaví paketů. Síťové prvky mohou danou značku přečíst, podle hodnoty značky je zařazují do fronty s určitou prioritou a implementují určitý mechanizmus obsluhy front, čímž se přiděluje danému paketu, a tedy službě určité množství síťových prostředků. V případě, že síťový prvek neimplementuje podporu QoS, jsou pakety obsluhovány v pořadí, ve kterém do síťového prvku přišly, což může v případě silného zatížení sítě podstatně navýšit zpoždění či dokonce způsobit ztráty paketů, a také výrazně ovlivnit kvalitativní parametry provozovaných služeb.

Nevyžádaným datovým tokem byla reálně nastolena situace zahlcení přenosového spoje mezi směrovači bez podpory QoS. Negativní dopady se dotkly všech datových služeb. Přenos hlasu byl velmi trhavý a ztrátový, video přenos byl zcela znehodnocen artefakty. Služby FTP a HTTP byly pro nedostupnost vzdálené strany přerušeny. Obranou proti nedostupnosti požadované datové služby při vytížení určitého spoje v síti je zavedení diferenciace služeb a vytvoření DiffServ domény.

Pro obsluhu prioritních front byly testovány dva základní principy, a to LLQ (Low Latency Queueing) a CBWFQ (Class-Based Weighted Fair Queueing). Při měření pouze mechanizmu LLQ pro jednotlivé služby bylo patrné, že překročení definovaného přenosového pásma v politice znamenalo zahájení částečného zahazování. Metoda LLQ striktně drží provoz ve vyhrazené šířce pásma a nedovolí využít nevyužitou šířku pásma spoje. Oproti tomu mechanizmus CBWFQ dovolil využít definované třídě celou nevyužitou kapacitu a zajistil, aby ostatní služby nebyly ovlivněny zvýšenou zátěží. Nevýhodou CBWFQ je, že nedefinovaný provoz v politice QoS dokáže vyhladovět. Proto se v praxi vytváří tzv. základní třída (class-default) kam spadá nedefinovaný provoz v politice s obsluhou WFQ (Weighted Fair Queueing). Z výsledků měření obsluhy prioritních řazení dostupných

mechanizmů vyplývá, že je vhodné pro obsluhu jednotlivých prioritních tříd použít více mechanizmů. Porovnáním výhod a nevýhod mechanizmů, které byly měřením ověřeny, je nejvhodnější kombinace mechanizmů tak, aby služby v reálném čase byly obsluhovány mechanizmem LLQ a ostatní datové služby měly přidělenu vhodnou prioritní frontu a obsluhovány mechanizmem CBWFQ.

Na základě získaných znalostí v problematice kvalitativních služeb byly navrženy dvě laboratorní úlohy pro výuku studentů. Cílem úloh je seznámit studenty s výhodami nasazení QoS v sítích a řízení datových toků. Umožnit jim přístup k nastavení politiky na směrovačích Cisco a následně provést měření nastavených parametrů.

SEZNAM ZKRATEK

AF	Assured Forwarding
BC	Committed Burst
BE	Best Effort
BE	Excess Burst
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
CS	Class Selector
DiffServ	Differentiated Services
DSCP	Differentiated Service Code Point
EF	Expedited Forwarding
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IntServ	Integrated Services
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	Open Systems Interconnection
ITU-T	International Telecommunication Union Telecommunication
MSB	Most Significant Bit
NAT	Network Address Translation
OSI	International Organization for Standardization
PBX	Private Branch eXchange
PHB	Per Hop Behaviours
PIR	Peak Information Rate
QoS	Quality of Service
RSVP	Resource Reservation Protocol
TC	Traffic Class
TCP	Transmission Control Protocol
ToS	Type of Service
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

WFQ	Weighted fair queuing
WLAN	Wireless Local Area Network
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*. [s.l.] : Brno : Computer Press, 2007. 225 s. ISBN 978-80-251-1458-2.

[4] HERMAN, I. *Komunikační technologi*e. [s.l.] : 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. 2010-11-10]. Dostupný z WWW: http://www.cesnet.cz/doc/techzpravy/2000-6/.

[6] LHOTKA, L. *Internet se zaručenou kvalitou služby*. [online]. [2000] [cit. 2010-10-21]. Dostupný z WWW: http://www.cesnet.cz/doc/seminare/ei2000liberec/lhotka.html.

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

[8] PETERKA, J. *Šířka pásma a její dělení.* [online]. [1996] [cit. 2010-10-12]. Dostupný z WWW: http://www.earchiv.cz/a91/a143c110.php3

[9] WALLACE, K. *Cisco VoIP*. Brno : Computer Press, [s.l.]: 2009. 527 s. ISBN 978-80-251-2228-0.

[10] PAUL, A. *QoS in Data Networks : Protocols and Standards.* [online]. [1999] [cit. 2010-11-09]. Dostupný z WWW: http://www.cse.wustl.edu/~jain/cis788-99/qos_protocols/

[11] Cisco Systems, Inc. *Internetworking Technologies Handbook* [online]. [2003] [cit. 2010-11-09]. Dostupný z WWW: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm

[12] FOGL, M. *Experimentální síť pro testování podpory QoS*. Brno: Vysoké učení technické v Brně, FEKT, 2009. 38s. Vedoucí bakalářské práce doc. Ing. Vít Novotný, Ph.D.

[13] Cisco Systems, Inc. *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* [online]. [2010] [cit. 2011-02-24]. Dostupný z WWW: http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpolsh.html

[14] SZIGETI, T., HATTINGH, CH., End-to-End QoS Network Design. Cisco Press, ISBN 1-58705-176-1, Indianapolis, USA

[15] DVOŘÁK, P. *Principy, funkce přepínání a směrování v počítačové síti.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 51 s. Vedoucí bakalářské práce Ing. Michal Polívka

[16] Cisco Systems, Inc. *Next Generation Enterprise MPLS VPN-Based MAN Design and Implementation Guide* [online]. [2006] [cit. 2011-05-01]. Dostupný z WWW: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/ngmane.pdf

[17] Cisco Systems, Inc.*QoS Frequently Asked Questions* [online]. [2009] [cit. 2011-05-10]. Dostupný z WWW: http://www.cisco.com/application/pdf/paws/22833/qos_faq.pdf