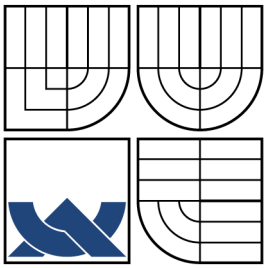
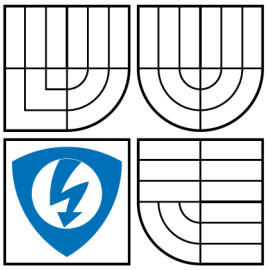


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

QOS V IP SÍTI

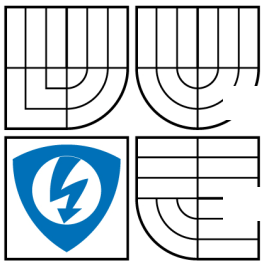
QoS IN IP NETWORK

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE — Bc. MIROSLAV BUMBÁL
AUTHOR

VEDOUCÍ PRÁCE — ING. LUKÁŠ RŮČKA
SUPERVISOR

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNE

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský studijní obor

Telekomunikační a informační technika

Student: Miroslav Bumbál ***ID:*** 83892

Ročník: 2 ***Akademický rok:*** 2008/2009

NÁZEV TÉMATU:

QoS v IP síti

POKYNY K VYPRACOVANÍ:

Popište základní vlastnosti a požadavky IP sítí při přenosu dat citlivých na kvalitu služby. Prostudujte principy a možnosti zajištění QoS v IP síti. Seznamte se možnostmi zajištění QoS v IP síti, která bude obsahovat směrovače Cisco řady 1800. S ohledem na dostupné zařízení navrhněte modelovou simulační IP síť pro zajištění QoS.

DOPORUČENÁ LITERATURA:

[1] Wang, Zhendi. Internet QoS: Architectures and Mechanisms for Quality of Service. San Francisco: Morgan Kaufmann, 2001. 256 s. ISBN 1-55860-608-4.

[2] Flannagan, Mike E. Administering Cisco QoS for IP Network. Syngress Publishing, 2001. 535 s. ISBN 1-928994-21-0.

Termín zadaní: 12. 2. 2009 ***Termín odevzdaní:*** 8.6. 2009

Vedoucí projektu: Ing. Lukáš Růčka

ANOTACE

Diplomová práce pojednává o počítačových sítích, které tvoří v současné době globální komunikační strukturu a sehrávají v dnešní společnosti velmi důležitou úlohu. Prudký rozvoj Internetu, vznik nových multimediálních aplikací a jejich rostoucí využití si vyžaduje k jejich efektivní činnosti vznik takových mechanizmů správy přenosu, které jsou schopny zabezpečit požadované parametry.

Práce se zabývá především problematikou kvality služeb (QoS) v IP sítích. Uvádí základní vlastnosti a požadavky těchto sítí při přenosu dat citlivých na kvalitu služeb, pojednává o definici QoS a popisuje její podstatní parametry, které je nutno dodržet pro dosáhnutí požadované kvality služeb v praktickém nasazení. Dále uvádí jednotlivé principy a možnosti zajištění QoS v počítačových sítích. Všeobecne představuje vlastnosti smerovačů Cisco 1841 a možnosti zajištění kvality služeb v síti postavené na těchto smerovačích.

Praktická část práce uvádí dva typy modelové IP sítě, které byly navrženy za účelem ověření vplyvu kvality služeb v reálné praxi. Ze známých způsobů zajištění QoS, ke kterým patří především mechanismus Integrovaných a Diferencovaných služeb se zaměřuje svým obsahem právě na Diferencované služby a jejich implementaci v navržené modelové síti. Poslední část práce představuje dosažené výsledky vlivu kvality služeb na aplikace a jejich zhodnocení.

Klíčová slova: kvalita služeb, QoS, IP síť, best-effort, integrované služby, diferencované služby, Cisco 1841, MQC

ABSTRACT

Master 's thesis deals about computer networks, which constitutes a global communication structure and play a very important role in today's society. The rapid development of Internet, the emergence of new multimedia applications and their increasing use of calls to the efficient functioning of the creation of such governance mechanisms of transmission, which are able to secure the required parameters.

The thesis deals about the issue of quality of service (QoS) in IP networks. It presents the basic characteristics and requirements of these networks for the transmission of sensitive data by the quality of services, deals with the QoS definition, and describes the essential parameters to be followed to achieve the required quality of service in practical deployment. In addition, lists the various principles and options to ensure QoS in computer networks. Generally, it represents the Cisco 1841 router features and options to ensure quality of service in the network based on these routers.

Practical thesis part provides two types of model IP networks, which were designed in order to verify the impact of service quality in real practice. Of the known methods to ensure QoS, which include a mechanism of Integrated services, Differentiated services, it focus its content about the Differentiated Services and the implementation of these in proposed network model. The last part of the work presents the results obtained by the impact of quality of service for the applications and their assessment.

Keywords: Quality of Services, QoS, IP network, best-effort, Integrated services, Differentiated services, Cisco 1841, MQC

BIBLIOGRAFICKÁ CITÁCIA:

BUMBÁL, M. *QoS v IP síti.*
Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 69 s. Vedoucí diplomové práce Ing. Lukáš Růčka.

PREHLÁSENIE

Prehlasujem, že svoju diplomovú prácu na tému "QoS v IP síti" som vypracoval samostatne pod vedením vedúceho diplomovej práce a s použitím odbornej literatury a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, predovšetkým som nezasiahol nedovoleným spôsobem do cudzích autorských práv osobnostných a som si plne vedomý následkov porušenia ustanovenia § 11 a následujúceho autorského zákona č. 121/2000 Sb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanoveníia § 152 trestného zákona č. 140/1961 Sb.“

V Brne dňa ……..... .....……..

(podpis autora)

Prehľad použitých skratiek a symbolov:

ACL	Access Control List
AF	Assured Forwarding
ARPANET	Advanced Research Projects Agency Network
ATM	Asynchronous transfer Mode
BGP	Boarder Gateway Protocol
CAR	Commmited Access Rate
CBWFQ	Class Based Weighted Fair Queuing
CLI	Command Line Interface
CoS	Class of Services
CP	Code Point
DARPA	Defense Advanced Research Projects Agency
DS, DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
FEC	Forwarding Equivalence Class
FIFO	First In, FirstOut
FQ	Fair Queuing
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IOS	Internetworking Operating System
IP	Internet Protocol
IPTV	IP TeleVision
ISP	Internet Service Provider
IS-IS	Intermediate system to intermediate system
ITU	International Telecommunication Union
LDP	Label Switching Path
LFI	Link Fragmentation and Interleaving
LLQ	Low Latency Queuing
LSR	Label Switching Router
LSP	Label Switchning Protocol

MPLS	Multi Protocol Label Switching
MQC	Modular QoS CLI
NBAR	Netwrok-Based Application Recognition
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PHB	Per Hop Behavior
PPP	Point-to-Point Protocol
PQ	Priority Queuing
QoS	Quality of Service
RED	Random Early Detection
RTI	Real Time Intolerant
RTT	Real Time Tolerant
RSVP	Resource Reservation Protocol
SBM	Subnet Bandwith Management
SDM	Security Device Manager
SLA	Service Level Agreement
SSH	Secure Shell
TC	Traffic Class
TCP	Transmision Control Protocol
ToS	Type of Service
TTL	Time to live
UDP	User Datagram Protocol
VoIP	Voice over IP
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin

OBSAH

1. ÚVOD

1.1 História a vývoj Internetu

Korene Internetu môžeme situovať do začiatku 70. rokov minulého storočia, kedy bola za podpory amerického Ministerstva obrany vyvinutá Agentúrou DARPA experimentálna dátová sieť nazvaná ARPANET [1]. Cieľom bolo vybudovať sieť, ktorá by odolala vojenským útokom a tak bol model siete postavený na datagramovej službe, ktorá doručuje každý paket nezávisle na jeho cieli. Táto sieť bola založená na jednoduchosti a schopnosti sa automaticky prispôsobiť zmenám topológie. Internet bol po mnohé ďalšie roky využívaný hlavne na vedecké výskumy vo vojenskom prostredí. To spôsobilo určité zabrzdenie jeho vývoja. Avšak aplikácie ako vzdialený prístup, prenos súborov a posielanie emailov sa stali populárnymi a fungovali veľmi dobre práve na datagramovom modeli vyvinutej siete. Rozvojom Internetu však došlo k jej zásadnej zmene. Internet sa stal neoddeliteľnou súčasťou života a práce ľudí.

V súčasnosti je na svete obrovský počet verejných sietí a nové aplikácie ako elektronické obchodníctvo, digitálny prenos videa, internetová telefónia, webové vyhľadávanie, elektronické média a diskusné fóra sa rozširujú nebývalou rýchlosťou. Vstupom do 21. storočia sa Internet stal globálnou komunikačnou štruktúrou. Mnohé z nových aplikácií majú veľmi odlišné požiadavky na rozdiel od tých, pre ktoré bol Internet vyvinutý. Problémom sa stáva zaistenie výkonu pre ich prevádzku. Datagramový model, na ktorom je Internet založený má len niekoľko jednoduchých možností riadenia zdrojov v rámci siete a preto nemôže poskytnúť žiadne záruky rezervácie zdrojov pre užívateľov. Pri pokuse uskutočniť telefónny hovor môže dôjsť k situácii, pri ktorej budú určité časti siete tak zahltené, že pakety jednoducho nebudú doručené. Väčšina real-timeových aplikácií vyžaduje určitú minimálnu úroveň zdrojov pre efektívnu činnosť. Vzhľadom k tomu, že Internet sa stáva nevyhnutnou súčasťou nášho života a práce, nedostatok jeho výkonu je významným problémom, ktorý treba riešiť.

1.2 Súčasná situácia

Klasická IP sieť, ktorá je až dodnes založená na pôvodnom datagramovom modeli a k prenosu dát využíva sadu TCP/IP protokolov dokáže poskytnúť dátam len jednu úroveň služieb. Nerozlišuje druh jednotlivých paketov a so všetkými zaobchádza rovnakým spôsobom. K doručeniu paketov používa tzv. metódu „best effort“, ktorá každý paket smeruje sieťou samostatne a nezávisle a jej hlavnou úlohou je doručenie jednotlivých paketov v čo najkratšom čase [1]. Všetky pakety sú si tak pri doručovaní rovnocenné a ak dôjde k zahlteniu siete, sú si pakety rovnocenné aj čo sa týka ich možnosti zahodenia. Ani doba ich doručenia nie je žiadnym spôsobom garantovaná. Z toho vyplýva, že neexistuje žiaden kontrolný mechanizmus, ktorý by zaručil určitú úroveň kvality sieťových služieb. Alternatívou k riadiacim mechanizmom QoS môže byť v týchto sieťach len poskytnutie vysoko kvalitnej komunikácie, ktorá zabezpečí prevádzkovú kapacitu pre očakávané zaťaženie.

Prudký rozvoj Internetu a vznik nových, predovšetkým multimediálnych aplikácií si vyžaduje zavedenie priorizácie dátových tokov týchto služieb voči prenosu ostatných dát na sieti.

2. KVALITA SLUŽIEB – QOS

2.1 Obecne o kvalite služieb

Interaktívne sieťové aplikácie, akými sú prenos hlasu a videa, vyžadujú relatívne konštantnú šírku pásma a sú veľmi citlivé na premenlivosť oneskorenia a stratu paketov. Čiastočná strata informácie je do určitej miery tolerovaná a možno ju kompenzovať rôznymi opravnými metódami. Ak však dôjde k prekročeniu určitej úrovne týchto nežiaducich parametrov, aplikácie sa stávajú nepoužiteľnými. Naproti tomu dátový prenos je charakteristický premennými nárokmi na šírku pásma a na spoľahlivosť spojenia. Z jeho podstaty vyplýva, že dokáže tolerovať relatívne vyššiu úroveň oneskorenia a straty paketov bez zníženia vnímaného výkonu. Požiadavky zákazníkov sa tiež odlišujú v závislosti od využitia Internetu. Napríklad organizácie, ktoré využívajú Internet na bankové operácie, alebo k riadeniu priemyselných zariadení sú ochotné pre zabezpečenie vyššej priority doručenia ich dát zaplatiť väčší poplatok.

Internet sa stane skutočne viacúčelovou sieťou len v prípade, že bude podporovať rozlíšenie jednotlivých služieb. Implementácia týchto schopností QoS v rámci Internetu bola jednou z najväčších výziev počas jeho vývoja, pretože sa dotýka takmer všetkých aspektov sieťových technológií a vyžaduje zmeny základnej architektúry Internetu. Za viac ako desať rokov nepretržitého úsilia o vyriešenie tohto problému vyvinula skupina ľudí pod označením IETF (Internet Engineering Task Force) nové technológie a štandardy, ktoré majú zabezpečiť zaistenie sieťových zdrojov a rozlíšenie služieb [1]. Tieto vystupujú pod spoločným názvom QoS.

2.2 Definícia QoS

Pojem kvalita služieb označuje schopnosť poskytovať zaistenie zdrojov a rozlíšenie služieb. V jednoduchosti možno povedať, že určuje riadenie jednotlivých dátových tokov v sieti. Zaisťuje rovnomerné delenie záťaže s ohľadom na druh prenášaných dát a spravodlivo rozdeľuje konektivitu medzi jednotlivých zákazníkov podľa nastavených parametrov a priorít jednotlivých služieb [2]. Predovšetkým však zabraňuje kritickému preťaženiu a zahlteniu siete. Kvalita služieb by mala byť nastavená tak, aby služby neboli

pod hranicou použiteľnosti a na druhej strane, aby nebolo rezervovaných zbytočne moc prostriedkov pre danú službu. Index kvality služieb by mal ležať niekde uprostred tohto pomyselného intervalu.

Alternatívnou definíciou kvality služieb využívanou predovšetkým pri VoIP (Voice over IP) a IPTV (IP Television) službách je metrika, ktorá vyjadruje subjektívnu kvalitu „výkonu“ vnímanú užívateľom, stupeň spokojnosti daného zákazníka a počet všetkých spokojných zákazníkov [3]. QoS tak označuje mieru súhrnného pôsobenia všetkých nedostatkov služby na spokojnosť účastníka siete.

Kvalita služby je ovplyvnená všetkými komponentmi siete a preto musí byť na všetkých prvkoch nakonfigurovaná určitá úroveň jej podpory. To znamená, že výkon celej siete bude výrazne závislý na najslabšom prvku v sieti. Výnimku tvoria fyzické spoje, kde si nejakú konfiguráciu možno len ťažko predstaviť. Istou výnimkou sú moderné spoje bezdrôtových sietí, kde vhodnou voľbou typu kódovania možno výrazne ovplyvniť kvalitu celého prenosu. Vysoká úroveň QoS je často spojená s vysokou úrovňou výkonu siete a dosiahnutou kvalitou služby, napr. vysokou prenosovou rýchlosťou, nízkou latenciou a nízkou pravdepodobnosťou výskytu chyby.

2.3 Hlavné parametre kvality služieb

Parametre QoS sú veličiny, ktoré ovplyvňujú výslednú kvalitu služby. Tieto veličiny sú v najväčšej miere závislé na sieťovom vybavení pozdĺž dátovej cesty paketu. Medzi hlavné parametre QoS patrí [4], [5]:

- **Šírka pásma** – Bandwith [kbit/s]
- **Oneskorenie** – Delay [ms]
- **Rozptyl oneskorenia** – Jitter [ms]
- **Stratovosť** – Lossrate [%]

2.3.1 Šírka pásma

Je to v podstate prenosová rýchlosť dát a označuje kapacitu daného systému pri prenose informácií sieťou. Obecne platí, že čím väčšiu šírku pásma v prenosovom systéme možno použiť, tým väčšiu prenosovú rýchlosť možno v tomto systéme teoreticky dosiahnuť. Interaktívne multimediálne aplikácie vyžadujú čo najväčšiu šírku pásma, teda aj čo najväčšiu prenosovú rýchlosť. Nedostatočná prenosová rýchlosť sa prejavuje najčastejšie oneskorením, ktoré spôsobuje trhanie hlasu či videa. Šírku pásma je nutné voliť predovšetkým podľa typu prevádzky u jednotlivých užívateľov. Pri určovaní dostupnej šírky pásma zohrávajú dôležitú úlohu fyzikálne vlastnosti siete, použité technológie a zákony fyziky.

Nemala by sa však zamieňať s priepustnosťou siete, ktorá vyjadruje priemernú mieru úspešného prenosu dát. Niektorí autori preferujú termíny ako hrubá prenosová rýchlosť, čistá prenosová rýchlosť a kapacita kanála, aby tak nedochádzalo k zámene medzi digitálnou šírkou pásma v bitoch za sekundu a analógovou šírkou pásma v Hz.

2.3.2 Oneskorenie

Celkové oneskorenie alebo tiež jednocestné oneskorenie je čas, ktorý zaberie dátam cesta z vysielacieho koncového zariadenia do cieľového koncového zariadenia. Väčšina ľudí zaregistruje oneskorenie pri prenose hlasu, až keď jeho hodnota presiahne čas 150 ms. Ak prevyšuje 200ms, je už kvalita prenášaného hlasu veľmi zlá. Nad 300ms je spojenie prakticky nepoužiteľné. Výsledná hodnota oneskorenia sa skladá z týchto častí [5]:

Propagačné oneskorenie – vzniká pri ceste dát z jedného konca siete na druhý. Je to teda čas, za ktorý sa prenesú dáta od vysielača k prijímaču. Je spôsobený konečnou rýchlosťou šírenia signálu po prenosovom médiu. Obecne sa dá zanedbať a jeho vplyv je pozorovateľný až pri komunikácii na väčšie vzdialenosti.

Paketizačné oneskorenie – je to čas potrebný na prevod analógového signálu do digitálnej formy, na prevod do aplikačného rámcu a jeho spätný prevod na analógový signál. Tento čas sa líši v závislosti od náročnosti kompresie použitého prevodového algoritmu v rámci danej služby. K nastaveniu parametrov použitého algoritmu sa musí pristupovať veľmi opatrne, pretože príliš veľké oneskorenie má nepriaznivý vplyv na komunikáciu.

Rozptyl oneskorenia vyrovnávacej pamäte – ide o oneskorenie vstupnej vyrovnávacej pamäte. Je spôsobené prijímačom pri ukladaní jedného alebo viacerých paketov, tak aby výsledné oneskorenie bolo konštantné a nedosahovalo vysokú kolísavosť.

Tab. 2.1: Závislosť oneskorenia od veľkosti fragmentu a rýchlosti linky

Rýchlosť linky [kb/s]	Veľkosť fragmentu [B]					
	64	128	256	512	1024	1500
	Hodnota oneskorenia [ms]					
64	8	16	32	64	128	187,5
128	4	8	16	32	64	93,8
256	2	4	8	16	32	46,9
512	1	2	4	8	16	23,4
1024	0,5	1	2	4	8	11,7

Z tabuľky [5] vyplýva, že vzhľadom k veľkosti oneskorenia sú vhodnejšie malé veľkosti fragmentov, pretože sa zmenší rozdiel medzi veľkosťou hlavičky a dátami v pakete a výrazne tak vzrastie zaťaženie siete.. Možno pozorovať, že hodnota paketizačného oneskorenia je nepriamo ovplyvnená aj rýchlosťou linky.

2.3.3 Rozptyl oneskorenia

Dáta sú po sieti vysielané v pravidelných časových intervaloch vo forme zhluku paketov. Vplyvom rôzneho vyťaženia siete, môže pri ich prenose dochádzať ku kolísaniu času príjmu. Toto premenlivé oneskorenie medzi doručením jednotlivých paketov sa označuje ako jitter – rozptyl (variácia) oneskorenia. V ideálnom prípade by mala cieľová aplikácia prijímať zhluky paketov v pravidelných časových intervaloch. V tomto prípade by bola veľkosť rozptylu nulová. V reálnej prevádzke sa pre potlačenie veľkosti jitteru používa vyrovnávacia pamäť umiestnená medzi sieťovou vrstvou a cieľovou VoIP aplikáciou. Jeho úlohou je vyrovnať premenlivosť príchodu paketov a umožniť i využitie paketov, ktoré boli prijaté mimo poradia v akom boli odoslané. Inštalovaná vyrovnávacia pamäť v snahe potlačiť kolísavosť príchodu pridrží pakety po určitú dobu a tým dochádza k zavedeniu ďalšieho jednosmerného oneskorenia do celej komunikácie. Ďalší problém nastáva ak dôjde k pretečeniu vyrovnávacej pamäti, vtedy sú všetky nové prichádzajúce pakety jednoducho zahodené a tým dochádza k ich strate.

2.3.4 Stratovosť

Vyjadruje pomer paketov, ktoré nedorazia ku cieľovej aplikácii v určitej dobe.. Ku strate môže dochádzať v dôsledku dočasného preťaženia niektorého sieťového zariadenia na komunikačnej trase. Napríklad pri spomínanom pretečení vyrovnávacej pamäte, alebo preťažení procesoru smerovača. Ďalej môže ku stratám dochádzať vplyvom externého rušenia, vznikom kolízií na linkovej vrstve spôsobených danou prístupovou metódou, alebo nesprávnym smerovaním či zahodením paketu z dôvodu zabránenia stavu zahltenia. Paket je považovaný za stratený aj v prípade, že je počas prenosu pozdržaný na príliš dlhú dobu a vyprší jeho vnútorný časovač. Dáta sú tak z hľadiska komunikačného protokolu považované za stratené.

Stratené pakety nemôžu byť obnovené a vytvárajú tak medzery v prenose. Ak je strata rozložená náhodne, nevedie to k významnému zhoršeniu kvality prenosu. Vysoká stratovosť paketov alebo strata veľkého množstva po sebe nasledujúcich paketov vedie k výraznému zhoršeniu kvality. Práve strata väčšieho množstva dát nasledujúcich za sebou najvýznamnejšie zhoršuje kvalitu prenosu. Tento efekt má za následok omnoho väčšie zhoršenie v kombinácii s vysokým oneskorením. Aplikácia síce môže požiadať znovu o vyslanie týchto informácií, to však spôsobí vážne oneskorenie v celkovom prenose.

Tab. 2.2: Tabuľka hodnôt sieťových parametrov [5]

Parametre QoS	Parametre siete		
	Dobrá	Prijateľná	Nevyhovujúca
Oneskorenie	0 - 150ms	150 - 300ms	nad 300ms
Rozptyl oneskorenia	0 - 20ms	20 - 50ms	nad 50ms
Stratovosť paketov	0 – 0,5%	0,5 – 1,5%	nad 1,5%

2.4 Aplikácie vyžadujúce QoS

Siete, ktoré využívajú ku komunikácii protokoly podporujúce kvalitu služieb sa môžu vzájomne dohodnúť s aplikáciou a rezervovať kapacitu sieťových uzlov, napr. v čase založenia spojenia. Počas spojenia môžu kontrolovať dosiahnutú úroveň parametrov, akými sú dátová priepustnosť a oneskorenie a dynamicky sledovať naplánovanú prioritu dátového toku v sieťových uzloch.

K takýmto typom aplikácií (služieb) patrí [6]:

- **Skupinové vysielanie** – vyžaduje takú garantovanú priepustnosť, aby bola zachovaná minimálna potrebná úroveň kvality, minimálnu úroveň stratovosti, oneskorenia a kolísania oneskorenia
- „**IP telefónia**“, prenos hlasu po IP sieti (**VoIP**) – vyžaduje prísne limity na rozptyl oneskorenia, oneskorenie samotné a dodržanie minimálnej stratovosti paketov.
- **Video Telekonferencia** – vyžaduje nízky rozptyl oneskorenia, zachovanie reakčnej doby a je citlivá na poskytnutú šírku pásma
- **IPTV** – je závislá na dodržaní určitého max. oneskorenia s minimálnym rozptylom
- **Elektronický obchod a bankové transakcie** – vyžadujú prísne limity na stratovosť paketov a oneskorenie, ktoré by postihli tento typ služby
- **Vyhradená emulácia linky** – vyžaduje garantovanú priepustnosť a splnenie určitých limitov maximálneho oneskorenia a kolísanie oneskorenia
- **Kritické aplikácie** (napr. diaľkovo riadená operácia) – vyžadujú garantovanú úroveň dostupnosti služby
- **Správa vzdialeného systému** – vyžaduje uprednostnenie SSH prenosu, aby bola zabezpečená reakcia nadviazanej relácie aj na silne zaťažených sieťových spojoch
- **On-line hry** – nedostatok kvality služieb môže vyvolať oneskorenie v prenose medzi jednotlivými hráčmi a spôsobovať „lagy“

Tieto typy služieb sa označujú ako nepružné, čo znamená, že vyžadujú určitú minimálnu úroveň šírky pásma, určitú hodnotu maximálneho oneskorenia s minimálnym rozptylom. Naopak, pružné aplikácie môžu využiť výhodu, či už väčšej, alebo menšej dostupnej šírky pásma. Väčšina aplikácii dátového prenosu založená na TCP protokole sa vo všeobecnosti chová ako pružná.

3. MECHANIZMY ZAISTENIA QOS V IP SIETI

K zaisteniu kvality služieb v IP sieťach možno použiť nasledujúce techniky [1], [2], [7]:

- predimenzovanie spojov
- rezervácia sieťových zdrojov
- použitie prioritných mechanizmov

Predimenzovanie dátových spojov – v minulosti bola jedinou možnosťou odstránenia nedostatku kapacity prenosovej linky. Aj v súčasnosti je naďalej najpoužívanejšou metódou, ako zaistiť v LAN prostredí jednotlivým aplikáciám postačujúce pásmo. Nejde však o „plnohodnotnú“ techniku zaistenia QoS a možno ju označiť len ako pasívnu z hľadiska zaručenia kvalít služieb na danej linke. Pri stávajúcom náraste používaných aplikácií je každé predimenzovanie spoja len dočasným riešením.

Rezervácia sieťových zdrojov – ako vyplýva z názvu, je založená na princípe rezervácie a alokácie potrebných prenosových prostriedkov pre rôzne typy dátových tokov v sieti. U všetkých prvkov zapojených do prenosu na danom spojení tak dôjde k vyčleneniu časti vlastných prostriedkov, ktoré nebude možné v rovnakej dobe využiť inými spojeniami. Typickými predstaviteľmi sú technológie Integrovaných služieb – IntServ, za podpory rezervačného protokolu RSVP a Diferencovaných služieb – DiffServ.

Technológia IntServ slúži k definícii služieb, ktoré už majú zaistené určité parametre kvality služieb a musí byť podporovaná oboma stranami koncových zariadení, medzi ktorými sa rezervácia vytvára. Z pohľadu prevodu a implementácie možno túto technológiu označiť za najnáročnejšiu, pre zaistenie kvality služieb v IP sieťach U Diffserv technológie ide o principiálne jednoduchší model založený na agregácii dátových tokov do tried služby – CoS (Class of Service).

Prioritné mechanizmy – ide o mechanizmy riadenia šírky pásma a optimalizácie výkonu na rôznych úrovniach komunikácie. V súčasnosti sú aplikované niekoľkými metódami a jedná sa o spôsob definície kritérií, podľa ktorých bude optimalizácia prevedená. Typickým predstaviteľmi metódy sú:

- Prepojovanie paketov s návestím – MPLS (*Multiprotocol Label Switching*)
- Správa prenosového pásma v podsieťach – SBM (*Subnet Bandwidth Management*).

3.1 Integrované služby

Mechanizmus integrovaných služieb pracuje na princípe rezervácie pásma a vychádza z modelu, ktorý pred samotným prenosom dát zaistí potrebnú kvalitu prenosového kanálu. Podporuje typické multimediálne aplikácie a poskytuje garantovanú službu i službu s riadením záťaže. Model integrovaných služieb sa stará hlavne o čas doručenia jednotlivých paketov. Zdieľanie prostriedkov je riešené samostatne pre každý dátový tok. Model obsahuje prvky pre určenie dôležitosti jednotlivých paketov v rámci daného toku (v prípade nutnosti sa zahadzujú menej dôležité) a spôsob dohovoru siete a užívateľa.
Architektúra integrovaných služieb rozlišuje nasledujúce kategórie aplikácií [8]:

Pružné aplikácie – bez požiadavku na doručovanie. Do tejto kategórie patria aplikácie, ktoré využívajú ku komunikácii TCP protokol. Nekladú si požiadavky na obmedzenie oneskorenia alebo kapacitu spojenia. Príkladom je el. pošta, http protokol, atď.
Real Time Tolerant (RTT) aplikácie – aplikácie požadujúce obmedzenie na maximálne oneskorenie. Občasná strata paketov je prijateľná. Príkladom sú aplikácie využívajúce ukladanie do vyrovnávacej pamäte, ktoré pred aplikáciou skryjú stratu paketov.
Real Time Intolerant (RTI) aplikácie – aplikácie požadujúce minimálnu odozvu a rozptyl oneskorenia (jitter). Príkladom sú video-konferenčné aplikácie..

Aplikácia oznámi v danej sieti svoje požiadavky na prenos dát vo forme požadovaných parametrov kvality služieb (viď kapitola 2.3) a očakáva, že tieto budú dodržané po celú dobu trvania spojenia. Sieť následne rozhodne o tom, či disponuje sieťovými prostriedkami pre požadované parametre aplikácie. Táto funkcia je označovaná ako riadenie prístupu (admission control). V prípade, že sieť nemôže požiadavkám vyhovieť, spojenie nie je povolené a aplikácia môže požiadať o nové spojenie s nižšími nárokmi na kvalitu služby, alebo prenos ukončiť.

V opačnom prípade musí sieť informovať všetky prvky komunikačnej cesty, aby pre dané spojenie rezervovali odpovedajúci objem sieťových prostriedkov, ako šírka pásma spojov, alebo kapacita fronty smerovačov. K rezervácii prostriedkov je využitý rezervačný protokol RSVP (Resource reSerVation Protocol), ktorý je však pomerne zložitý a predstavuje významnú réžiu pri riadení chodu siete.

Pre riadenie siete sa používajú nasledujúce stratégie [8]:

- Udržovanie stavu vyžiadaných pripojení
- Dohľad a úprava dátového prenosu
- Predchádzanie stavu zahltenia
- Správa predchádzania alebo odstránenia stavu zahltenia
- Mechanizmus sledovania výkonnosti linky

3.1.1 Triedy služieb

K zaisteniu obsluhy aplikácií má RSVP k dispozícii nasledujúce triedy služieb [7]:
Zaručená služba – zaručuje hodnotu maximálneho oneskorenia pri danej prenosovej rýchlosti a to, že paket nebude zahodený v prípade preplnenia fronty niektorého zo smerovačov. Cieľom však nie je minimalizovať rozdiely v oneskorení.
Služba s riadením záťaže – pre dátový tok zaisťuje rovnakú kvalitu služieb, akú by bola schopná zaistiť sieť typu best-effort v nezaťaženom stave. Nezaručujú sa žiadne vlastnosti týkajúce sa oneskorenia prenosu. Tento typ služby zaisťuje, že dohodnuté dátové toky nezahltia sieťové prvky, a pakety nesplňujúce vopred dohodnuté podmienky sú spracované na úrovni služby best-effort.

Referenční sieť technológie IntServ obsahuje nasledujúce prvky [9]:

Plánovač paketov – riadi prenos paketov. Môže podporovať rôzne typy front.
Vstupnú kontrolu (Admission control) – rozhoduje, či možno novovzniknutému dátovému toku garantovať požadovanú kvalitu služby bez toho aby to ovplyvnilo ostatné.
Klasifikátor (Classifier) - triedi pakety do skupín pre určenie úrovne služby.
Protokol pre rezerváciu prostriedkov (RSVP) – stará sa o vznik a udržovanie informácií o kvalite služby daného toku po celej dĺžke prenosu.

Základnou nevýhodou modelu IntServ je, že vyžaduje prispôsobenie všetkých aplikácií signalizácii RSVP a spoluprácu sieťových prvkov, ktoré musia každý dátový tok spracovať samostatne. To kladie značné nároky na výkon jednotlivých uzlov. Z toho vyplýva, že model je nepraktický pre široké využitie v sieti Internet.

3.2 Rezervačný protokol RSVP

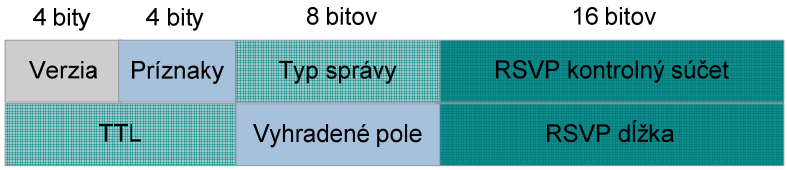
U best effort modelu môže aplikácia odosielať pakety, kedy sa jej zachce. Naproti tomu, architektúra integrovaných služieb vyžaduje od aplikácie zriadenie rezervácie sieťových prostriedkov skôr než začne samotný prenos dát. Táto činnosť vyžaduje protokol pre zaistenie rezervácie prostriedkov v danej sieti. Výsledkom je protokol RSVP vyvinutý organizáciou IETF, ktorý je využívaný koncovými stanicami k zasielaniu služobných požiadaviek do siete a smerovačmi v sieti k vytvoreniu rezervácie prostriedkov medzi odosielateľom a príjemcom dát výhradne v jednom smere [1]. Príjemcovia sú zodpovedný za rozhodovanie o tom, aké prostriedky budú vyhradené a inicializáciu rezervácie. Požiadavky putujú od príjemcu k odosielateľovi a vytvoria rezervačný strom.

RSVP protokol bol navrhnutý ako doplnkový protokol k existujúcej sade IP protokolu a je schopný pracovať so súčasnými a budúcimi smerovacími protokolmi.

Protokol využíva k obnove stratených paketov vlastný obnovovací mechanizmus. V prípade silného zahltenia linky môže značná strata správ spôsobiť zlyhanie rezervácie prostriedkov. V ideálnom prípade sú RSVP správy doručované pri zahltení prioritne.

3.2.1 Formát a typy RSVP správ

Každá RSVP správa začína spoločnou hlavičkou, po ktorej nasledujú dáta zložené zo série RSVP objektov premennej dĺžky. Formát hlavičky je možno vidieť na obrázku č.1 [1].



Obr. 1: Hlavička RSVP správy

Kontrolný súčet RSVP je podobný tomu, ktorý sa využíva v TCP, UDP, IP protokoloch. 4-bitové pole príznakov a 8-bitové vyhradené pole nie sú definované, TTL pole zaznamenáva hodnotu TTL využívanú odosielateľom IP hlavičky. Celková dĺžka správy v bajtoch vrátane objektov premenlivej dĺžky vyjadruje dĺžku RSVP správy.

Jednotlivé typy správ sú popísané v tab. 3.1. V tabuľke je možné vidieť 7 typov definovaných správ, ktoré určujú funkciu správy [1].

Typ správy	Popis
PATH	Path správa
RESV	Rezervačná správa
PATHErr	Indikácia chyby v reakcii na správu PATH
RESVErr	Indikácia chyby v reakcii na správu RESV
PATHTear	Path Tear správa
RESVTear	Resv Tear správa
RESVConf	Resv Confirmation správa

Tab. 3.1: Typy RSVP správ

Protokol obsahuje niekoľko druhov RSVP správ, ale najdôležitejšie pre jeho činnosť sú dva typy správ; PATH a RESV správy [1].

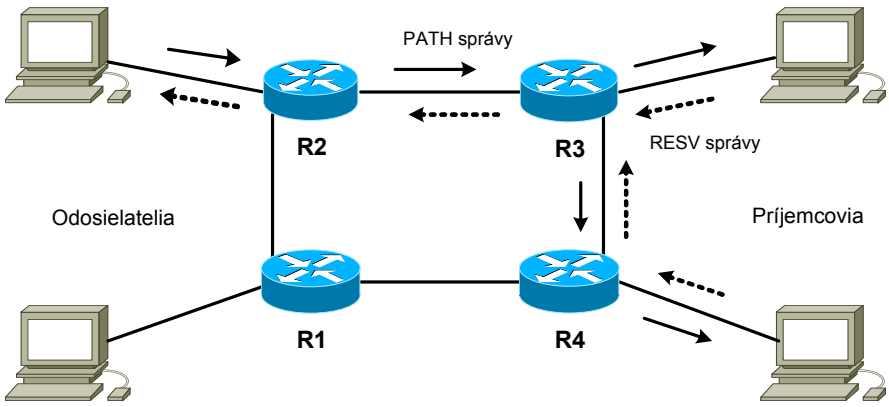
PATH správy – sú odosielané unicastovou alebo multicastovou linkou, ktorou sú nasledovne prenášané dátové pakety. PATH správa predurčí stav linky u každého sieťového uzla na danej trase.
Parameter stavu linky zahŕňa vždy aspoň unicastovú adresu predchádzajúceho uzlu, ktorý je používaný k smerovaniu príslušných RESV správ v opačnom smere. PATH správa obsahuje informáciu o predošlom uzle, šablónu odosielateľa a parametre odosielateľa TSpec a ADSpec. Šablóna odosielateľa obsahuje informácie, ktoré jednoznačne identifikujú dátový tok a môže špecifikovať iba IP adresu odosielateľa a voliteľne jeho UDP/TCP port.
Parameter TSpec charakterizuje prevádzku generovanú odosielateľom. Môže byť použitý pri rozhodovaní o tom aká veľka časť prostriedkov by mala byť rezervovaná a ako súčasť vstupu prijímacieho riadiaceho systému. Parameter ADSpec je voliteľným prvkom PATH správ a je používaný k prenosu OPWA

RESV správy – su rezervačnými požiadavkami posielanými príjemcom po spätnej ceste odosielateľovi. RESV správa obsahuje informácie o spôsobe rezervácie a špecifikuje objekt dátového toku. Parameter Flowspec udáva požadovanú kvalitu služieb a parametre pre plánovanie paketov. V RESV správe môže prenášať požadovanú triedu služby a dve sady prídavných parametrov:

Rspec, ktorý definuje požadovanú kvalitu služby a Tspec, popisujúci dátový tok. Presný formát závisí na tom, či prijímateľ vyžaduje riadenú záťaž služby alebo garantovanú službu. Garantovaná služba vyžaduje obidva parametre Rspec a Tspec, riadená záťaž služby iba Tspec.

3.2.2 Prehľad činnosti RSVP

RSVP odosielateľ pošle PATH správu s rezervačnými informáciami a táto je spracovaná v každom uzle prenosovej cesty dátového toku vyžadujúceho danú úroveň kvality služieb. PATH správy slúžia k šíreniu informácii o prevádzkových prostriedkoch a nastavujú potrebný stav pre RESV správy pre zistenie ako dosiahnuť odosielateľa zo strany príjemcu. RSVP príjemca následne vygeneruje RESV správu a pošle ju opačným smerom k odosielateľovi. Tým si vyžiada rezerváciu v každom sieťovom uzle na danej ceste. Po prijatí RESV správy môže odosielateľ začať posielať pakety po rezervovanej linke. Nákres základných RSVP operácií možno vidieť na obr. 2 [1].



Obr. 2: Základné operácie v RSVP sieti

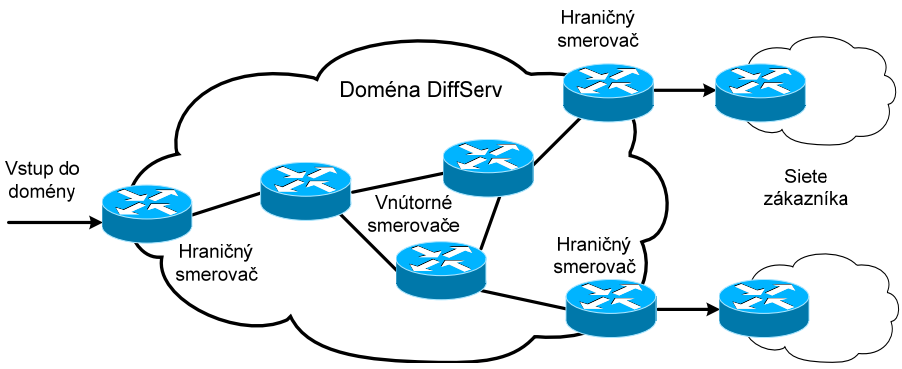
3.3 Diferencované služby – DiffServ

U mechanizmu diferencovaných služieb neoznamuje aplikácia sieti svoje požiadavky na kvalitu služieb a teda nevyžaduje existenciu akýchkoľvek rezervačných protokolov. Toto je základná vlastnosť, ktorou sa tento mechanizmus odlišuje od Integrovaných služieb. Na sieť nie sú kladené žiadne vysoké nároky, pretože jednotlivé smerovače neudržujú žiadne stavové informácie o spojoch v sieti. Model DiffServ je založený na agregácii dátových tokov do malého počtu tried CoS (Class of Service). Definíciou pravidiel v smerovači možno týmto triedam priradiť určitú kvalitu služieb. Zaradenie paketov do jednotlivých tried sa definuje v hlavičke IP protokolu.

Implementácia kvality služieb sa zaisťuje označením každého vstupného paketu značkou, ktorá určuje poskytovanú triedu prenosu. Označkovanie prebieha len na vstupe do siete a počas prenosu nedochádza k zmene značky. Jednotlivé smerovače nazrú na obsah priradenej značky a podľa toho riadia spôsob spracovania daného paketu. Diferencované služby tak nevyžadujú, aby smerovače udržiavali informáciu o požadovaných parametroch na spojenie, ale udržujú si len informácie o triedach prenosu. Mechanizmus DiffServ je súčasťou jednotlivých koncových staníc i celej siete.

3.3.1 Klasifikácia a značkovanie paketov

Z hľadiska diferencovaných služieb sa komunikačná sieť delí na oblasti so samostatnou správou služieb [2], tzv. DiffServ (DS) domény (viď obr.3) [1]. Tie zaručujú jednotnú administráciu a rovnaké spracovanie paketov v rámci jednotlivých domén.



Obr. 3: DiffServ doména

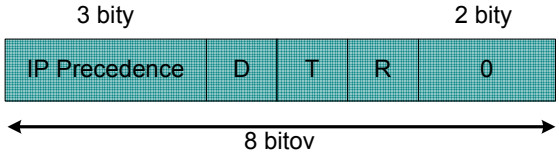
Doména obsahuje dva druhy smerovačov [10].

Vnútorné smerovače – zaisťujú spojenie vo vnútri DiffServ domény. Neprevádzajú žiadnu klasifikáciu paketu a zaobchádzajú s ním podľa príslušnej značky.

Hraničné smerovače – ležia na rozhraní jednotlivých DiffServ domén. V závislosti od funkcie možno rozdeliť na vstupné (ingress) smerovače, zaisťujúce značkovanie paketov pri vstupe do domény a výstupné (egress) smerovače, zaisťujúce odobratie značky pri odchode z domény. Ak sú prepojené dve DiffServ domény, pracuje tento typ smerovača súčasne ako výstupný smerovač jednej domény a vstupný domény druhej. V súvislosti s prechodom medzi Diffserv doménami a značkovaním paketov súvisí označenie „hranica dôveryhodnosti“.

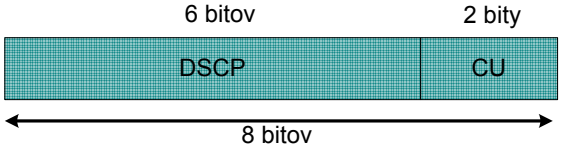
Klasifikácia paketov prebieha vo vstupnom smerovači na základe IP adresy odosielateľa alebo príjemcu, čísiel portov apod. Pakety môžu byť klasifikované už pri odosielaní aplikáciou, prvý vstupný smerovač môže túto značku pozmeniť alebo zachovať. Značenie paketov závisí od použitého protokolu alebo technológie. Značka je obsiahnutá v hlavičke protokolu, alebo je doplnená mimo paket. V hlavičke sa značka nachádza u protokolu IPv4 v poli „Typ služby“ – ToS (Type of Service) alebo v poli „Trieda prevádzky“ – TC (Traffic Class) u prenosového protokolu IPv6 [8].

V 8-bitovom poli ToS (viď obr.4) sa pôvodne určovala priorita pomocou 3 bitov IP Precedence, ktoré umožňovali zaradiť prevádzku do jednej z 8 tried.



Obr. 4: Pole ToS hlavičky IP

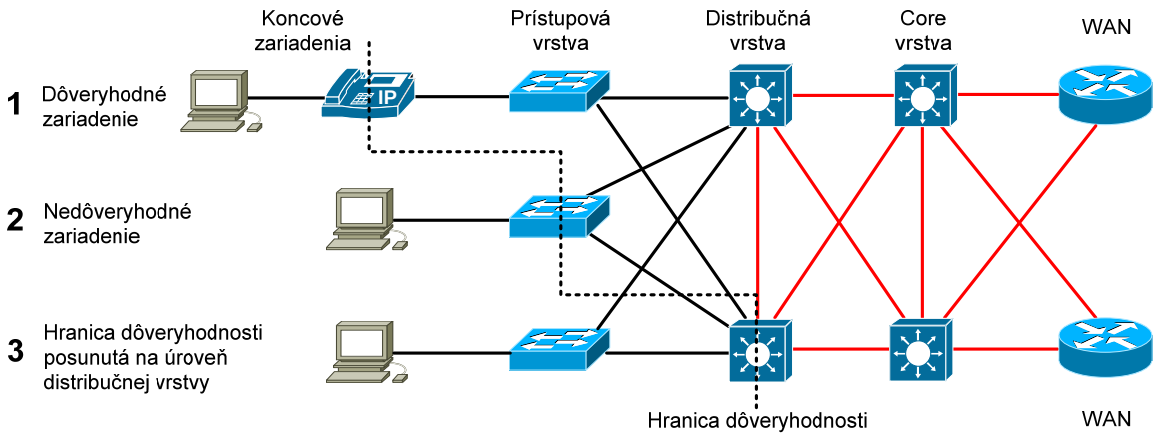
V súčasnosti sa časť IP Precedence poľa ToS nahradzuje hodnotou DSCP (Diferentiated Service Code Point), ktoré využíva 6 bitov poľa ToS (viď obr. 5) a umožňuje tak zaradiť prevádzku do jednej zo 64 definovaných tried a určiť spôsob zaobchádzania s paketom. 2 zvyšné bity položky ToS ostali vyhradené do budúcna.



Obr. 5: DS pole hlavičky IP

3.3.2 Hranica dôveryhodnosti

Hranica dôveryhodnosti je bod v sieti, kde sa začína akceptovať značkovanie na základe CoS alebo DSCP značiek. Predošlé nastavené značky sú v tomto bode prepísané novými. Prevedenie hranice je spravidla čo najbližšie koncovému zariadeniu, tak ako to znázorňuje obrázok č.6 [6].



Obr. 6: Hranica dôveryhodnosti

Definícia hranice dôveryhodnosti záleží na schopnostiach koncových zariadení, ktoré sú pripojené k prístupovej vrstve LAN siete. Preto sa rozlišujú 3 hlavné typy koncových zariadení:

- Dôveryhodné zariadenie
- Nedôveryhodné zariadenie
- Podmienené dôveryhodné zariadenie

Dôveryhodné zariadenie

Zariadenie, ktoré sa vyznačuje schopnosťou a inteligenciou značkovať sieťovú prevádzku príslušnou CoS a DSCP hodnotou. Ďalej sa vyznačuje schopnosťou preznačkovať tok paketov, ktorý bol označkovaný predošlým nedôveryhodným zariadením. K typickým dôveryhodným zariadeniam patria analógové ústredne, IP telefóny, IP videokonferenčné stanice, ústredne a systémy, servery v datacentrách, bezdrôtové prístupové body a bezdrôtové IP telefóny.

Nedôveryhodné zariadenie

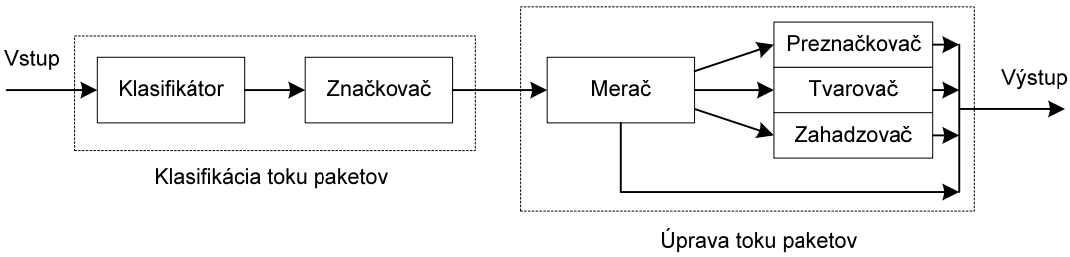
Z hľadiska zabezpečenia požadovanej kvality služieb v sieti je nevhodné zaradiť niektoré servery a všetky užívateľské koncové stanice do skupiny dôveryhodných zariadení. Novšie operačné systémy totiž umožňujú pomerne jednoducho označkovať výstupnú prevádzku nevhodnými CoS alebo DSCP hodnotami. To môže mať silný dopad na úroveň služieb v sieti s viacerými užívateľmi.

Podmienečne dôveryhodné zariadenie

K takýmto zariadeniam sa zaraďujú niektoré IP telefóny aj napriek tomu, že patria k dôveryhodným zariadeniam. Ak však užívatelia využívajú svoje telefóny v spojení s častými presunmi, dochádza k zmene pripojenia IP telefónu k prvkom prístupovej vrstvy. Môže tak nastať problém, že užívateľ pripojí svoj telefón na port, kde bolo pripojené nedôveryhodné zariadenie a preto sa odporúča zaradiť ho do skupiny podmienečne dôveryhodných zariadení.

3.3.3 Referenčný model architektúry DiffServ

Referenčný model sa skladá z niekoľkých blokov a je ho možno vidieť na obr.č.7 [1], [6]. Prvky úpravy prevádzky sa nachádzajú vo vnútri domény vstupných a výstupných uzlov.



Obr. 7: Rozloženie prvkov modelu DiffServ

Klasifikátor (Classifier) – zaraďuje jednotlivé pakety do určitých skupín, podľa príslušnosti k dátovému toku, alebo podľa množiny hodnôt. Existujú 2 druhy klasifikátorov:

- Združené zaobchádzanie – BA (Behaviour Agregate) – klasifikuje pakety len podľa DSCP. Tento typ klasifikátora je väčšinou používaný v prípadoch, keď prichádzajúci paket je už označený iným sieťovým prvkom.
- Viacpoložkový klasifikátor – MF (Mutlifield) – vyberá pakety podľa jednej, alebo viacerých kombinácií položiek obsiahnutých v hlavičke paketu.

Klasifikátor rozlišuje typ trafficu v závislosti od ACL (Access control list), vstupného rozhrania, použitého protokolu, class-mapy alebo podľa konfigurácie CoS, DSCP a IP Precedence. Pakety možno tiež klasifikovať samotnou aplikáciou, ktorá pakety generuje.

Značkovač (Marker) – v závislosti od zaradenia paketu do niektorej z tried priraďuje paketu značku podľa stanovených pravidiel. Proces spočíva v pridelení DS časti DSCP poľa hlavičky paketu. V závislosti od stavu merača môže značkovať všetky pakety, alebo len určité.

Merač parametrov dátového toku – jeho funkciou je prieskum dátového toku a podľa nastavených parametrov pre prenos a úpravu prevádzky rozhodne o príslušnej triede zaradenia paketu.

Tvarovač (Shapper) – slúži k zavedeniu takého oneskoreniu paketov v dátovom toku, aby bol dodržaný dopravný profil prednastavený parametrom úpravy prevádzky. K úprave sa používa metóda nazvaná „token bucket“. Metódu možno parametrizovať dvoma spôsobmi a to kapacitou výstupnej linky alebo kapacitou výstupnej fronty. Tvarovač má obmedzenú veľkosť vlastnej vyrovnávacej pamäte a ak dôjde k zahlteniu, automaticky nové pakety zahadzuje.

Zahadzovač (Dropper) – zahadzuje niektoré alebo všetky pakety dátovom toku, aby bol dodržaný dopravný profil prednastavený parametrom úpravy prevádzky. K zahadzovaniu dochádza pri splnení určitej podmienky, napr. vyčerpanie kapacity fronty, alebo prekročení určitého objemu prichádzajúcich dát.

3.3.4 Spracovanie paketov

Spracovanie paketov smerovačom na základe značky paketu sa nazýva per-hop-behaviour (PHB). V súčasnej dobe sú štandardizované dve PHB - urýchlené doručenie (EF) a zaistené doručenie (AF). U Diffserv domény môže dôjsť k implementácii aj iných spôsobov spracovania paketov. Nezaradené toky paketov a základná trieda (default-class) sa spracúvajú metódou Best effort, ktorá je vhodná pre nenáročné dátové toky.

Urýchlené predávanie – EF (Expedited forwarding)
Každý smerovač v Diffserv doméne odosiela pakety zaradené do EF PHB priemernou rýchlosťou aspoň rovnou stanovenej rýchlosti. Priemerná rýchlosť sa meria v akomkoľvek časovom intervale, ktorý je dlhší alebo rovný dobe potrebnej pre odoslanie paketu maximálnej dĺžky stanovenou rýchlosťou [8], [10]. EF PHB je vhodný pre implementáciu virtuálneho prenajatého okruhu. Ideálne pre malé dátové pásmo, alebo nízke oneskorenie

Zaručené predávanie – AF (Assured forwarding)
Umožňuje zaradiť pakety do jednej zo 4 tried. Každej triede je v smerovačoch pridelený určitý objem prostriedkov (veľkosť vyrovnávacej pamäte, kapacita výstupnej linky). V rámci každej triedy je každému paketu priradená jedna z troch priorít zahodenia paketu, ku ktorému môže dôjsť v prípade zahltenia. Smerovač musí odoslať paket s nižšou hodnotou priority s rovnakou alebo vyššou pravdepodobnosťou ako paket majúci vyššiu hodnotu priority [8], [10]. AF PHB sa používa pre implementáciu služieb, u ktorých je požadovaná voliteľná úroveň kvality prenosu.

3.3.5 Fronty a ich radenie

Pri správnej funkcii úpravy premávky na vstupnom smerovači Diffserv domény by nemalo na vnútorných smerovačoch dochádzať k vyčerpaniu kapacity front. Vstupné a vnútorné smerovače implementujú požadovaný spôsob spracovania paketov (PHB) a následne dochádza k úprave prevádzky. Jednotlivé PHB sú typicky realizované za použitia viacerých front s určitým algoritmom pre zaraďovanie paketov do front, výber paketov z front a ich odoslanie. Paket je vložený do jednej z front na základe svojej značky.

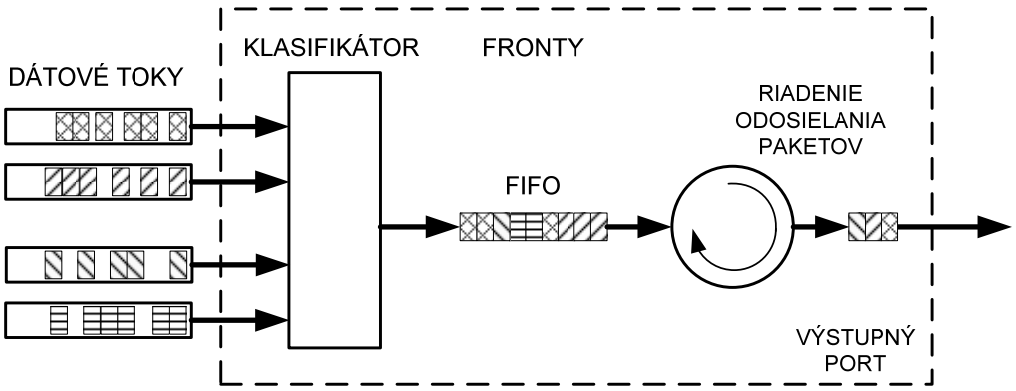
Medzi základné metódy spracovania front patrí podľa lit. [11]:

- Fronta s obsluhou typu FIFO
- Fronta s prioritnou obsluhou – PQ
- Fronta so spravodlivou obsluhou – FQ
- Fronta s váženou cyklickou obsluhou – WRR
- Fronta s váženou spravodlivou obsluhou – WFQ
- Fronta s váženou spravodlivou obsluhou riadenou podľa tried – CBWFQ

Jednotlivé metódy sa líšia spôsobom obsluhy fronty.

Fronta s obsluhou typu FIFO

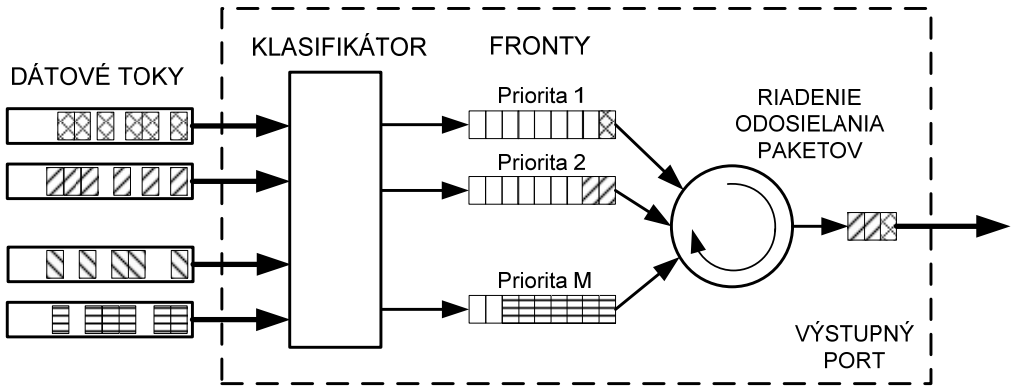
Fronta FIFO (First In First Out) je východzí typ fronty a dodnes sa používa v prípade, že nie je implemtentovaný nijaký špecifický algoritmus odosielania paketov. Jej najväčšou výhodou je jednoduchá implementácia a princíp spracovania paketov na výstup spočíva v ich zaradení do poradia v akom boli prijaté. Z princípu obsluhy vyplýva, že so všetkými paketmi zaobchádza rovnakým spôsobom a je teda vhodná predovšetkým pre sieťovú prevádzku „best effort“. Jej veľkou nevýhodou je však neschopnosť rozlišovať jednotlivé triedy služieb. Zahltenie sieťového uzlu má tak dopad na všetky triedy rovnakým podielom. V prípade kombinovanej UDP a TCP prevádzky je fronta FIFO príznačná vlastnosťou zvýhodnenia UDP prenosu z dôvodu absencie mechanizmov riadenia priepustnosti u tohto typu prevádzky.



Obr. 8: Fronta s obsluhou typu FIFO

Fronta s prioritnou obsluhou – PQ

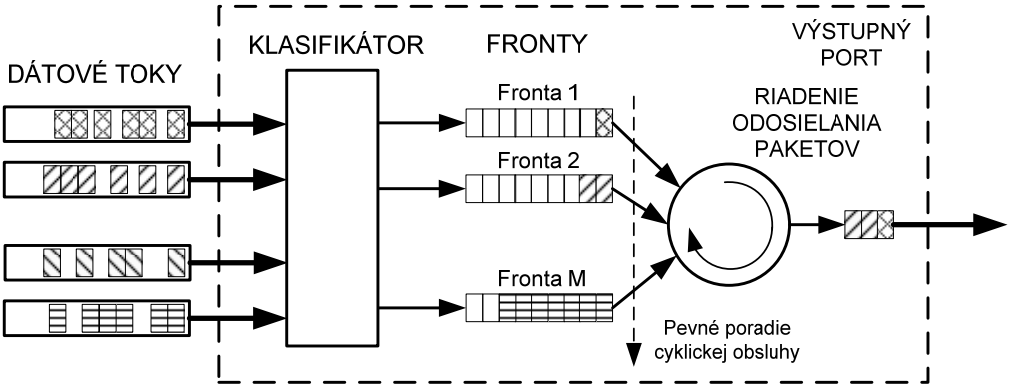
Jednotlivé fronty majú priradenú určitú prioritu, ktorá je vždy iná.. Ako vyplýva z názvu, princíp riadenia spočíva v obsluhe jednotlivých front na základe týchto priorít. Prednostne sú odoslané pakety z fronty s najväčšou prioritou a až po jej vyprázdnení sa dostane na rad fronta s nižšou prioritou. Podobne ako u fronty FIFO je jej obrovskou výhodou jednoduchosť algoritmu riadenia. Jej veľkou nevýhodou je však možnosť úplného potlačenia fronty s najnižšou prioritou, kedy sú dáta pozdržané natoľko, že dôjde k rozpadu spojenia, alebo ich vysielacia stanica považuje za stratené, prevedie ich znovu vyslanie a tým ešte zvýši zaťaženie siete. Metódu možno použiť k implementácii spracovania paketov urýchleným predávaním (EF PHB), kedy jedna fronta slúži EF PHB a druhá pre prevádzku typu „best effort“. Prioritný systém front sa tak využíva k prenosu hlasu alebo videa v reálnom čase.



Obr. 9: Fronta s prioritnou obsluhou – PQ

Fronta so spravodlivou obsluhou – FQ

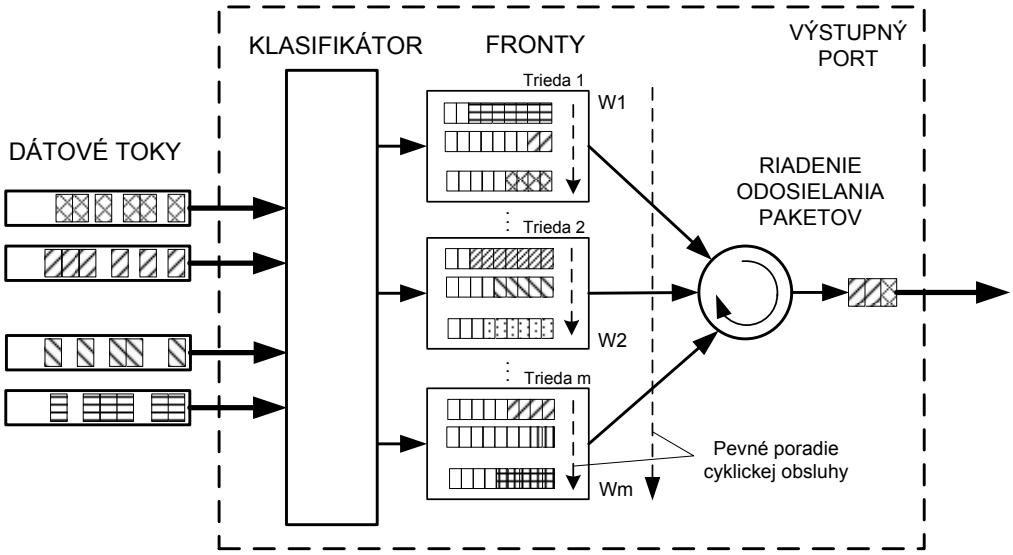
Ide o spôsob riadenia paketov do jednotlivých front podľa dátového toku. Implementácia systému fronty sa vyznačuje pomernou jednoduchosťou, pretože nevyžaduje algoritmus pre vyhradenie šírky pásma jednotlivým frontám. Ak dôjde k definícii ďalšej prevádzky s riadeným zaobchádzaním, jednoducho sa pridá ďalšia fronta, ktorá ju spracuje. K nevýhodám tejto metódy patrí vlastnosť, že pri spracovaní nezohľadňuje veľkosť jednotlivých paketov a teda rovnaký počet rôzne veľkých paketov vo frontách bude spracovaný rozdielne. Ďalej sa metóda vyznačuje pevnou šírkou pásma pridelenou jednotlivým frontám. V prípade, že jednotlivé dátové toky majú nejednotné nároky na šírku pásma, uvedená metóda nie je schopná rozdeliť dostupnú šírku pásma podľa požiadaviek..



Obr. 10: Fronta so spravodlivou obsluhou – FQ

Fronta s váženou cyklickou obsluhou – WRR

Metóda fronty s váženou cyklickou obsluhou bola vyvinutá za účelom odstránenia nedostatku pevného rozdelenia šírky pásma jednotlivým frontám ako je tomu o mechanizmu fronty so spravodlivou obsluhou. Systém fronty WRR zaisťuje jednotlivým triedam služieb rôznu šírku pásma na základe váhovej hodnoty priradenej jednotlivým triedam. Súčet všetkých váhových hodnôt musí odpovedať hodnote celkovej dostupnej šírky pásma. Odosielanie paketov v rámci jednej triedy dátového toku je následne riadené metódou fronty so spravodlivou obsluhou. Metóda WRR sa vyznačuje použitím dvojúrovňového plánovania Round-Robin. Prvá úroveň sa vyznačuje výberom konkrétnej triedy z celkového počtu a druhá slúži k výberu určitej fronty v rámci danej triedy.

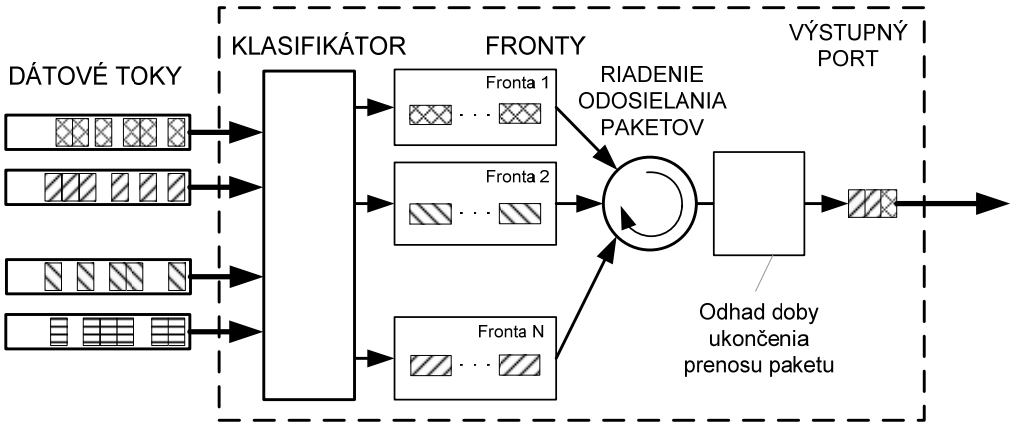


Obr. 11: Fronta s váženou cyklickou obsluhou – WRR

Fronta s váženou spravodlivou obsluhou – WFQ

U tejto metódy je priebežne obslúžená každá fronta, pričom všetky fronty majú rovnakú prioritu. Jednotlivým frontám je pridelená časť kapacity výstupnej linky, odpovedajúca váhovej hodnote priradenej ku každej fronte. Systém fronty s váženou spravodlivou obsluhou bol vyvinutý za účelom eliminácie vplyvu dĺžky paketu na dostupnú šírku pásma.

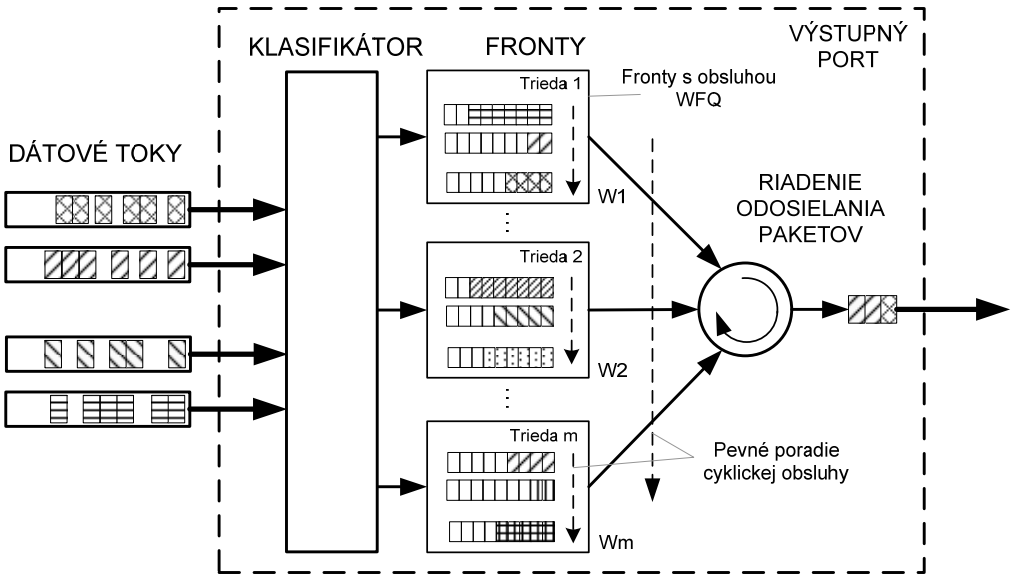
Ak nie je kapacita určitej fronty obsadená, môže byť využitá inou frontou. Mechanizmus ďalej využíva model výpočtu času, kedy najneskôr má byť prichádzajúci paket odoslaný. Tento výpočet vychádza z počtu paketov umiestených vo fronte, do ktorej by mal byť paket zaradený a z rýchlosti obsluhy danej fronty. Po skončení obsluhy paketov sa určuje, ktorý z paketov čakajúcich vo frontách má byť obslúžený ako ďalší v poradí.



Obr. 12: Fronta s váženou spravodlivou obsluhou – WFQ

Fronta s váženou spravodlivou obsluhou riadenou podľa tried – CBWFQ

Metóda fronty s váženou spravodlivou obsluhou riadenou podľa tried sa vyznačuje rovnakými vlastnosťami ako metóda fronty s váženou cyklickou obsluhou. Sieťová prevádzka je rozdelená do definovaného počtu tried a šírka pásma je určená na základe váhovej hodnoty. Rozdiel však spočíva v odlišnosti obsluhy dátových tokov v rámci jednotlivých tried. Tento mechanizmus využíva systém obsluhy WFQ, na rozdiel od WRR, ktoré používa systém FQ.



Obr. 13: Fronta s váženou spravodlivou obsluhou podľa tried – CBWFQ

3.3.6 Správa front

Úlohou aktívnej správy front je zabrániť úplnému zahlteniu vyrovnávacej pamäte v jednotlivých sieťových prvkoch. Technológie aktívnej správy front predstavujú pokročilé mechanizmy riadenia priepustnosti paketov. Pracujú na princípe detekcie vzniku zahltenia ešte skôr než k samotnému zahlteniu dôjde [11].

Medzi základné metódy aktívnej správy front patrí:

- Predčasná detekcia s náhodnou reakciou – RED
- Predčasná detekcia s váženou náhodnou reakciou – WRED
- Explicitná signalizácia zahltenia – ECN

Tieto mechanizmy postupne nahradzujú staršiu technológiu označovanú ako pasívna správa front, ktorej základom je metóda „Tail Drop“.

Tail Drop

Triviálne riešenie spočívajúce v zahodení príchodzích paketov, ktoré nie je možné zaradiť do vyrovnávacej pamäte. Koncová stanica nie je žiadnym spôsobom informovaná o zahodení a nedochádza ani k opätovnému preposlaniu. Je len na nej aby detekovala stratu paketov.

Tail Drop zahadzuje pakety až keď sú vyčerpané všetky sieťové prostriedky. V danom moente to znamená, že prvok neakceptuje žiadne ďalšie pakety, až dokiaľ sa fronta neuvoľní. Plná fronta tak blokuje ďalšie pakety v prenose, ktorré sú automaticky zahadzované. V prípade, že sú sieťové prostriedky značne vyčerpané dlhší čas, koncové stanice neinterpretujú takýto stav zahltenia až do chvíle, kým nedôjde úplnému zahlteniu fronty. V prípade sieťovej prevádzky založenej na protokole TCP je Tail drop veľmi nevhodnou technikou. Ak dochádza k stratám paketov, automaticky sa zníži rýchlosť odosielania paketov a vtedy budú pakety jednotlivých TCP spojení prechádzajúcich určitým smerovačom zahodené aj napriek zníženej prenosovej rýchlosti. Toto vedie k javu nazvanému globálna TCP synchronizácia. Priemerné využitie skutočnej kapacity výstupných portov sa tak drasticky znižuje.

RED – Random early detection

Metóda umožňuje smerovačom proaktívne reagovať na možnosť zahltenia priebežným pozorovaním napĺnenia výstupnej fronty. V prípade blížiaceho sa zahltenia začne náhodne zahadzovať pakety vo frontách a nie len z konca fronty.

Táto metóda sa používa predovšetkým na chrbticových spojoch (backbone) smerovačoch vo veľkých sieťach. Ak dôjde k zahodeniu jedného z paketov odošle smerovač informáciu o zahodení. Metóda by mala spolupracovať s algoritmom kontroly toku a technikou predchádzania zahlteniu, ktorá je súčasťou protokolu TCP. Týmto sa predchádza zahlteniu výstupnej fronty a globálnej synchronizácii protokolu TCP. To však platí len pri TCP spojení. Na pakety protokolu UDP to nemá žiaden vplyv a preto sa mechanizmus javí ako nevhodný, z hľadiska riadenia dátového toku.

WRED – Weighted random early detection

Metóda rozširuje základný mechanizmus RED o viaceré triedy zahadzovania paketov. Každá trieda má nastavený určitý profil pre danú frontu, podľa kality služby, ktorú sa snažíme zabezpečiť. Naviac umožňuje aplikovať viacero profilov v rámci jednej fronty. Okrem samotného zahadzovania paketov využíva značkovanie paketov, ktoré slúži k určeniu pravdepodobnosti zahodenia daného paketu na základe značky pridelenej pri klasifikácii.

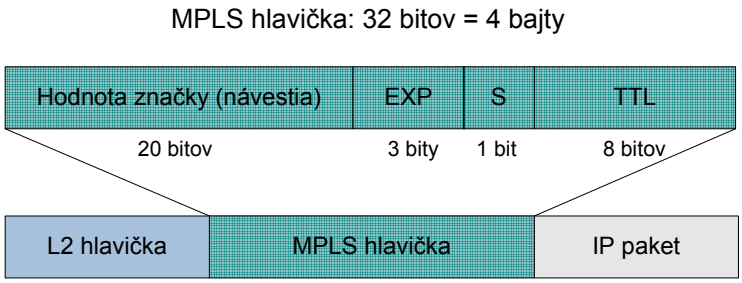
ECN – Explicit Congestion Notification

Ide o pokusné rozšírenie TCP protokolu, ktoré využíva posledné dva bity poľa DS. Nastavením týchto bitov u náhodne vybraných paketov informuje koncové uzly o možnosti zahltenia. Pracuje však len so segmentami protokolu TCP, datagramy UDP protokolu nie sú nastavované a takáto prevádzka nie je ovplyvnená žiadnym spôsobom. V prípade zahltenia sieťových prostriedkov sú pakety podobne ako u metódy Tail drop zahodené.

3.4 Prepojovanie paketov s návestím - MPLS

Mechanizmus MPLS (Multiprotocol Label Switching) je založený na koncepte prepínania štítkov (značiek). Do každého dátového paketu je vložený nezávislý a unikátny štítok, ktorý je využívaný k smerovaniu daného paketu sieťou. Štítok je v podstate krátkou verziou informácií, ktoré sú obsahom MPLS hlavičky dátového paketu, viď obr. č. 14 [13]. Hlavná myšlienka MPLS spočíva v tom, že použitím štítku k rozpoznaniu nasledujúceho uzlu sa podstatne zjednoduší smerovací proces (znížením správy prenosu dôjde k zvýšeniu výkonu) a zároveň sa zvýši jeho pružnosť. U smerovačov tak dôjde k odľahčeniu a pôsobia ako jednoduché prepínače [12].

Signalizáciu spojov a šírenie štítkov v MPLS sieti zabezpečuje niekoľko signalizačných protokolov, vrátane LDP protokolu (Label Switchning Protocol), RSVP a RSVP-TE protokolu (Tunneling Extensions). Najčastejšie používaným signalizačným protokolom je LDP. Definuje rad metód pre výmenu štítkov smerovačmi a mapovanie toku informácií. Zároveň je použitý pre stanovenie trasy smerovania dát.



Obr. 14: Hlavička MPLS

Je však dôležité pochopiť rozdiel spôsobu smerovania dát v MPLS a bežných IP sieťach. Klasický IP paket je smerovaný na základe cieľovej IP adresy, podľa ktorej smeruje každý smerovač v sieti daný paket na ďalší uzol. K tomu sú využívané smerovacie protokoly, ktoré sú navrhnuté tak, aby našli najkratšiu cestu sieťou s úvahou aj ďalších faktorov, ako sú latencia, alebo zápchy v určitých spojoch. MPLS je spojovo orientovaná architektúra, ktorá stavia na IP sieťach, kombinuje inteligenciu smerovania s vysokým výkonom prepínania a otvára tak nové možnosti pre správu prevádzky IP sietí. Súčasne poskytuje

primeranú úroveň bezpečnosti a znižuje potrebu šifrovania vo verejnej IP sieti. K jeho ďalším výhodám patrí lepšia škálovateľnosť VPN sietí (Virtual Private Network).

Mechanizmus je v niektorých ohľadoch, akými je napr. značkovanie prevádzky na vstupných hraniciach siete a odobratím značky na výstupnej hranici MPLS siete, podobný diferencovaným službám. Tie však používajú značkovanie k určeniu priority v rámci smerovača. MPLS je na rozdiel od ostatných mechanizmov implementovaný len v sieťových prvkoch (smerovačoch) a nie je tak súčasťou koncových staníc. Mechanizmus z hľadiska referenčného modelu OSI nemožno jednoducho zaradiť. Nemá vlastné sieťové adresovanie a k smerovaniu využíva rôzne sieťové protokoly a technológie. V princípe pracuje medzi druhou – linkovou a treťou – sieťovou vrstvou, často sa však označuje ako technológia vrstvy 2+.

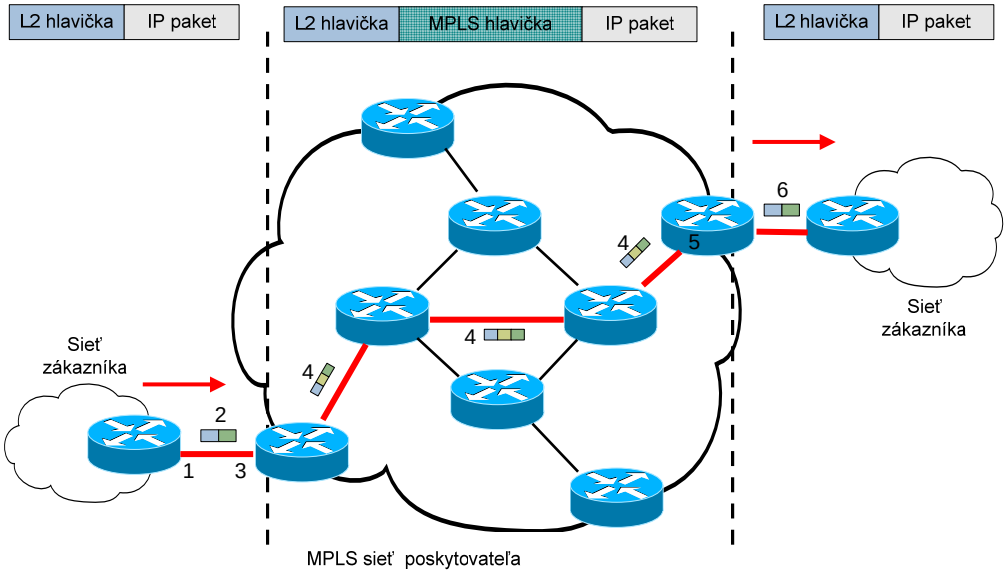
K prenosu dát sieťou existujú dva typy smerovania [13]:

Smerovanie „hop-by-hop“ (skok po skoku) – každý MPLS smerovač nezávisle vyberie ďalší uzol siete. U tohto smerovania sú využité informácie o sieťovej topológii, ktoré sa distribuujú prostredníctvom bežných IGP protokolov (Interior Gateway Protocol) akými sú OSPF, BGP, alebo IS-IS. Tento proces sa podobá smerovaniu v IP sieťach.

Explicitné smerovanie – celý zoznam uzlov na trase je špecifikovaný v dostatočnom predstihu a trasa je založená na celkovom pohľade na topológiu siete. Pozdĺž cesty môžu byť pre zabezpečenie kvality služieb rezervované prostriedky. Toto povoľuje prevádzkovej technike v sieti optimalizovať využitie šírky pásma.

3.4.1 Princíp činnosti MPLS siete

Obrázok č.15 znázorňuje typickú MPLS sieť a jej pridružené prvky [13]. Ústredný oblak predstavuje samotnú MPLS sieť. Celá dátová prevádzka v rámci tejto siete je značkovaná štítkami. Všetka ostatná komunikácia medzi oblakom a zákazníckymi sieťami nie je značkovaná. Rozhranie smerovačov vlastnených zákazníkom je označované ako Customer Edge (CE) a rozhranie smerovača poskytovateľa vystupuje pod pojmom Provider Edge (PE). V rámci MPLS siete sú rozmiestnené smerovače poskytovateľa P (nazývané tiež Label Switching Router – LSR).



Obr. 15: Zobrazenie MPLS siete a jej typických častí

Smerovač s podporou MPLS pridelí na okraji siete prichádzajúcemu paketu značku, ktorá sa používa pre jeho predávanie medzi smerovačmi vo vnútri siete. Smerovače tak môžu dáta smerovať výhradne na základe svojich individuálnych jednoduchých tabuliek indexov. Nemusia skúmať svoje smerovacie tabuľky a starať sa o ich aktuálnosť. Všetky pakety s rovnakou značkou (v rámci triedy FEC, Forwarding Equivalence Class) sa posielajú rovnakým spôsobom, a rovnakou sieťovou cestou LSP (Label Switched Path). Predávanie datagramov sa môže z tohto pohľadu javiť ako triviálna záležitosť.

Cesta LSP je zostavená tak, že postupne všetky LSR medzi vstupným (ingress) a výstupným (egress) smerovačom na rozhraní PE si vytvárajú väzbu medzi prichádzajúcou a odchádzajúcou značkou pre daný dátový tok. Cesta LSP je jednosmerná. K MPLS sieti sa pripájajú klientske siete prostredníctvom svojich smerovačov na rozhraní CE, ktoré nepotrebujú žiadnu špeciálnu podporu pre MPLS, vystačia si s bežný IP smerovaním.

Lokálna prevádzacia MPLS tabuľka (tabuľka značiek) teda jednoznačne určuje smerovacie rozhodnutie tak, že pre každú vstupnú hodnotu značky paketu prijatého z určitého rozhrania jednak priraďuje, do ktorého výstupného rozhrania má byť tento paket ďalej smerovaný, a jednak definuje novú hodnotu výstupnej značky. Tabuľka je generovaná z kombinácie informácií získaných z lokálneho smerovacieho protokolu a protokolu distribúcie značiek využívaného medzi jednotlivými MPLS prepínačmi [12].

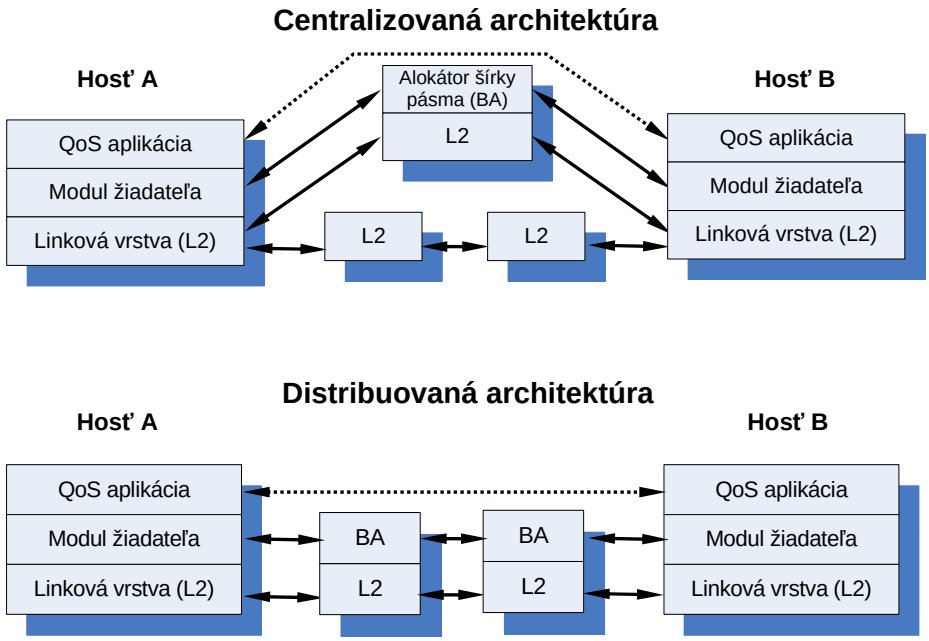
3.5 Správa prenosového pásma v podsieťach – SBM

Jedná sa o mechanizmus správy šírky pásma, ktorý je určený najmä pre sieťové topológie LAN [7]. Správa šírky pásma sa uskutočňuje na linkovej vrstve referenčného modelu OSI a k rezervácii sieťových prostriedkov sa podobne ako u integrovaných služieb využíva protokol RSVP. Od klasickej služby Best effort sa odlišuje princípom prideľovania priorít jednotlivým rámcom linkovej vrstvy na základe známych aplikačných požiadavkov. U aplikácií, ktorých činnosť je citlivá na oneskorenie sú tak rámce prenášané prednostne voči rámcom ostatných aplikácií [15].

Základné časti systému SBM sú:

- Alokátor šírky pásma (Bandwith Allocator) – udržuje stav ohľadom pridelenia prostriedkov v podsieti a vykonáva vstupnú kontrolu v závislosti od dostupných zdrojov a ostatných definovaných kritérií.
- Modul žiadateľa (Reguestor module) – je súčasťou každej stanice a uzlu siete.

Podľa umiestnenia alokátora šírky pásma rozlišujeme 2 typy SBM architektúry, centralizovanú a distribuovanú. Štruktúru týchto architektúr ukazuje obr. č. 16 [15].



Obr. 16: Dva typy SBM architektúry

Správa a riadenie sieťovej komunikácie je u tohto mechanizmu zabezpečená Správcom prenosovej kapacity (Subnet Bandwidth Manager). Je to signalizačný protokol SBM techník, ktorý zaisťuje mapovanie QoS požiadavkov vyšších vrstiev modelu OSI do nižších a koordinuje chovanie sieťových uzlov a prepínačov v danej SBM podsieti [14]. Jeden segment SBM podiete môže byť tvorený viacerými SBM prepínačmi, ktoré pracujú medzi druhou a treťou vrstvou OSI modelu. Pri žiadosti o pridelenie sieťových prostriedkov je zodpovedný za riadenie prístupu na danom segmente jeden z prepínačov, ktorý je označený ako „určený“ (Designated SBM – DSBM). DSBM môže byť určený staticky, alebo zvolený ostatnými prepínačmi. Základnou požiadavkou u SBM je, že celá sieťová prevádzka prejde najmenej jedným takýmto prepínačom s podporou SBM.

Hoci je SBM mechanizmus navrhnutý tak, aby bol nezávislý od QoS protokolov, podporuje i spoluprácu s inými QoS protokolmi. Mechanizmus je implementovaný vo všetkých koncových zariadeniach a uzloch komunikačnej siete.

4. KONFIGURÁCIA MODELOVEJ SIETE

4.1 Smerovače Cisco rady 1800

Ide o smerovače s integrovanými službami. Architektúra Cisco smerovačov rady 1800 bola špeciálne navrhnutá pre splnenie požiadaviek malých a stredne veľkých podnikov, podnikových pobočiek a malých poskytovateľov služieb za účelom poskytnutia čo najširšej škály prostriedkov pre bezpečné možnosti pripojenia v priemysle v kombinácii s vysokou dostupnosťou služby. Softvér Cisco IOS podporuje kompletnú sadu transportných protokolov, kvalitu služieb a bezpečnosť sietí.

Smerovače Cisco rady 1800 s integrovanými službami prinášajú vysoko bezpečné paralelné služby vrátane podpory bezpečných bezdrôtových sietí IEEE 802.11 a ponúkajú malým kanceláriám jednotný a odolný systém. Tieto vysoko výkonné smerovače plne využívajú výhody širokopásmového spojenia a poskytujú kľúčové vlastnosti, akými sú napríklad vyspelé možnosti zabezpečenia, vzdialenú správu a zálohovanie v sieti WAN.

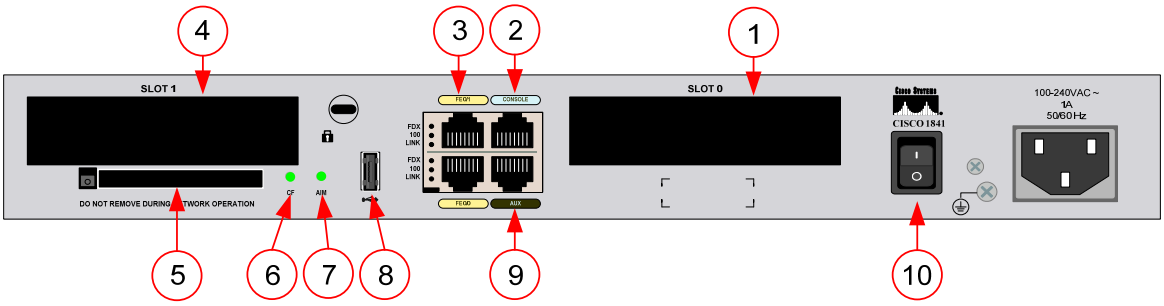
Rada 1800 poskytuje v základnej konfigurácii tieto možnosti:

- bezpečné širokopásmové pripojenie pre pobočky a malé kancelárie
- Integrované ISDN rozhranie
- Integrované zabezpečenie v podobe firewallu a šifrovania
- zabezpečené bezdrôtové pripojenie LAN s podporou 802.11a a 802.11b/g pri použití viacerých antén
- 8-portový manažovateľný prepínač s podporou VLAN a napájaním po sieti
- jednoduché nasadenie a možnosť vzdialenej správy prostredníctvom webového rozhrania a Cisco IOS softvéru.

Okrem iného poskytujú rozšírené funkcie modulu pre analýzu siete (Network Analysis Module), funkcie odhadu prenosového pásma v systéme Cisco IOS 12.4 pre užívateľom definovanú kvalitu služby (QoS), navyše pomáhajú riadiť prevádzku v sieti a optimalizovať využitie prenosového pásma. Nástroje pre správu zariadení, ktoré sú k dispozícii, výrazne zvyšujú rýchlosť implementácie aplikácií a znižujú zložitosť a prevádzkové náklady,

4.1.1 Smerovače Cisco 1841

Model smerovača Cisco 1841 zo série 1800 poskytuje voči ostatným uvedeným modelom z tejto série výhodu modulárnej konfigurácie, ktorá obnáša doplnenie základnej hardvérovej výbavy smerovača pomocou zásuvných modulov. Firma poskytuje široké portfólium rozširujúcich modulov, ktoré tak umožnia širšie využitie smerovača. Na obrázku 17 je možno vidieť zadnú stranu tohto modelu, jeho jednotlivé prvky sú uvedené v tabuľke 4.1.



Obr. 17: Zadná strana smerovača Cisco 1841

Tab. 4.1: Popis prvkov smerovača Cisco 1841

č.	Prvky smerovača 1841	č.	Prvky smerovača 1841
1	Slot 0 (WIC, VWIC, or HWIC)	**6**	LED dióda CompactFlash karty
2	Konzolový port	**7**	AIM LED dióda
3	2 x Fast Ethernet porty	**8**	USB port
4	Slot 1 (WIC, VWIC, or HWIC)	**9**	Auxiliary port
5	slot na pamäťovú kartu CompactFlash	**10**	Hlavný vypínač

Tento typ smerovačov podporuje nasledovné QoS protokoly:
Rezervačný protokol RSVP, protokol o dohodnutej prístupovej rýchlosti – CAR, protokol pre rozpoznanie sieťových aplikácií – NBAR, mechanizmus diferencovaných služieb – Diffserv, mechanizmus spojovej fragmentácie a prekladania – LFI, mechanizmus radenia do front s nízkou prioritou – LLQ, metódy správy front WFQ, CBWFQ a WRED

Smerovač je použitý ako základný sieťový uzol modelovej IP siete pre demonštráciu vplyvu kvality služieb na multimediálne aplikácie. Z dostupných QoS funkcií boli využité Diffserv, mechanizmus radenia do front s nízkou prioritou a metóda správy front CBWFQ.

4.2 Možnosti zaistenia QoS

Pre zaistenie kvality služieb v sieti postavenej na smerovačoch firmy Cisco je možné nakonfigurovať tieto prvky dvoma spôsobmi:

- konfigurácia pomocou AutoQoS
- konfigurácia pomocou systému MQC

4.2.1 AutoQoS konfigurácia

Umožňuje nastaviť funkčný model QoS na sieťových prvkoch Cisco pomocou pár príkazov. Dramaticky tak zjednodušuje nasadenie QoS automatizovaním odpovedajúcich možností a funkcií systému Cisco IOS (Internetwork Operating System), ktorý je používaný na smerovačoch a prepínačoch rovnomennej firmy. Správca takej siete nemusí byť špecialista s rozsiahlymi vedomosťami o základných sieťových technológiách (PPP, ATM, Frame-relay, Ethernet a 802.1 siete), ktoré sú potrebné pre nasadenie QoS s cieľom zabezpečiť požadovanú kvalitu hlasu, znížiť latenciu, jitter a stratovosť paketov.

Funkcia AutoQoS je však obmedzená len na VoIP služby, resp. v základnej konfigurácii je primárne zameraná len na uprednostnenie datagramov služby VoIP. Dátový prenos ostatných aplikácií je preznačkovaný na hodnotu DSCP 0 a bez zmeny priority prenesený sieťou metódou „best effort“. Cisco AutoQoS je vhodné nasadiť predovšetkým v podnikoch, ktoré vyžadujú zavedenie IP QoS služieb pre hlasovú komunikáciu bez potreby zložitého plánovania, časovej náročnosti a skúseností na špecializovanej úrovni.

Aktivácia AutoQoS na rozhraní smerovača [16]:

```
Router> enable
Router# configure terminal
Router(config)# interface interface-id
Router(config-if)# auto qos voip trust|cisco-(soft)phone
Router(config-if)# end
Router# show auto qos interface interface-id
```

Príkazmi **enable** a **configure terminal** spustíme na smerovači globálny konfiguračný mód . Vyberieme rozhranie (port), na ktorom máme pripojený IP telefón alebo rozhranie, ktoré je pripojené k ďalšiemu smerovaču, prepínaču označenému ako

dôveryhodné zariadenie (trust). Samotná AutoQoS funkcia sa aktivuje príkazom **auto qos voip**, kde treba definovať pripojené zariadenie. Príkazom **end** vystúpime z globálneho konfiguračného a dostaneme sa do privilegovaného EXEC módu, kde môžeme zadaním **show auto qos interface** *interface-id* skontrolovať nastavenie služby pre konkrétne rozhranie.

4.2.2 Konfigurácia pomocou MQC

MQC (Modular QoS Command-Line Interface) - jedná sa o modulárny systém konfigurácie QoS [17], [18]. Jeho použitím sa dosiahne oddelenie kvality služieb na smerovači od fyzickej implementácie, čím sa zaistí univerzálnosť na rôznych platformách. Umožňuje užívateľom vytvárať prevádzkové politiky a tieto následne aplikovať na určité rozhranie. Spočíva v definovaní tried prevádzky (class map) na jednotlivých zariadeniach. Definíciou tried sa nastavujú kritéria, podľa ktorých sa jednotlivé dátové toky radia do tried. Následne nastavením policy mapy určíme pravidlá, akým spôsobom sa bude zaobchádzať s jednotlivými triedami sieťovej prevádzky. Nakoniec je nutné pomocou „service policy“ aplikovať pravidlá politiky nastavené v policy-mape na jednotlivé rozhrania.

Príklad nastavenia MQC na smerovači Cisco [17]:

```
1  Router(config)# class-map match-any business-critical-traffic
   Router(config-cmap)# matcb protocol http url "*customer*"
   Router(config-cmap)# match protocol citrix

2  Router(config)# policy-map myqos policy
   Router(config-pm am)# class business-critical-traffic
   Router(config-pm am-c)# bandwidth 1000

3  Router (config)# interface Serial 0/0
   Router (config-if)# service-policy output myqos  policy
```

- **Konfigurácia prevádzkovej triedy (class-mapy)**

K vytvoreniu prevádzkovej triedy sa používa príkaz **class-map**. Syntax príkazu je nasledujúca [18]:

```
Router(config)# class-map [match-any | match-all] class-name
```

V prípade, že chceme klasifikovať dátový tok viac ako jedným kritériom, musíme toto špecifikovať kľúčovým slovom **match-any | match-all.**

match-any – používa sa v prípade, že musí byť splnené aspoň jedno zadané kritérium, aby bol dátový tok zaradený do danej triedy. Reprezentuje tak logickú funkciu OR.

match-all – používa sa v prípade, že musia byť splnené všetky zadané kritéria, aby bol dátový tok zaradený do triedy. Reprezentuje tak logickú funkciu AND.

Ku klasifikácii dátového toku sa v konfiguračnom režime triedy používa príkaz **match**, ktorý má niekoľko nasledujúcich možností:

match access-group *access-group* – kritérium pre porovnanie s ACL

match cos *cos-number* – kritérium pre porovnanie s CoS hodnotou

match [**ip**] **dscp** *dscp-value* – kritérium pre porovnanie s hodnotou DSCP

match class-map *class-name* – kritérium pre porovnanie s konkrétnu triedou

match protocol *protocol-name* – kritérium pre porovnanie s konkrétnym protokolom

match [**ip**] **precedence** *precedence-value* – porovnáva s hodnotou IP precedence

match destination-address mac *address* – porovnáva s cieľovou MAC adresou

match source-address mac *address-destination* – porovnáva s MAC adresou zdroja

- **Konfigurácia prevádzkovej politiky (policy-mapy)**

K vytvoreniu politiky slúži príkaz **policy-map**. Pri zadávaní príkazu sa špecifikuje meno „policy mapy“ a následne vstúpime do konfiguračného režimu politiky. Syntax príkazu je:

```
Router(config)# policy-map policy-name
```

K asociácii triedy prevádzky k danej politike slúži príkaz **class** *class-name*, tým sa vyberie trieda, pre ktorú budú aplikované pravidlá politiky. K definovaniu pravidiel sa naskytujú viaceré možnosti [18]:

bandwidth {*bandwidth-kbps* | **percent** *percent*} – rezervuje šírku pásma pre triedu

priority {*bandwidth-kbps* | **percent** *percent*} – rezervuje šírku pásma

random-detect [**dscp-based** | **prec-based**] – definuje WRED správu front

fair-queue – definuje počet front pre danú triedu, využíva WFQ metódu správy front

police *bps* – nastavuje kontrolu prevádzky

queue-limit – nastavuje max. počet paketov fronty pre danú triedu

set precedence *precedence-value* – nastavuje hodnotu priority v hlavičke paketu

service-policy *policy-map-name* – špecifikuje meno policy mapy

shape {**average** | **peak**} *mean-rate* – limituje prevádzku na predvolenú šírku pásma

- **Aplikácia prevádzkovej politiky na rozhranie**

K priradeniu „policy mapy“ na rozhranie smerovača sa v konfiguračnom režime používa príkaz **service-policy**. Príkaz umožňuje tiež určiť smer, v ktorom bude daná politika na rozhranie aplikovaná. Syntax príkazu [18]:

```
Router(config-if)# service-policy {input | output} policy-map-name
```

Možnosť input aplikuje politiku na rozhranie vo vstupnom smere, teda na dátový tok, ktorý vstupuje do smerovača, output vo výstupnom smere. Platí tu pravidlo, že na jedno fyzické rozhranie možno nastaviť len jednu prevádzkovú politiku a v jednom smere. Je treba na to dať pozor pri plánovaní a nastavovaní QoS pravidiel v sieti.

- **Overenie nastavených tried a politík prevádzky**

Zobrazenie a kontrolu informácií o definovaných triedach a politikách umožňujú v konfiguračnom režime smerovača tieto príkazy [18]:

```
Router# show class-map [class-map-name]
```

! zobrazí všetky nakonfigurované triedy a kritériá pre zaradenie do tried

```
Router# show policy-map policy-map class class-name
```

! zobrazí konfiguráciu policy-mapy pre danú triedu prevádzky

```
Router# show policy-map policy-map
```

! zobrazí konfiguráciu všetkých tried pre danú policy-mapu

```
Router# show policy-map interface [input | output]
```

! zobrazí štatistiku všetkých tried upravených politikou pre dané rozhranie

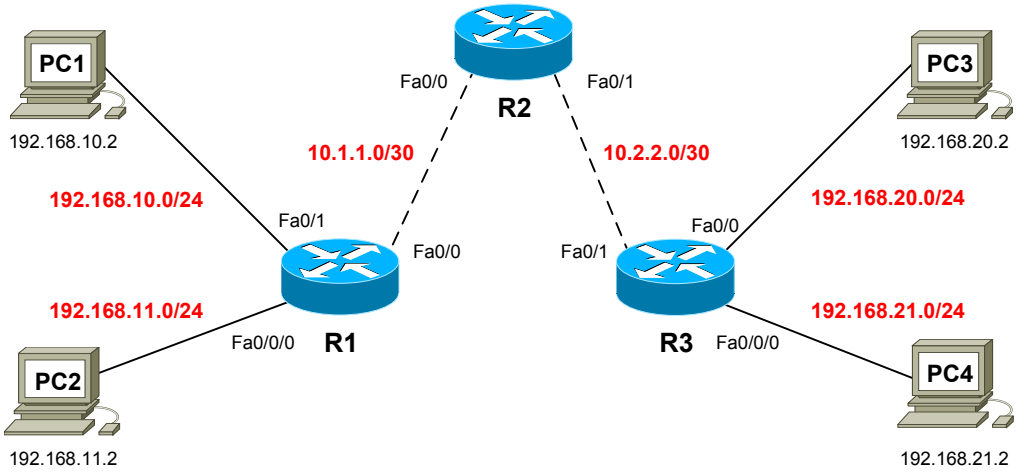
4.3 Konfigurácia IP siete v scenári s „best effort“ službami

Best effort vyjadruje, že v sieti nie sú aplikované žiadne nastavenia kvality služieb a jednotlivé dátové toky sú si rovnocenné. Neexistuje tu žiaden kontrolný mechanizmus a cieľom sieťových prvkov je doručiť dáta na sieti v čo najkratšom čase. Cieľom praktického merania v takejto sieti bolo získať základné hodnoty parametrov ovplyvňujúcich QoS pre porovnanie so scenárom s manuálne nakonfigurovanou QoS v rámci Diffserv domény

Zloženie modelovej IP siete:

- 3x smerovač Cisco1841, softwarová verzia IOS 12.4(24)T
- 4x PC, OS Windows XP

Schéma zapojenia siete je uvedená na obrázku nižšie (viď Obr.18). Hlavnými prvkami sú smerovače R1, R2, R3. Nastavenie fyzických rozhraní na jednotlivých zariadeniach pre správne zapojenie uvádza adresovacia tabuľka v prílohe práce. K prepojeniu sieťových prvkov je použitý UTP kábel kategórie 5e.



Obr. 18: Schéma zapojenia IP siete

Konfigurácia smerovačov v tomto scenári spočívala v nastavení parametrov rozhraní každého smerovača, nastavení smerovacieho protokolu, nastavení konzolového portu a virtuálnych liniek vty. V prípade, že má smerovač vymazanú „startup konfiguráciu“, jednotlivé rozhrania sú po štarte vypnuté a do činnosti sú uvedené až po ich nastavení. Ako príklad uvádzam definíciu rozhraní na smerovači R1 v jeho konfiguračnom režime. Rozhrania ostatných prvkov sa konfigurujú rovnakým spôsobom.

```
R1> enable
R1# configure terminal
R1(config)# interface FastEthernet0/0
R1(config-line)# description Line to R2
R1(config-line)# ip address 10.1.1.1 255.255.255.252
R1(config-line)# duplex auto
R1(config-line)# speed 10
R1(config-line)# interface FastEthernet0/1
R1(config-line)# description Line to PC1
R1(config-line)# ip address 192.168.10.1 255.255.255.0
R1(config-line)# duplex auto
R1(config-line)# speed 10
R1(config-line)# interface FastEthernet0/0/0
R1(config-line)# description Line to PC2
R1(config-line)# ip address 192.168.11.1 255.255.255.0
R1(config-line)# duplex auto
R1(config-line)# speed 10
R1(config-line)# end
```

Ďalej je treba nastaviť smerovací protokol. Použitý je dynamický smerovací protokol OSPF, ktorý zabezpečí medzi smerovačmi výmenu informácií o pripojených sieťach.

```
R1(config)# router ospf 1
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 192.168.11.0 0.0.0.255 area 0
```

Pre potreby monitorovania činnosti smerovača bol ešte spustený HTTP a HTTPS server, aby bolo možné cez webové rozhranie nadviazať komunikáciu s programom Cisco SDM (Security Device Manager). Všetky smerovače majú okrem fyzických rozhraní nastavené zvyšné funkcie rovnakým spôsobom a jednotlivé konfigurácie a ich výpisy z pamäte možno nájsť v elektronickej prílohe práce.

4.4 Automatická konfigurácia QoS v sieti funkciou AutoQoS

Spôsob nastavenia kvality služieb v sieti pomocou AutoQoS uvádza kapitola 4.2.1. Táto funkcia, ako som spomínal je zameraná len na VoIP prevádzku v sieti. Dátový prenos ostatných aplikácií je prenesený sieťou bez zmeny priority. S ohľadom na dostupné zariadenie modelovej siete a bez prítomnosti hardvérových telefónov Cisco, ktoré si sami zabezpečujú značkovanie prevádzky vyplýva, že realizácia tohto scenára je bezpredmetná, pretože by nebol badateľný žiaden vplyv pôsobenia takto nastavenej QoS v sieti. Z toho dôvodu nebola uvažovaná pre meranie vplyvu QoS.

4.5 Konfigurácia IP siete v scenári s manuálne nastavenou QoS

Scenár bol realizovaný za účelom zistenia vplyvu QoS v sieti LAN. Zo smerovačmi podporovaných funkcií a s ohľadom na zadanie práce je implementovaný mechanizmus diferencovaných služieb. Aktívne sieťové prvky, smerovače R1, R2, R3 tvoria jednotnú Diffserv doménu. Z praktického hľadiska možno označiť prvky R1 a R3 ako hraničné smerovače, ktoré slúžia na klasifikáciu prichádzajúcej sieťovej prevádzky do DS domény. Prvok R2 plní funkciu vnútorného smerovača, čím zaisťuje spojenie vo vnútri domény. Neprevádza klasifikáciu a s dátovými tokmi zaobchádza podľa pridelených značiek. Topológia zapojenia je rovnaká ako v predošlom scenári s best effort službami, viď obr. č.18. Scenár vychádza z predpokladu základnej konfigurácie rozhraní, smerovacieho protokolu, HTTP, HTTPS servera a ostatných portov, ktoré boli popísané v predchádzajúcej časti. Všetky popisované nastavenia QoS sa aplikujú prostredníctvom MQC.

Koncové počítače v sieťach pripojených k hraničným smerovačom domény sú označené ako nedôveryhodné a pre účel overenia vplyvu QoS na sieťovú prevádzku sú v sieti prenášané kritické multimediálne služby. Tie predstavuje prenos VoIP hlasu – IP telefónie, streamovaného videa a dátového FTP toku, ktorý simuluje vyťaženie siete na pozadí. Pre správnu klasifikáciu jednotlivých sieťových tokov sú na smerovačoch definované nasledujúce triedy prevádzky:

- VOICE – do tejto triedy je nutné klasifikovať prenos VoIP hlasu. To sa dosiahne nasledujúcim nastavením:

```
R1(config)# class-map match-any VOICE
R1(config-cmap)# match ip dscp ef
R1(config-cmap)# match access-group 101
```

  Ako možno pozorovať z príkazov, klasifikácia prebieha na základe 2 kritérií, pričom musí byť splnené aspoň jedno kritérium, aby bol tok zaradený do triedy VOICE. Zvolenými kritériami v tomto prípade je porovnávanie DSCP značky 46 (ef) priradenej testovacou aplikáciou IxChariot a porovnávanie na základe pravidiel definovaného Access-listu pre potreby rozpoznania „simulovanej“ VoIP prevádzky generovanej aplikáciou iPerf.

- VIDEO – do triedy je treba zaradiť prenos streamovaného videa. To sa klasifikuje na základe access-listu podľa uvedeného nastavenia:

```
R1(config)# class-map match-any VIDEO
R1(config-cmap)# match access-group 102
```

- WEB – sem patrí sieťová prevádzka protokolu HTTP a porovnanie je opäť nakonfigurované na základe access-listu pre rozpoznanie www prevádzky v sieti. Pretože aplikácia IxChariot si dokáže pre potreby testovania sama značkovať prevádzku, patrí sem i trieda AF3, do ktorej sú zaradené už označkované pakety webovej prevádzky. Nastavenie sa prevedie pomocou príkazov:

```
R1(config)# class-map match-all WEB
R1(config-cmap)# match ip dscp af31  af32  af3
R1(config-cmap)# exit
R1(config)# class-map match-all AF3
R1(config-cmap)# match access-group 104
```

- BULK_DATA – podľa štandardného doporučenia pre vytváranie tried je dodatočne nakonfigurovaná na uvažovaných smerovačoch táto trieda, do ktorej spadá dátový tok aplikačných protokolov Telnet a SMTP (Email), avšak neboli k meraniu využité. Štandardne sa doporučuje sem zaradiť i FTP dátový prenos, v simulovanom scenári bol však použitý pre vyťaženie siete na pozadí a bolo žiadúce aby nebol označený značkou žiadnej triedy. Smerovač ho tak zaradí do základnej triedy so značkou DSCP 0. Rozradenie prebieha na základe access-listu alebo v prípade umelého generovania aplikáciou IxChariot už označkovaného toku DSCP hodnotami AF21, AF22. Konfigurácia triedy sa prevedie podľa príkazov:

```
R1(config)# class-map match-all BULK_DATA
R1(config-cmap)#  match ip dscp af21  af22
R1(config-cmap)# class-map match-all AF21
R1(config-cmap)#  match access-group 108
R1(config-cmap)# class-map match-all AF22
R1(config-cmap)#  match access-group 109
```

Na takto klasifikovanú prevádzku je treba definovať na smerovači príslušné politiky. Pre tieto potreby sú vytvorené 2 policy-mapy. Politika SET-DSCP zabezpečuje značkovanie prichádzajúcej prevádzky na vstupných portoch okrajových smerovačov. Značkovanie prebieha priradením DSCP hodnoty jednotlivým rozradeným triedam prevádzky

a dosahuje sa tým požadované spracovanie sieťových tokov ďalšími smerovačmi v doméne. Konfigurácia politiky SET-DSCP sa prevedie nižšie uvedenými príkazmi:

```
R1(config)# policy-map SET-DSCP
R1(config-pmap-c)# class VOICE
R1(config-pmap-class)# set ip dscp ef
R1(config-pmap-c)# class AF3
R1(config-pmap-class)# set ip dscp af31
R1(config-pmap-c)# class AF21
R1(config-pmap-class)# set ip dscp af21
R1(config-pmap-c)# class AF22
R1(config-pmap-class)# set ip dscp af22
```

Klasifikovanej a označkovanej sieťovej prevádzke je treba určiť pravidlá QoS, ktoré budú platiť od hranice domény – hranice dôveryhodnosti. Okrajový smerovač je považovaný pre Diffserv doménu za prvé dôveryhodné zariadenie, keďže v sieti sa nenachádzajú Cisco IP telefóny. Pravidlami QoS sa rozumie požadovaný spôsob spracovania jednotlivých tokov smerovačmi v rámci domény. K tomuto účelu je nutné definovať politiku nazvanú QOS, ktorá sa uplatňuje na port smerovača pripojeného k ďalšiemu aktívnemu prvku siete. Podľa odporúčaných nastavení a s uvážením zadania, boli zvolené tieto pravidlá spracovania sieťových tokov:

- VOICE – prenos hlasu patriaci do tejto triedy by mal byť prednostne doručený s čo najnižším oneskorením, ktoré mu zaručuje spracovanie fronty typu PQ spolu s mechanizmom LLQ. Je mu vyhradená požadovaná šírka pásma 500kb/s, to sa dosiahne príkazom `priority 500`. Túto hodnotu má vyhradenú za každých okolnosti a zároveň je tým udaná maximálna garantovaná šírka pásma pre túto triedu v prípade preťaženia siete.
- VIDEO – prenosu streamovaného videa je vyhradených 20% celkovej šírky pásma, čo sa dosiahne použitím príkazu `bandwidth percent 20`. Pri nastavení sieťových liniek na 10Mbps je tak zaručená minimálna šírka pásma 2Mbps. Ak nie je sieť plne využitá, alebo sa nenachádza v stave preťaženia, je triede priradená časť voľnej šírky pásma nad hranicu rezervovanej hodnoty. Zároveň sa príkazom všeobecne určí spracovanie fronty typu WFQ, alebo CBWFQ, v tomto prípade je to CBWFQ, keďže prevádzka sa spracúva na základe tried.
- WEB – webovej prevádzke je vyhradených 15% šírky pásma, avšak v prípade stavu preťaženia siete je uplatnené pravidlo určené príkazom `shape average 320000`. Takto je presne nastavená kapacita výstupnej linky tvarovača na 320kbps.

Pri preťažení je webová prevádzka nad túto hodnotu zahodená blokom zahadzovača, ktorý zabezpečuje dodržanie určeného profilu prevádzky.

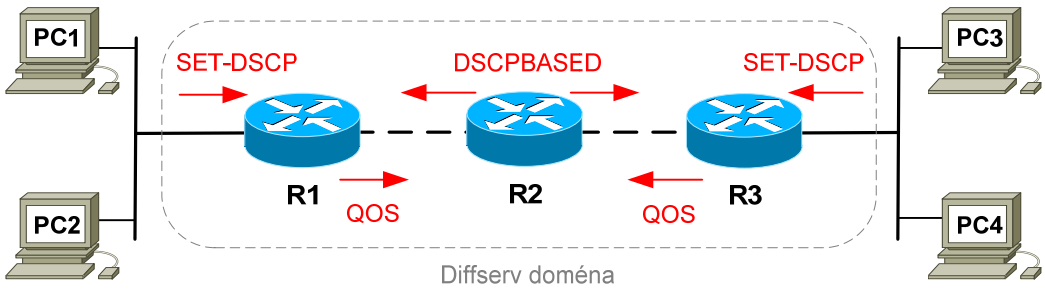
- BULK_DATA – trieda má vyhradených svojich 10%, ktoré sú jej garantované za akýchkoľvek podmienok vyťaženia siete. V stave nevyužitej linky jej môže byť podľa potreby pridelená časť voľnej šírky pásma.

Okrem definovaných tried existuje v každej politike základná trieda nazvaná „class-default“, do ktorej spadá zvyšná neklasifikovaná prevádzka a sieťové toky s hodnotou značky DSCP 0.

Všetky popisované pravidlá politiky QOS sa nastavujú na smerovači týmito príkazmi

```
R1(config)# policy-map QOS
R1(config-pmap-c)# class VOICE
R1(config-pmap-c)# priority 500
R1(config-pmap-c)# class VIDEO
R1(config-pmap-class)# bandwidth percent 20
R1(config-pmap-c)# class WEB
R1(config-pmap-class)# shape average 320000
R1(config-pmap-class)# bandwidth percent 15
R1(config-pmap-c)# class BULK_DATA
R1(config-pmap-class)# bandwidth percent 10
```

Nakoniec je potrebné prideliť vytvorené politiky na jednotlivé rozhrania. Súčasne je nutné určiť smer, v akom bude politika aplikovaná. Pridelenie a ich smer v rámci domény zobrazuje nižšie uvedený obrázok č. 19.



Obr. 19: Vyznačenie smeru pridelenia politík na rozhraniach smerovačov

Pridelenie politík na rozhranie smerovača R1 sa nastaví príkazmi:

```
R1(config)# interface FastEthernet0/0
R1(config-line)# service-policy output QOS
R1(config-line)# interface FastEthernet0/1
R1(config-line)# service-policy input SET-DSCP
```

Ako poslednú časť konfigurácie je potreba definovať Access-listy slúžiace k vyfiltrovaniu určitého typu prevádzky pre zaradenie do príslušnej triedy. Nastavenie je prevedené nižšie uvedenými príkazmi v konfiguračnom režime smerovača. Uvedená konfigurácia Access-listu je aplikovaná na každý použitý smerovač.

```
R1(config)# access-list 101 permit udp any any range 5001 5002
R1(config)# access-list 102 permit udp any any range 5003 5004
R1(config)# access-list 103 permit udp any any range 1234 1236
R1(config)# access-list 104 permit tcp any any eq www
R1(config)# access-list 105 permit ip any any
R1(config)# access-list 106 permit tcp any any range 5005 5006
R1(config)# access-list 108 permit tcp any any eq telnet
R1(config)# access-list 109 permit tcp any any eq smtp
R1(config)# access-list 110 permit tcp any any eq ftp
```

V tejto časti bola popísaná konfigurácia okrajového smerovača R1. Bolo však vychádzané z nastavení prevedených v predošlom scenári best-effort. Rovnako je nutné nakonfigurovať okrajový smerovač R3, keďže v celej doméne sú požadované jednotné pravidlá QoS. Jediná zmena spočíva v aplikácii politík na rozhranie v opačnom smere. Vnútorný smerovač R2 používa rovnaké triedy prevádzky, odlišuje sa len v nastavení politiky. Tá je len jedna a aplikuje sa na oba porty smerovača vo výstupnom smere. Neurčuje pravidlá zaobchádzania s triedami a zaručuje tak len predávanie prevádzky smerovačom podľa nastavených pravidiel v politike okrajových smerovačov R1, R3.
Jednotlivé nastavenia a výpisy konfigurácii smerovačov možno nájsť v elektronickej prílohe práce.

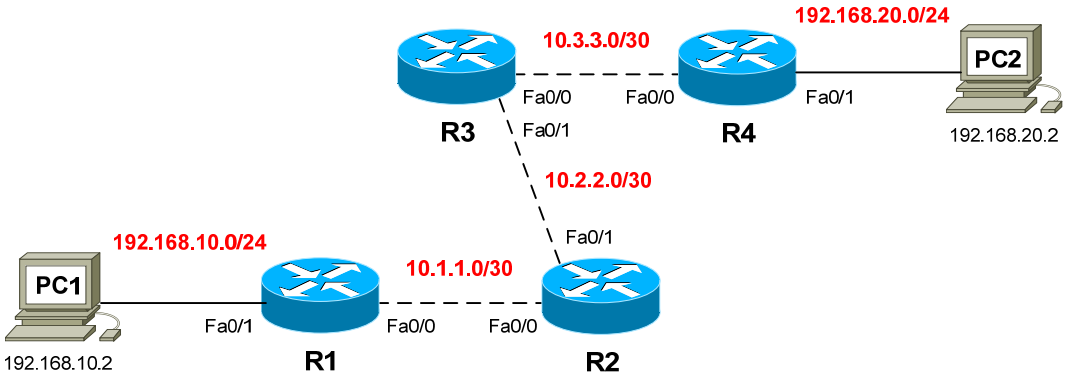
4.6 Konfigurácia QoS v IP sieti na rozhraní dvoch DS domén

Posledný scenár IP siete je konfigurovaný s cieľom zistiť vplyv pôsobenia kvality služieb na rozhraní dvoch DS domén, ktoré využívajú k spracovaniu prevádzky rôzne profily QoS. Opäť je aplikovaný mechanizmus diferencovaných služieb

Zloženie IP siete II:

- 4x smerovač Cisco1841, softwarová verzia IOS 12.4(24)T
- 2x PC, OS Windows XP

K zapojeniu siete je použitá topológia uvedená na obrázku č. 20. Hlavnými prvkami sú smerovače R1, R2, R3 a R4. Nastavenie fyzických rozhraní na jednotlivých zariadeniach pre správne zapojenie uvádza adresovacia tabuľka v prílohe práce.



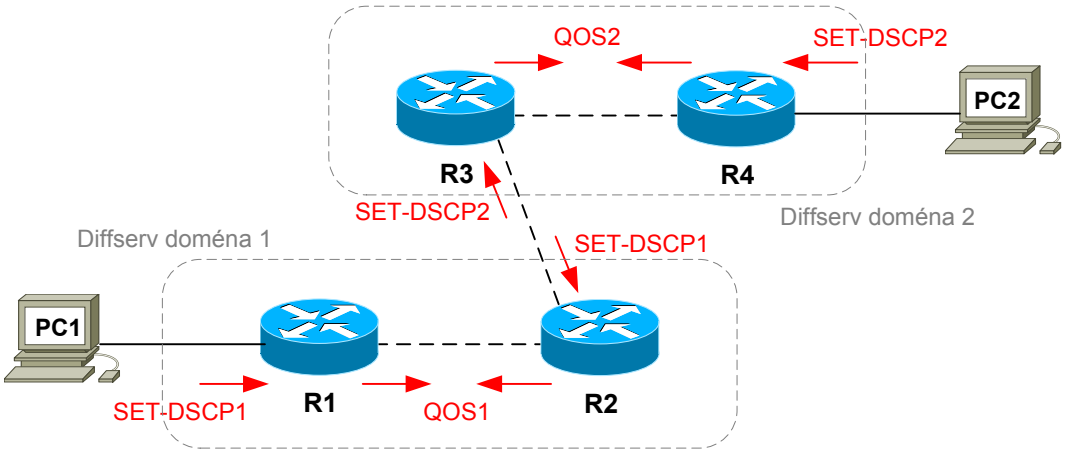
Obr. 20: Schéma zapojenia IP siete II

Zariadenia R1, R2 tvoria Diffserv doménu DS1, zariadenia R3 a R4 zasa doménu DS2. Všetky aktívne prvky tak fungovali vo funkcii okrajových smerovačov a z principiálneho hľadiska nebolo potrebné využívať ďalšie zariadenia vo funkcii vnútorných smerovačov, keďže klasifikácia a spracovanie prevádzky je prevedená hraničnými smerovačmi.

Konfigurácia smerovačov vychádza opäť z predpokladu základnej konfigurácie rozhraní, smerovacieho protokolu, HTTP, HTTPS servera a ostatných portov. Nastavenie QoS

v uvedených doménach je veľmi podobné tomu z okrajových smerovačov predošlého scenára. Sú použité rovnaké multimediálne služby a teda je potrebné definovať rovnaké triedy prevádzky. Na vstupných portoch DS domén je tak nutné implementovať rovnakú politiku SET-DSCP, ktorá prevedie označenie prichádzajúcich tokov do domény DSCP značkou. Na porty smerovačov vo vnútri domén sú aplikované politiky QOS1 pre doménu DS1 a QOS2 pre doménu DS2. Tie zabezpečia požadované spracovanie jednotlivých tokov smerovačmi. Politiky QOS1 a QOS2 sa odlišujú v nastavených pravidlách spracovania tokov podľa zadania práce. Jednotlivé vytvorené politiky sú aplikované na rozhrania spôsobom a v smere, aký je zobrazený na obr. č. 21. Cela konfigurácia kvality služieb na aktívnych prvkoch je opäť prevedená prostredníctvom MQC.

Poslednou časťou nastavenia smerovačov je definícia Access-listu, ktorý je využitý pre filtrovanie prevádzky jednotlivých tried. Je opäť použitý rovnaký profil Access-listu ako v predošlom scenári.
Jednotlivé nastavenia a výpisy konfigurácii smerovačov možno nájsť v elektronickej prílohe práce.



Obr. 21: Vyznačenie uplatnených politík na rozhraniach smerovačov

5. PRAKTICKÉ MERANIE VPLYVU QOS

5.1 Metodika merania

Pre potreby merania vplyvu QoS boli zapojené 2 typy modelovej IP siete. Prvý typ obsahuje 3 smerovače Cisco 1841 a 4 PC. Detailné zapojenie je uvedené v prílohe práce V rámci tejto testovacej siete sú odsimulované 2 scenáre. Prvý scenár predstavuje bežnú LAN sieť bez aplikovanej kvality služieb. Prenos sieťovej prevádzky tak plne zastupuje metódu best effort. Podrobný popis praktickej konfigurácie je uvedený v kapitole 4.3.
V druhom scenári, ktorý je simulovaný na rovnakom type siete je aplikovaná manuálna konfigurácia QoS, ktorej praktické nastavenie je podrobne popísané v kapitole 4.5. Testovacia sieť svojím nastavením predstavuje ucelenú Diffserv doménu, ktorá z hľadiska QoS využíva pre správu sieťovej prevádzky radenie front s váženou spravodlivou obsluhou riadenou podľa tried – CBWFQ.
Druhý typ modelovej siete slúži k testovaniu vplyvu kvality služieb na rozhraní dvoch Diffserv domén. Kvôli prítomnosti dvoch DS domén je nutné použiť 4 smerovače. Každá doména obsahuje 2 prvky, ktoré plnia úlohu okrajových smerovačov. Hranica dôveryhodnosti tak pripadá na každý smerovač domény. K spracovaniu prevádzky využíva rôzne profily nastavenej QoS a podrobný postup konfigurácie je uvedený v kapitole 4.6.

Vzhľadom k dostupným zariadeniam je nutné vo všetkých scenároch siete generovať jednotlivé sieťové toky softvérovou aplikáciou. Tá musí byť schopná generovať hlasovú prevádzku, ktorá predstavuje VoIP komunikáciu, video prevádzku, ktorá zastupuje prenos streamovaného videa a dátový tok FTP, ktorý slúži k vyťaženiu siete a predstavuje tak bežnú záťaž siete LAN na pozadí. Ďalším kritériom na výber aplikácie je jej schopnosť analyzovať chovanie siete a taktiež musí disponovať funkciou zobrazenia sieťových parametrov. S ohľadom na QoS sú takýmito parametrami šírka pásma, oneskorenie, rozptyl oneskorenia a stratovosť.
Vhodnou aplikáciou, ktorá dokáže generovať požadovanú záťaž siete je iPerf, ktorý zvláda úlohu servera i klienta a po spárovaní koncových uzlov a prevedení testu dokáže zobraziť namerané výsledky. Ďalšou takouto aplikáciou je profesionálny nástroj IxChariot od firmy Ixia, ktorý poskytuje obrovské množstvo možností a nastavení testovacích skriptov.

Dátové toky jednotlivých typov prevádzky tvoria podľa požiadaviek zadania dátový profil aplikovaný na modelovú sieť jednej domény a sú špecifikované nasledovne:

- hlasová komunikácia – generovaný tok 500 kbit/s
- video prenos – generovaný tok 2 Mbit/s
- dátový prenos FTP - generovaný tok 8 Mbit/s

K otestovaniu vplyvu QoS na rozhraní dvoch domén boli použité dva odlišné profily.
Špecifikácia profilu 1:

- hlasová komunikácia – generovaný tok 330 kbit/s
- video prenos – generovaný tok 1500 kbit/s
- dátový prenos FTP - generovaný tok 8 Mbit/s

Špecifikácia profilu 2:

- hlasová komunikácia – generovaný tok 500 kbit/s
- video prenos – generovaný tok 2 Mbit/s
- dátový prenos FTP - generovaný tok 8 Mbit/s

Uvedené špecifikácie udávajú nielen veľkosti generovaných tokov, ale zároveň hodnoty uvedené pre hlas a video definujú nastavenia politík pre spracovanie danej prevádzky v Diffserv doménach.
Z dôvodu vyťaženia a simulácie preťaženia liniek, sú všetky linky v sieti nastavené na rýchlosť 10 Mb/s. Programy Iperf a IxChariot sú inštalované na počítači PC1 v oboch typoch sietí. Ako druhý koncový uzol pre generovanú prevádzku slúži PC2. Programu IxChariot sa tu nachádza spustený koncový uzol – endpoint.
Na počítačoch PC3 a PC4 je v prvom type siete prevádzkovaný reálny FTP dátový tok. Kvôli možnosti subjektívneho porovnania vplyvu QoS je pokusne medzi PC3 a PC4 prenášaný video stream pomocou aplikácie VLC. V druhom type IP siete je FTP dátový tok prenášaný medzi PC1, PC2 súčasne pri spustenom generovaní sieťovej prevádzky aplikáciou. V tomto prípade nahrádza reálny FTP prenos bežiacu inštanciu programu, ktorá predstavuje FTP dátový tok. Generovanú VoIP prevádzku nemá zmysel nahrádzať reálnou aplikáciou, pretože programy fungujúce v sieti LAN bez potreby pripojenia k Internetu využívajú veľmi úsporné kodeky schopné minimalizovať sieťový prenos na hodnotu do cca 30kbit/s a nepredstavujú tak reálne chovanie prenosu VoIP.

5.2 Výsledky merania

Výsledky merania pre jednotlivé scenáre uvádza nižšie uvedená tabuľka č.5.1. Toto meranie bolo prevedené pomocou programu iPerf. Potrebné dátové toky boli vytvorené viacerými spustenými inštanciami programu, pričom ich bolo nutné vzájomne spárovať pomocou čísla portu, ktorý využívali. VoIP komunikácia bola generovaná obojsmerne.
Z nameraných výsledkov je vidieť vplyv pôsobenia nastavenej QoS. Na šírke pásma u VoIP a video prenosu je jasne vidieť dodržanie rezervovanej hodnoty. FTP prenos, ktorý predstavoval prevádzku na pozadí a jeho spracovanie nebolo nijak špecifikované, je pri zapnutej QoS trochu potlačený na úkor uprednostnených tokov. Implementáciou QoS je tiež viditeľne zlepšená hodnota rozptylu oneskorenia u VoIP prevádzky. U videa síce došlo pri meraní k zhoršeniu tejto hodnoty, ale stále spĺňa doporučené požiadavky na kvalitu služieb. V poslednom scenári boli namerané zvýšené hodnoty rozptylu, aj napriek nastavenej QoS. Meranie stratovosti paketov programom iPerf vykazovalo pri zapnutej QoS nulové hodnoty i po viacerých opakovaniach, čo možno prisúdiť chovaniu programu.

Tab. 5.1: Výsledky merania programom iPerf

SCENÁR	Typ sieťovej prevádzky	Šírka pásma				Rozptyl oneskorenia			Stratovosť
		Nastavená	Priemer	MIN	MAX	Priemer	MIN	MAX	Pkts / %
		kb/s	kb/s	kb/s	kb/s	ms	ms	ms	
No-QoS	VoIP	500	500	494	506	3,194	0	6,50	112 / 2,2%
	Video	2000	1942	1874	1963	3,325	3,51	10,45	631 / 4,1%
	FTP	8000	7537	6810	7936	-	-	-	-
QoS DS1[1]	VoIP	500	500	494	506	0,54	0	1,65	1 / 0%
	Video	2000	1946	1929	2011	4,05	2,41	7,58	1 / 0%
	FTP	8000	6482	5704	6236	-	-	-	-
QoS DS2[2]	VoIP	330	340	282	517	0,85	0	9,90	1 / 0%
	Video	1500	1752	1576	1976	6,46	0	10,98	1 / 0%
	FTP	8000	6614	4129	7143	-	-	-	-
QoS DS2[3]	VoIP	500	500	494	517	5,26	0	9,70	1 / 0%
	Video	2000	1985	1964	2011	7,58	2,1	11,38	1 / 0%
	FTP	8000	6152	4129	7012	-	-	-	-

Vysvetlivky:

DS1[1] – meranie bolo prevedené v modelovej sieti s jednou Diffserv doménou.

DS2[2] – meranie v sieti s dvoma DS doménami, Video a FTP prevádzka posielané z PC1 na PC2.

DS2[3] – meranie v sieti s dvoma DS doménami. Video a FTP prevádzka posielané z PC2 na PC1.

Pri meraní aplikáciou IxChariot boli využité preddefinované skripty generátorov pre jednotlivé typy prevádzky. Program umožňuje zaťažiť sieť výberom väčšieho množstva dátových tokov. Týmto je navyše možné určiť smer prenosu paketov v sieti. Zvolený testovací profil s rôznymi typmi prevádzky je možné spustiť naráz a nie je potrebné využívať viaceré inštancie programu alebo viaceré koncové stanice v sieti. Takto sa dá vystačiť s dvoma koncovými počítačmi. Na jednom musí byť predinštalovaný IxChariot, ktorý si generuje a analyzuje prevádzku, na druhom postačuje, aby bol spustený koncový bod programu (endpoint), ktorý zabezpečuje spárovanie počítačov v sieti.

Tab. 5.2: Výsledky merania programom IxChariot

SCENÁR	Typ sieťovej prevádzky	Šírka pásma				Rozptyl oneskorenia			Stratovosť
		Nastavená	Priemer	MIN	MAX	Priemer	MIN	MAX	Pkts / %
		kb/s	kb/s	kb/s	kb/s	ms	ms	ms	
No-QoS	VoIP	448	437,5	434	441	3,5	3	4	51 / 1,7%
	Video	2000	1953	1952,7	1953	1,5	1	4	57 / 2,8%
	FTP	8000	7682	7145	8024	-	-	-	-
QoS DS1[1]	VoIP	448	437,5	437	441	1,5	1	5	2 / 0,1%
	Video	2000	1953	1952,7	1953	4,5	4	5	3 / 0,1%
	FTP	8000	7682	7145	8024	-	-	-	-
QoS DS2[2]	VoIP	320	312,5	312	314	5,5	4	7	7 / 0,3%
	Video	1500	1465	1464	1465	2,5	1	5	4 / 0,2%
	FTP	8000	6282	5015	6985	-	-	-	-
QoS DS2[3]	VoIP	320	311	314	439	3	2	10	9 / 0,4%
	Video	2000	1942	1832	2030	8	5,5	17	3 / 0,1%
	FTP	9280 [4]	6800	5720	9280	-	-	-	-

Vysvetlivky:

DS1[1] – meranie bolo prevedené v modelovej sieti s jednou Diffserv doménou.

DS2[2] – meranie v sieti s dvoma DS doménami, Video a FTP prevádzka posielané z PC1 na PC2.

DS2[3] – meranie v sieti s dvoma DS doménami. Video a FTP prevádzka posielané z PC2 na PC1.

Výsledky uvedené v tabuľke 5.2 však zavádzajú určité pochybnosti o účinku kvality služieb. Síce všetky vyhovujú požiadavkám kladeným na hodnoty pre splnenie doporučení QoS, ale medzi scenármi s aplikovanou kvalitou služieb a bez nej nie sú viditeľné jednoznačné rozdiely v prospech QoS implementácie. Toto možno pozorovať na hodnotách šírky pásma. Čo sa týka hodnôt rozptylu oneskorenia u VoIP prevádzky, možno

vysledovať zlepšenie v scenári s jednou Diffserv doménou, ale naopak, nemožno to potvrdiť v scenári s doménami dvoma.

Z výsledkov merania parametrov QoS v scenári s dvoma DS doménami možno vyvodiť záver, že najnižšia rezervovaná hodnota pre multimediálne dátové toky bola vždy dodržaná. Podľa smeru, z ktorého bola prevádzka poslaná sieťou, bola šírka pásma prevádzky definovaná politikou domény, ktorou prevádzka prešla najskôr. Ak bol teda dátový tok prenášaný z PC1 na PC2 cez doménu DS1, DS2, politika správy bola určená doménou DS1. V opačnom smere bola určená doménou DS2. Podľa teórie dochádza na hranici domény k odobratiu značky smerovačom a na nasledujúcom hraničnom smerovači k novému označeniu a uplatneniu odlišného profilu nastavenej politiky. Aj napriek predpokladu vidieť z výsledkov, že šírka pásma prevádzky prenesenej prvou z domén v ceste prenosu bola zachovaná i v druhej doméne. Nedochádza k zníženiu a následnému zahadzovaniu prevádzky. Akoby okrajový smerovač takejto prevádzke zachoval predošlý profil a rezervoval pri prechode šírku pásma nad hranicu hodnoty určenej jeho politikou. Toto sa deje na úkor šírky pásma základnej triedy, do ktorej okrem iného spadá aj dátový tok FTP. Možno to vypozorovať z hodnôt jeho prenosu. Na obr. č.22 je vidieť priepustnosť jednotlivých dátových tokov pri zaťažení Ďalšie grafy možno nájsť v elektronickej prílohe.

Obr. 22: Priepustnosť jednotlivých dátových tokov v sieti

Pre potreby subjektívneho porovnania s prevádzkou v reálnej sieti, bol video prenos nahradený streamovaným dátovým tokom pomocou aplikácie VLC. Bol použitý MPEG2 video prenos s bitovým tokom 1400 kb/s. Streamované video dosahovalo v scenári bez QoS dobrej kvality len pri súčasnej VoIP komunikácii. Ak bol spustený na linke FTP prenos na pozadí, čím sa dosiahlo vyťaženie celej kapacity linky, došlo k úplnému výpadku zvuku, obraz veľmi sekalo a vyskytovali sa v ňom rôzne artefakty. Rovnakým testom v scenári s implementovanou QoS sa dosiahlo výsledku, že pri plnom vyťažení siete prenosom FTP dochádzalo len k občasnému preskoku zvuku a k veľmi zriedkavému výskytu obrazovej vady. Bolo tak možné pozorovať pozitívny dopad aplikovanej kvality služieb na takúto prevádzku. Rovnakého výsledku bolo dosiahnuté v oboch scenároch s QoS.

Výsledky všetkých vykonaných meraní a jednotlivé grafy sú priložené v elektronickej verzii prílohy práce, na CD.

6. ZÁVER

Pre kvalitu služby IP sietí v súčasnej dobe neexistuje štandardizovaný a ucelený popis, ktorý by zahrnoval všetky aspekty tejto problematiky. Vzhľadom k tomu, že novodobé siete sa potýkajú s problémami, ako efektívne a v čo najväčšej miere poskytnúť multimediálnym aplikáciám zaistenie kvality služieb, museli za posledné desaťročia mnohé svetové organizácie pristúpiť k úpravám stávajúcich mechanizmov a návrhu nových. Medzi najznámejšie subjekty, ktoré sa zaoberajú kvalitou služieb v IP sieti patria organizácie ako IETF, ITU-T.

Diplomová práca podáva ucelený pohľad na možnosti poskytnutia QoS v IP sieťach. Uvádza základné vlastnosti parametrov a požiadavky na dodržanie týchto parametrov v sieti s multimediálnou prevádzkou. Postupne rozoberá jednotlivé techniky pre zaistenie kvality služieb. Najjednoduchšou možnosťou zabezpečenia dostatočnej šírky pásma je predimenzovanie dátovej linky. Nejde však o plnohodnotnú techniku a v súčasnosti je pri nasadení v sieti vždy len dočasným riešením. Postupným vývojom sa organizácie dopracovali k mechanizmu Integrovaných služieb a s ním spojeným rezervačným protokolom RSVP. Tieto možno zaradiť do kategórie architektúr, ktoré si zabezpečia vyžadovanú úroveň služieb rezerváciou sieťových prostriedkov. Posledným popisovaným zástupcom tejto skupiny je mechanizmus Diferencovaných služieb, ktorý je založený na agregácii dátových tokov do malého počtu tried s priradenou kvalitou služby. Treťou skupinou popisovaných architektúr uvedenou v práci, sú prioritné mechanizmy MPLS a SBM, ktoré sú založené na riadení šírky pásma a optimalizácii výkonu komunikácie. Popis jednotlivých mechanizmov poskytuje prehľad o výhodách, či nevýhodách danej architektúry, možnosti jej nasadenia a benefity plynúce z jej použitia na danej linke, či v rámci určitej časti siete.

Nadväzujúca časť práce sa zaoberá popisom smerovačov Cisco série 1800. Obsahuje základné vlastnosti a možnosti, ktorými disponuje táto séria a podrobnejšie uvádza informácie o smerovači Cisco 1841. Súčasne predstavuje dve možnosti konfigurácie uvedených smerovačov pre zaistenie QoS v sieti.

Praktická časť práce uvádza podrobný spôsob nastavenia smerovačov pre použitie v jednotlivých scenároch modelovej siete. Za účelom zistenia vplyvu implementovanej QoS boli vytvorené dva typy modelovej IP siete. Topológie oboch typov možno nájsť v prílohe práce, detailný popis je uvedený spolu s nastavením smerovačov v kapitole 4.

Testovanie bolo vykonané v troch scenároch, ktoré simulovali využitie siete bez prítomnosti QoS, s manuálne nastavenou QoS pomocou MQC v jednej Diffserv doméne a manuálne nastavenou QoS na rozhraní dvoch Diffserv domén. V rámci týchto scenárov boli simulované tri typy reálnej prevádzky na sieti, VoIP a streamovanie videa (IPTV), ktoré sú najviac citlivé na zaťaženie siete. Tretím typom bol FTP dátový tok simulujúci vyťaženie siete na pozadí. Kvôli možnosti vzájomného porovnania výsledkov bola vytvorená vhodná metodika merania, ktorá je popísaná v kapitole 5.1.

Výsledkom práce sú namerané hodnoty parametrov ovplyvňujúcich QoS uvedené v tabuľkách 5.1 a 5.2. Z hodnôt možno vypozorovať určité zlepšenie pri aplikovanej QoS, meranie však ukázalo, že nie vždy to platí. Rozdiely v niektorých hodnotách sú tak malé, že to možno prisúdiť chybe merania, alebo zvýšenej réžii prenosu spôsobenej zložitejším spracovaním. Každopádne všetky hodnoty sa držia v rozmedzí hodnôt vyžadovaných doporučeniami kvality služieb. Reálny dopad nastavenia QoS bol pozorovateľný pri nahradení generovaného video prenosu skutočným TV streamom. Aj pri plnom zaťažení siete s QoS dochádzalo len k občasným výpadkom zvuku, kdežto v scenári bez QoS vypadol zvuk úplne a obraz bol takpovediac stojatý a plný rôznych artefaktov.

Problematika aplikácie kvality služieb v počítačových sieťach tak skutočne napĺňa teoretické predpoklady a potreby, pre ktoré boli tieto mechanizmy vyvinuté.

ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM UVEDENÝCH TABULIEK

ZOZNAM POUŽITEJ LITERATÚRY

[1] WANG, Zheng. Internet QoS: Architectures and Mechanisms for Quality of Service San Francisco: Morgan Kaufmann, 2001. 240 s. ISBN 1-55860-608-4

[2] FLANNAGAN, Michael E. Administering Cisco QoS for IP Network Syngress Publishing, 2001. 535 s. ISBN 1-928994-21-0

[3] FRANKEN, Leonard. Quality of Service Management: A Model-Based Approach. Centre for Telematics and IT, 1996. 267 s. ISBN 90-72125-56-8

[4] MOLNÁR, Karol. Moderní síťové technologie, Skripta FEKT VUT Brno, 2007

[5] KACÁLEK, Ján. Modely pro zajištení kvality služeb IP sítích [online]. 2006. [cit. 2008-11-15]
URL: <http://amarok.cesketelekomunikace.cz/xkacal00/index.php?action=intro>

[6] SZIGETI, Tim, HATTINGH, Christina. End-to-End QoS Network Design. Cisco Press, 2004. 734 s. ISBN 1587051760

[7] BEZPALEC, Pavel. Kvalita služeb datových sítí z hlediska VoIP [online]. 2006. [cit. 2008-11-22], URL:
<http://www.ip-telefon.cz/archiv/dok_osta/ipt-2006_Kvalita_sluzeb_VoIP.pdf>

[8] LEDVINA, Jiří. QoS v datových sítích, IntServ a DiffServ [online]. 2007. [cit. 2008-11-22], URL:
<http://www.kiv.zcu.cz/~ledvina/Prednasky-PSI-2007/qos-text.pdf.>

[9] MÁCHA, Jakub. Kontrola síťového provozu [online], FI MUNI, Brno 2000.
URL: <ftp://ftp.linux.cz/pub/linux/people/jakub_macha/traffic-control.ps>

[10] UBIK, S. QoS a diffserv - Úvod do problematiky [online]. 2000 [cit. 2008-12-10]
URL: <http://www.cesnet.cz/doc/techzpravy/2000-6/diffserv.html>

[11] MOLNÁR K. Mechanizmus diferencovaných služeb. [online], 2008, [cit. 2009-04-12], URL:<http://www.utko.feec.vutbr.cz/~molnar/mmos/QoS.pdf.>

[12] PUŽMANOVÁ R. Vývoj paketových sítí a postavení MPLS [online]. 2006. [cit.2008-12-13], URL: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=302>

[13] Multi-Protocol Label Switching Conformance and Performance Testing [online], MILLER Bruce, STEWART Elliott [online]. 2004, [cit.2008-12-13], URL: <http://www.ixiacom.com/library/white_papers/display?skey=mpls>

[14] IETF. SBM (Subnet Bandwidth Manager) : A Protocol for RSVP-based Admission Control over IEEE 802-style networks. [online]. 2000. [cit. 2008-12-13]. URL: <ftp://ftp.rfc-editor.org/in-notes/rfc2814.txt>

[15] Yee-Ting Li, SBM – Subnet Bandwidth Management [online]. 2003. [cit. 2008-12-12], URL: <http://www.hep.ucl.ac.uk/~ytl/qos/sbm_01.htm>

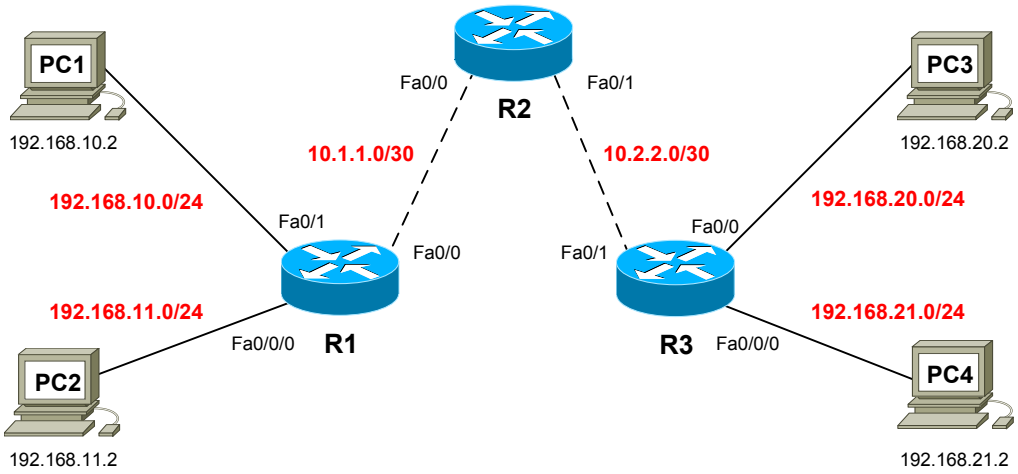
[16] AutoQoS – VoIP [oline], [cit. 2009-05-16], URL: <http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftautoq1.html>

[17] Cisco Systems, Cisco Modular Quality of Service Command Line Interface [online], 2005 [cit. 2009-05-16], URL: <http://www.cisco.com/en/US/technologies/tk543/tk545/technologies_white_paper09186a0080123415.pdf>

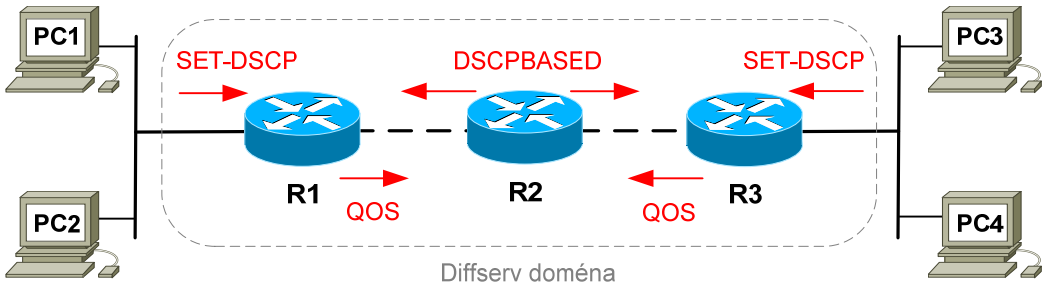
[18] Cisco Configuring the Modular Quality of Service Command-Line Interface. [online], [cit. 2009-05-16], URL: www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmcli2.html

PRÍLOHY

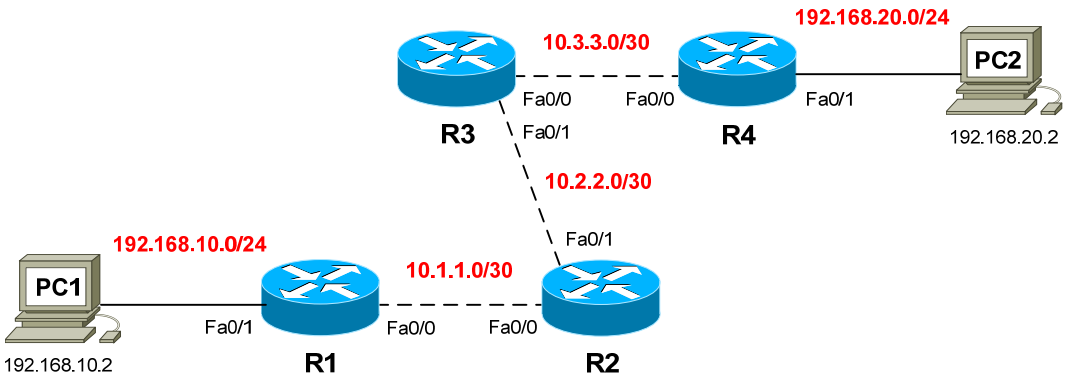
Príloha 1: Topológia zapojenia modelovej IP siete s jednou DS doménou, adresovacia tabuľka a zobrazenie aplikovaných politík v sieti



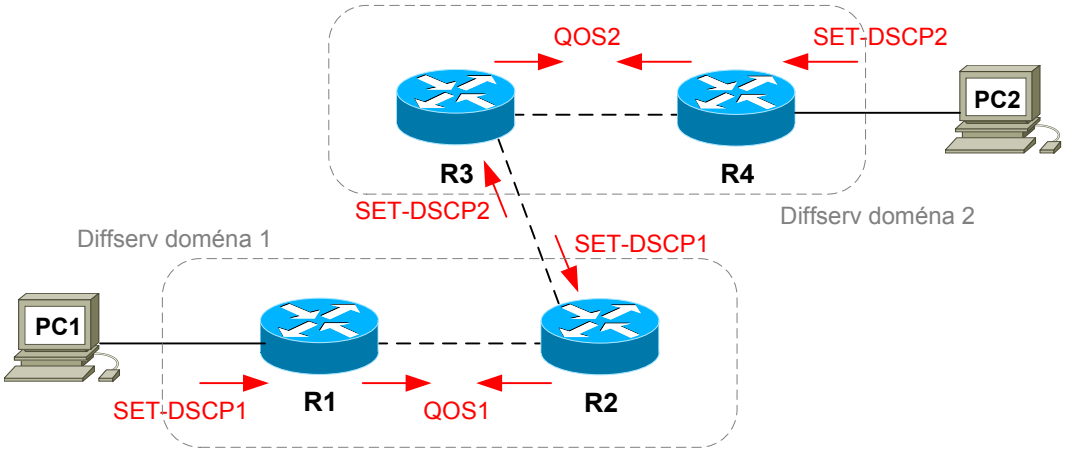
Zariadenie	Rozhranie	Adresa IP	Maska	Východzia brána
R1	Fa0/0	10.1.1.1	255.255.255.252	N/A
	Fa0/1	192.168.10.1	255.255.255.0	N/A
	Fa0/0/0	192.168.11.1	255.255.255.0	N/A
R2	Fa0/0	10.1.1.1	255.255.255.252	N/A
	Fa0/1	10.2.2.1	255.255.255.252	N/A
R3	Fa0/0	192.168.20.1	255.255.255.0	N/A
	Fa0/1	10.2.2.2	255.255.255.252	N/A
	Fa0/0/0	192.168.21.1	255.255.255.0	N/A
PC1	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.2	255.255.255.0	192.168.11.1
PC3	NIC	192.168.20.2	255.255.255.0	192.168.20.1
PC4	NIC	192.168.21.2	255.255.255.0	192.168.21.1



Príloha 2: Topológia zapojenia modelovej IP siete s dvoma Dsiffserv doménami, adresovacia tabuľka a zobrazenie aplikovaných politík v sieti



Zariadenie	Rozhranie	Adresa IP	Maska	Východzia brána
R1	Fa0/0	10.1.1.1	255.255.255.252	N/A
	Fa0/1	192.168.10.2	255.255.255.0	N/A
R2	Fa0/0	10.1.1.2	255.255.255.252	N/A
	Fa0/1	10.2.2.1	255.255.255.252	N/A
R3	Fa0/0	10.3.3.1	255.255.255.252	N/A
	Fa0/1	10.2.2.2	255.255.255.252	N/A
R4	Fa0/0	10.3.3.2	255.255.255.252	N/A
	Fa0/1	192.168.20.2	255.255.255.0	N/A
PC1	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.2	255.255.255.0	192.168.11.1



Príloha 3: Monitorovanie klasifikovaných tried prevádzky programom Cisco SDM (Security Device Manager)