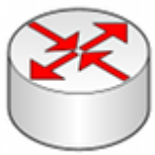
Portál pre odborné publikovanie ISSN 1338-0087

Preventívne metódy zabezpečenia kvality služby v IP

Mičuch Juraj · Elektrotechnika, Študentské práce

03.05.2010



Na zabezpečenie kvality služieb v prostredí IP existujú mnohé mechanizmy. Článok sa zameriava na preventívne metódy a predovšetkým na riadenie prístupu spojení AC (Admission Control). AC je veľmi dôležité z pohľadu zabezpečenia sieťových prostriedkov a predchádzania zahlteniu v sieti. V práci sú analyzované a vzájomne porovnané rôzne AC metódy z pohľadu IP sietí. Na záver sú uvedené metódy simulované v programe Matlab.

1 Úvod

Dlhé roky slúžil Internet zväčša pre potreby vedcov, ktorí ho využívali na výskum a komunikáciu medzi sebou. Ťažiskovými službami boli najmä email, prenos súborov a vzdialený prístup, ktoré pracovali v rámci datagramového modelu dobre. Revolúcia nastala s príchodom World Wide Web (WWW). Ten mal za následok rozmach takých služieb ako distribúcia videa cez Internet, IP telefónia a mnohé iné, čo prudko zvýšilo zaťaženie sietí. Mnohé nové aplikácie mali úplne iné požiadavky ako tie, pre ktoré bol Internet pôvodne navrhnutý. Ak sa napr. niekto snažil uskutočniť telefónny hovor, sieť mohla byť natoľko vyťažená, že v dôsledku oneskorenia bol rozhovor prenesený za hranicou zrozumiteľnosti. Preto bolo dôležité riešiť otázku kontroly a zaťaženia sietí.

Postupom času vznikli rôzne špeciálne skupiny zaoberajúce sa problematikou manažmentu v sieti a bolo navrhnutých niekoľko ochranných mechanizmov. Cieľom bolo zabrániť kritickým momentom ako zahltenie a zabezpečiť dostupnosť sieťových prostriedkov tým službám, ktoré boli označené ako uprednostňované, čiže boli najdôležitejšie z pohľadu zabezpečenie kvality služby QoS (Quality of Service). Takýmito službami sú video konferencia a VoIP, hromadne označované ako aplikácie v reálnom čase.

2 Existujúce riešenia pre zabezpečenie QoS

Všetky doteraz vyvinuté mechanizmy na zlepšenie kvality prenosu informácií v sieťach by sa dali zhrnúť do základných dvoch skupín: rezervovanie zdrojov a optimalizácia výkonnosti v sieti. Ak by sme to zjednodušili, tak sieť pozostáva zo zdieľaných zdrojov ako napr. šírka prenosového pásma. Sieť, ktorá podporuje QoS, sa musí aktívne podieľať na riadení týchto zdrojov a jej úlohou je rozhodovať komu, kedy a koľko zdrojov pridelí.

Túto úlohu na seba prevzali v IP sieťach architektúry Diferencovaných služieb a Integrovaných služieb. Druhá alternatíva, optimalizovanie výkonnosti, sa zaoberá otázkou ako efektívne organizovať zdroje siete, ako maximalizovať pravdepodobnosť doručenia informácií s požadovanou kvalitou a minimalizovať náklady na doručenie. Z koncepcií založených na daných postupoch je najznámejšia MPLS (MultiProtocol Label Switching).

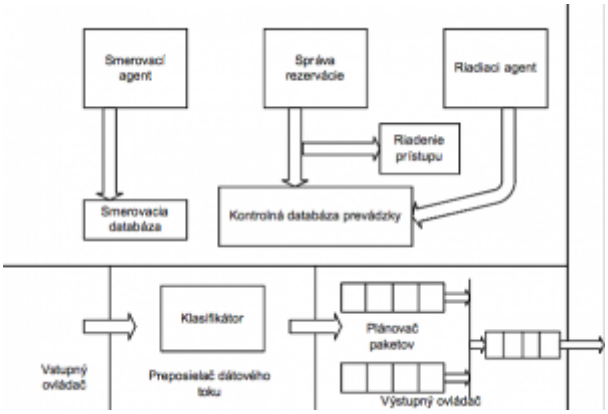
2.1 Integrované služby

Integrované služby IntServ (Integrated Services) je pomenovanie pre skupinu rozšírení a vylepšení aplikovaných na tradičný model služieb v Internete, ktorých cieľom je umožniť QoS pre rôzne aplikácie. Podstata architektúry IntServ spočíva v rezervovaní sieťových prostriedkov *per flow*, čiže pre jednotlivé dátové toky. Kvôli zlepšeniu manipulácie s dátami a zefektívneniu dosahovania kvality služby v IntServ hovoríme o troch triedach služieb, ktoré sa líšia na základe tolerovaného oneskorenia aplikácií:

- trieda garantovaných služieb – vyžaduje dodržanie presne stanoveného oneskorenia (videokonferencia, prenos hlasu v reálnom čase)
- trieda služieb s riadením záťaže – povoľuje občasné zvýšenie oneskorenia (aplikácie nie v reálnom čase)
- trieda best effort služieb – klasické služby bez požiadaviek na QoS (Web, FTP, email)

Hlavné nástroje dosahovania QoS v architektúre IntServ, obr. 1, sú riadenie prístupu AC a protokol RSVP. V oboch prípadoch je nutné pre správnu činnosť vedieť charakterizovať dátové toky, pre ktoré sa zabezpečuje QoS. Nositeľmi informácií o jednotlivých tokoch sú správy flowspec. Jeden typ správ, Rspec, definujú požadovanú QoS; druhý typ správ, Tspec, popisuje parametre toku. Na základe týchto informácií pracuje blok AC v architektúre IntServ. Jeho úloha je jednoduchá a v podstate jedna z najdôležitejších pri zabezpečovaní QoS.

Ak príde nový tok do uzla v sieti, AC skontroluje Rspec a Tspec dátového toku a rozhodne, či mu umožní komunikáciu bez toho, aby ovplyvnilo kvalitu už predtým povolených tokov. Ak vyhovie podmienke AC, tok je pustený ďalej. Rozhodujúce kritérium je závislé na žiadajúcej službe. Ak sa rozhoduje o službe s riadením záťaže, podmienky nemusia byť príliš kritické a postačuje rozhodovanie na základe predchádzajúcich skúseností. Pri garantovaných službách musí byť algoritmus pre výpočet podmienky čo najpresnejší, aby zabezpečil požadovanú QoS. AC je detailnejšie rozobrané v nasledujúcej kapitole.



Obr. 1. Implementácia Intserv v smerovači.

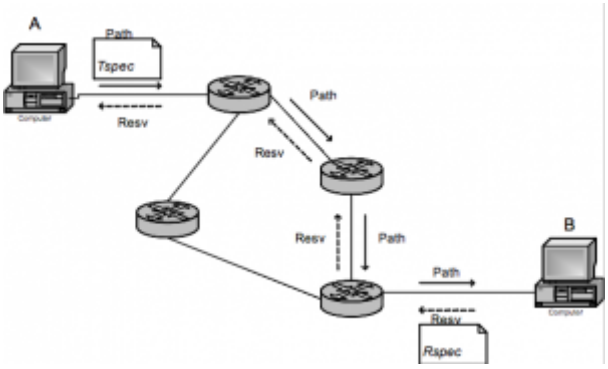
2.2 Protokol RSVP

V spojovo orientovaných sieťach, aby mohla prebiehať komunikácia, existujú mechanizmy, ktoré majú za úlohu vystavať cestu pre posielané dáta. Naproti tomu Internet túto možnosť nemá a najvážnejšie sa dôsledky plynúce z absencie podobného mechanizmu prejavujú pri aplikáciách v reálnom čase. Nutné je preto nájsť spôsob, ktorým by sa dosiahol rovnaký efekt ako pri spojovo orientovaných sieťach. Odpoveďou na toto hľadanie je protokol RSVP (Resource Reservation Protocol). RSVP je signalizačný protokol pre Integrované služby a nie smerovací, akoby sa mohlo zdať. Správy, ktoré RSVP posiela, sú smerované podľa algoritmov na príslušnom smerovači.

Zjednodušene sa dá povedať, že úlohou RSVP je zabezpečiť cestu, kadiaľ sa budú posielať všetky dáta od jedného zdroja. Vytvorená cesta však nemusí byť rovnaká počas celej komunikácie medzi zdrojom a príjemcom. Proces rezervovania zdrojov sa periodicky opakuje a výhodou je, že RSVP môže zmeniť cestu, ak sa vyskytne situácia na aktuálnej trase, ktorá by zhoršovala kvalitu prenosu. Na druhej strane opakovanie rezervácie má nezanedbateľný vplyv na záťaž smerovačov.

Rezervovanie zdrojov má dve fázy: vytvorenie cesty pre dáta a alokácia zdrojov. Na tieto činnosti sa používa rôzne druhy správ ako: Path, Resv a iné. V nasledujúcich riadkoch je v skratke vysvetlená podstata RSVP. Nech koncové zariadenie A , obr. 2, je zdrojom informácií a chce poslať dáta užívateľovi B. Aby prebehla rezervácia sieťových prostriedkov, pošle správu Path, ktorá obsahuje charakteristiku budúcej prevádzky Tspec, na adresu užívateľa B.

Správa sa pohybuje v sieti podľa príslušných smerovacích tabuliek, pričom každý uzol predtým ako správu pošle ďalej, vloží do nej informácie o svojich voľných kapacitách. Keď správa Path dorazí na cieľovú adresu, užívateľ B pošle požiadavku na rezerváciu zdrojov. Vyšle správu Resv so špecifikáciou Rspec späť cez všetky uzly, cez ktoré prišla správa Path. Ak koncové zariadenie A dostane správu Resv, boli rezervované sieťové zdroje pre dané spojenie.



Obr. 2. Princíp rezervácie zdrojov v sieti.

2.3 Diferencované služby

Zabezpečenie QoS ponímajú Diferencované služby DiffServ (Differentiated Services) opačne ako to bolo v architektúre IntServ. Namiesto vytvárania dátových tokov je snahou DiffServ vytvoriť triedy rôznej priority, do ktorých sa budú zadeľovať dáta. To,

že dáta majú nejakú príslušnosť k triede, sa zohľadňuje pri smerovaní a tiež pri zahadzovaní paketov v kritických situáciách. Označenie jednotlivých paketov sa robí pomocou poľa ToS (Type of Service) v hlavičke IPv4. Z ôsmich bitov, ktoré sú k dispozícii, sa využíva prvých šesť, ostatné sa momentálne nevyužívajú. Hodnota zapísaná vnútri poľa sa označuje ako DSCP (Differentiated Services Code Point) a signalizuje, ako sa má zaobchádzať s paketom s touto hodnotu.

Správanie sa uzlu voči konkrétnemu paketu PHB (Per-Hop Behavior) je rôzne pre rôzne hodnoty DSCP. Dôležité je povedať, kto zapisuje hodnoty DSCP. V prípade, že je vytvorená oblasť DiffServ, rozoznávame dva typy smerovačov: smerovače na hranici domény a vo vnútri domény. Úlohou hraničných smerovačov je práve zapisovať hodnotu DSCP.

K činnostiam, ktoré tieto smerovače vykonávajú patria aj meranie, tvarovanie prevádzky a porovnávajú prevádzku s prevádzkovým profilom. Keď už je paket označený a prechádza vnútrom DiffServ domény, vnútorné smerovače aplikujú PHB prislúchajúce DSCP na konkrétny paket. Súčasťou činností vykonávaných vnútornými uzlami sú aj stanovovanie prenosového pásma a riadenie prístupu. Existujú dva typy PHB, ktoré sa aplikujú:

1. Urýchlené smerovanie EF (Expedited Forwarding) – pakety by mali byť preposielané s minimálnym oneskorením, minimálnou stratou, mali by mať minimálny jitter a presne stanovenú šírku prenosového pásma. Dané podmienky presne charakterizujú potreby aplikácií v reálnom čase. Pre EF sa používa hodnota DSCP 101110.
2. Zabezpečené smerovanie AF (Assured Forwarding) – v tomto prípade sú parametre (ako oneskorenie a jitter) nie až tak dôležité ako správne doručenie paketov. Pakety sa vyznačujú vysokou pravdepodobnosťou doručenia pokiaľ spĺňajú vopred stanovené podmienky. V rámci AF existujú štyri triedy, z ktorých každá trieda má tri podtriedy.

2.4 MPLS

V mnohých IP sieťach sú pakety smerované staticky, na základe najkratšej cesty. To môže viesť k nerovnomernému využívaniu prenosového pásma v rámci siete. Ak napríklad v jednom mieste siete nastane preťaženie, iné miesto siete môže byť využité len minimálne. Riešením tohto problému sa zaoberá práve MPLS (Multiprotocol Label Switching). Nové riešenie, ktoré MPLS prinieslo, spočíva v tom, že pri smerovaní sa využívajú špeciálne značky (návestia) namiesto informácií obsiahnutých v IP hlavičke. Výsledkom je smerovanie jednoduchšie a rýchlejšie.

Celý proces začína príchodom paketov na hraničné smerovače LER (Label Edge Router) MPLS domény, kde sa pakety zadeľujú do tried FEC (Forwarding Equivalence Class) na základe určitého kritéria (rovnaká QoS, cieľová adresa, atď.). Príslušnosť paketov k FEC sa určí raz, a potom všetky pakety danej FEC sú označované značkami o dĺžke štyri byty. Pre každú triedu je vytvorená vnútri MPLS domény cesta, označovaná ako LSP (Label Switched Path), kadiaľ budú pakety smerované.

Keď označený paket, nasmerovaný na LER po konkrétnej LSP, dorazí na vnútorný smerovač LSR (Label Switch Router), už nedochádza k analyzovaniu IP hlavičky. Namiesto toho sa prečíta informácia v návestí a stanoví sa ďalší uzol a nové návestie,

ktoré nahradí starú značku. Pri výstupe paketu zo siete používajúcej MPLS sa na LER odstráni značka a paket sa ďalej pohybuje v pôvodnom formáte. V záujme maximalizovania QoS sa MPLS rozširuje o prvky DiffServ a tým zvyšuje možnosť kontroly a riadenia siete.

3 Riadenie prístupu

V rámci viacerých metód zabezpečujúcich kvalitu služieb sa spomína potreba riadiť prístup prichádzajúcich dátových tokov. AC má nezanedbateľný význam, pretože ako prvé sa zaoberá zabezpečovaním kvality spojenia a má aj najväčší vplyv na QoS. Základnou úlohou AC je pokúsiť sa odhadnúť šírku prenášaného pásma prislúchajúcu dátovému toku, ktorý žiada o prenos a následne rozhodnúť, či je možné zabezpečiť danú šírku pásma. Hlavnou oblasťou pôsobnosti riadenia prístupu sú služby citlivé na oneskorenie a jitter. Túto oblasť predstavujú predovšetkým prenos hlasu a videa, aplikácie v reálnom čase.

Známe je množstvo metód, ktoré riešia problematiku alokácie pásma, rozdiel medzi nimi spočíva predovšetkým v rôznych typoch prevádzkach, ktoré používajú pri svojich výpočtoch. Ak by sme chceli odlíšiť jednotlivé metódy a zatriediť ich, jedným z kritérií by mohol byť spôsob realizácie. Niektoré AC sú založené na matematických výpočtoch a štatistických ukazovateľoch, iné na meraní prevádzky. Ďalší druh kategorizácie by bol podľa toho, či využívajú pre svoju činnosť vyrovnávacie pamäte alebo nie a pod. Od AC sa očakávajú určité vlastnosti, ktoré by mali spĺňať a ich dôležitosť je pre každého prevádzkovateľa iná, no vo všeobecnosti by mali:

- predovšetkým dodržať QoS prichádzajúceho spojenia a zároveň neovplyvniť ostatné spojenia
- reagovať resp. rozhodnúť v čo najkratšom čase, aby nespôsobovali oneskorenie
- efektívne prideľovať dostupné pásmo a maximalizovať tak využitie kapacít
- byť ľahko implementovateľné s možnosťou obsluhy a úpravy

Na začiatku je dobré zamyslieť sa nad AC z pohľadu celkovej architektúry siete a s tým súvisiacej lokalizácie riadenia prístupu. Ako bolo spomenuté v predchádzajúcich kapitolách, AC je súčasťou tak architektúry IntServ ako aj DiffServ. Existuje viacero názorov na použitie AC v architektúre Diferencovaných služieb. Jednou z možností je aplikovať rozhodovacie kritérium na hranicu DiffServ domény, zatiaľ čo vnútorné smerovače vypočítavajú šírku prenosového pásma a informácie o nej posielajú na hraničné uzly. Umiestnenie AC na hranici domény dáva možnosť kontrolovať množstvo prevádzky vstupujúcej do siete. Ak sa pozrieme na sieť všeobecne, nie je až tak dôležitá prítomnosť riadenia prístupu v chrbticových vedeniach, kde sú vysoké prenosové rýchlosti a aplikované metódy dimenzovania, ako v prístupových sieťach.

Ako už bolo spomenuté, sú dve základné kategórie metód z pohľadu zdrojových informácií použitých pri rozhodovaní. Riadenie prístupu založené na prevádzkových parametroch PBAC (Parameter-Based Admission Control) potrebuje na adekvátne zabezpečenie QoS poznať charakteristiku zdroja. Vďaka parametrom získaných od zdroja stanoví metóda rozhodovacie kritérium a následne určí či spojenie prijme alebo nie. Týmto postupom sa docieli vysoké využitie poskytovaných sieťových prostriedkov. Problémom však je, že požadujúcu charakteristiku je veľmi ťažké stanoviť vopred

a parametre musia verne opisovať skutočnosť na to, aby bol algoritmus dobrý. Ak tomu tak nie je, pridelené pásmo môže byť značne veľkorysé, čo vedie k neefektívnosti a plytvaniu prenosového pásma.

V prípade AC založených na meraní MBAC (Measurement-based Adimission Control) sa namiesto spoľahnutia na parametre, riadenie prístupu snaží naučiť sa charakteristiku tokov prostredníctvom vlastných meraní, ktoré prebiehajú v reálnom čase. K svojej činnosti potrebujú len minimálne znalosti o zdroji, z ktorého prichádza spojenie do siete. Sú algoritmy [7], ktorým stačí poznať charakteristiku zdroja len na začiatku, ešte pred tým ako bol prijatý nový tok. Keď už je spojenie prijaté, AC používa pri budúcich rozhodovaniach informácie radšej z vlastných meraní ako parametre od zdroja. V iných metódach [9] je pre vykonávanie AC potrebných len minimum informácií ako napr. špičková prenosová rýchlosť zdroja. Okrem základných dvoch skupín AC existujú metódy, hybridné AC, ktoré spájajú v sebe výhody algoritmov založených na meraní a metód PBAC.

3.1 Metódy riadenia prístupu

Napriek tomu, že existuje mnoho metód a algoritmov riadenia prístupu, všetky majú spoločný základ, na ktorom sa odvíjajú a ku ktorému spejú. Matematicky vyjadrené to znamená splniť nasledovnú nerovnosť:

Formula does not parse (2)

Koeficient k, ktorým prenásobujeme dostupnú kapacitu, je menší ako jedna a je volený podľa skúseností správcov siete, zvyčajne 0,95 [10].

Pre lepšie porovnanie sa zameriame iba na metódy bez vyrovnávacích pamätí. Nasledujúci algoritmus v [10], ktorý k svojej činnosti potrebuje informácie od zdroja (PBAC), je založený na odhadovaní efektívnej šírky prenosového pásma. Pod pojmom efektívna šírka sa rozumie minimálna hodnota prenosového pásma, ktorá dokáže zabezpečiť požadovanú QoS. Konkrétna hodnota efektívnej šírky sa nachádza medzi špičkovou prenosovou rýchlosťou a strednou hodnotou prenosovej rýchlosti.

Predpokladom tejto metódy je, že výsledná prevádzka zo všetkých zdrojov vstupujúca do oblasti rozhodovania má Gaussovo rozdelenie. Ak označíme m ako priemernú prenosovú rýchlosť agregovanej premávky, σ ako štandardnú odchýlku agregovanej prenosovej rýchlosti a ϵ ako hornú hranicu pravdepodobnosti pretečenia, potom môžeme napísať vzťah pre efektívnu šírku ako:

$$c = m + a'\sigma \tag{3}$$

kde

$$a' = \sqrt{-2ln(\epsilon) - ln(2\pi)} \tag{4}$$

Tento model však nevystihuje reálne podmienky v IP sieti, pretože vždy je nutná prítomnosť aspoň malej vyrovnávacej pamäti. Za zmienku stojí tiež to, že prichádzajúca prevádzka dosahuje charakteristiku Gaussovho rozdelenia iba v prípade

vysokého počtu zdrojov.

Ďalší algoritmus, ktorý je zo skupiny bez vyrovnávacej pamäte, je určitou variáciou na vzťah (3). Odlišuje sa však tým, že parametre potrebné pre výpočet získava meraním. Meranie údajov priemerná rýchlosť $m_{meraná}$ a rozptyl (variancia) σ^2_{merana}meraná prebieha vo vstupnej fronte v rámci celkovej už prijatej prevádzky. K tomu, aby sa dal urobiť odhad prenosovej kapacity, potrebuje algoritmus poznať špičkovú prenosovú rýchlosť toku žiadajúceho o vstup $p_{nový}$. Potom, podľa [9] za predpokladu, že zdroj žiadajúci o prístup bude vysielať svojou maximálnou rýchlosťou, odhad prenosového pásma je:

$$c_{odhad} = m_{merana} + p_{novy} + a' \sqrt{\sigma^2_{merana}} \tag{5}$$

kde *a'* sa vypočíta pomocou vzťahu (4). Na základe odhadu šírky prenosového pásma a celkovej prenosovej kapacity výstupnej linky C, AC rozhodne či povolí alebo zamietne prístup do siete:

$$\left(c_{odhad} \times APF\right) \leq C \text{ prijať} \tag{6}$$

$$\left(c_{odhad} \times APF\right) > C \text{ zamietnuť} \tag{7}$$

Pomocou koeficientu APF (Admission Policy Factor) sa korigujú nepresnosti tejto metódy a tiež vyjadruje, aké prísne sú nároky na požadované prenosové pásmo. Nepresnosti, s ktorými sa APF vyrovnáva sú dvojakého druhu: prvé sú spôsobené rôznorodosťou prevádzky a zhlukovým charakterom tokov paketov, druhé sú chyby pri meraní. APF sa počíta na základe porovnania meraných hodnôt s hodnotami referenčného zdroja [9]. Ak je vypočítaná hodnota menšia ako jedna, APF sa stanoví ako 1.

Nasledujúca metóda je založená na stanovení hornej hranice prenosového pásma. K informáciám, ktoré potrebuje poznať, patria špičková prenosová rýchlosť p a priemerná rýchlosť m. Teoreticky táto metóda vychádza z Hoeffdingovej hranice, pričom parameter p pozná od zdroja a priemerná rýchlosť je meraná. Postupnou aproximáciou, ukázanou v [11], dostávame vzťah pre odhad efektívnej šírky:

$$c = \frac{1}{s} \sum_{i=1}^{n} ln \left(\frac{\sum_{j=1}^{n} m_j + \sum_{j=1}^{n} \frac{p_i}{e^{sp_i} - 1} e}{n} . \frac{e^{sp_i}}{p_i} \right) + \frac{\gamma}{s} \tag{8}$$

kde pi a mi sú špičková resp. priemerná rýchlosť jednotlivých tokov, $\gamma = -ln(\epsilon)$. Parameter s vyjadruje kompromis medzi využitím prenosovej kapacity a stratou paketov [12]. Jeho optimálna hodnota je pre každý zdroj iná a dá sa vypočítať ako:

$$s = \sqrt{\frac{\gamma}{\frac{1}{8} \sum_{j=1}^{n} p_i^2 - \frac{1}{2n} \left(\sum_{j=1}^{n} m_i - \frac{1}{2} \sum_{j=1}^{n} p_i \right)}} \tag{9}$$

Najväčšou výhodou tejto metódy je malé množstvo parametrov potrebných pre výpočet pásma. Vylepšením vyššie spomenutej metódy je pribratie ďalšieho parametra do výpočtu, ktorý by mal stanoviť hranicu alokovaného pásma presnejšie [11]. Na

zlepšenie odhadu pásma sa využíva meranie rozptylu rýchlostí, čo má veľký význam pri zdrojoch s premenlivou rýchlosťou vysielania. Vzťah pre výpočet celkovej efektívnej šírky je:

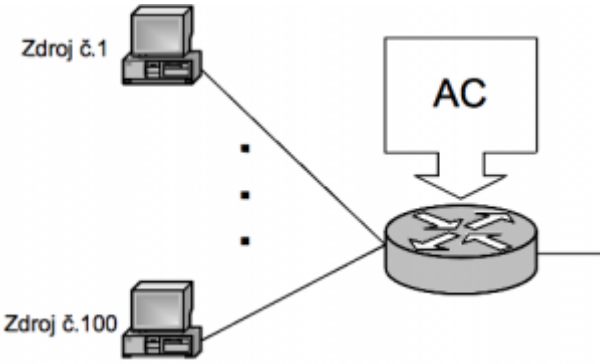
$$c = \frac{1}{s}\sum_{i=1}^{n} ln\left(\frac{\sum_{j=1}^{n}\sigma_j^2+\sum_{j=1}^{n}\frac{p_j^2}{e^{sp_j-spj-1}}e}{n}.\frac{e^{sp_i-sp_i-1}}{p_i^2}\right) + \sum_{i=1}^{n} m_i + \frac{\gamma}{s} \quad (10)$$

kde σ_j^2 je rozptyl rýchlostí jednotlivých tokov. Takisto je definované pre túto metódu optimálne s:

$$s = \sqrt{\frac{\gamma}{\frac{1}{2}\sum_{j=1}^{n}\sigma_j^2+\frac{1}{18}\sum_{j=1}^{n}p_j^2-\frac{1}{18n}\left(\frac{1}{2}\sum_{j=1}^{n}p_j\right)}} \quad (11)$$

3.2 Simulácia metód riadenia prístupu

V nasledujúcej podkapitole bude snahou nasimulovať jednotlivé metódy a porovnať ich medzi sebou. Na zhodnotenie jednotlivých algoritmov riadenia prístupu bola navrhnutá topológia siete podľa obr. 3 s využitím programu Matlab.

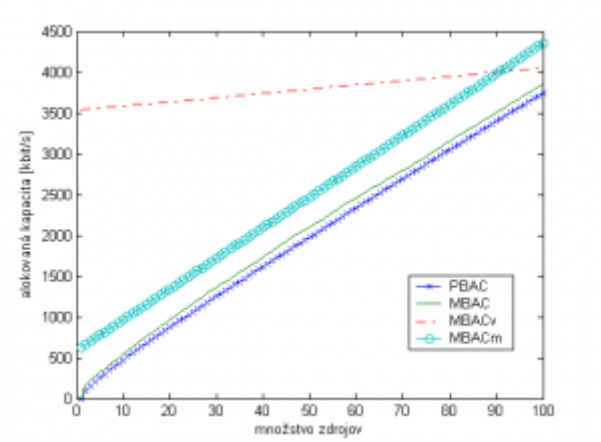


Obr. 3. Topológia simulovanej siete.

Situácia na obr. 3 znázorňuje uzol siete, na ktorom je aplikovaná metóda riadenia prístupu. Predpokladáme, že do daného uzla vstupuje 100 zdrojov. Každý z týchto zdrojov je charakterizovaný pomocou vzorky 1000 náhodne vygenerovaných hodnôt, čo symbolizuje hodnoty zachytené v čase. Náhodnosť generovaných čísel predstavuje kolísanie rýchlosti, teda neuvažujeme zdroj s konštantnou rýchlosťou. Maximálna hodnota prenosovej rýchlosti pre všetky zdroje sa pohybuje v rozmedzí 0 až 64 kbit/s. Hodnota pravdepodobnosti straty paketov bola stanovená na $\epsilon = 10^{-3}$ pri všetkých simuláciách, čo zodpovedá situácii v reálnej sieti. Do simulácií boli zahrnuté všetky štyri metódy spomenuté v kapitole 5. 1. Prvá (3) bude označovaná ako PBAC, metóda (5) ako MBAC, (8) ako MBACm a algoritmus (10) ako MBACv.

V prvom prípade bola vykonaná simulácia pre zistenie správania sa AC na základe počtu zdrojov, obr. 4. Meranie parametrov prebiehalo na jednej časovej vzorke pri agregovanej prevádzke. Ako možno vidieť metóda MBACv pri malom počte zdrojov určila hornú hranicu alokovaného pásma značne väčšiu ako ostané metódy, z čoho

vyplýva nízka flexibilita metódy.

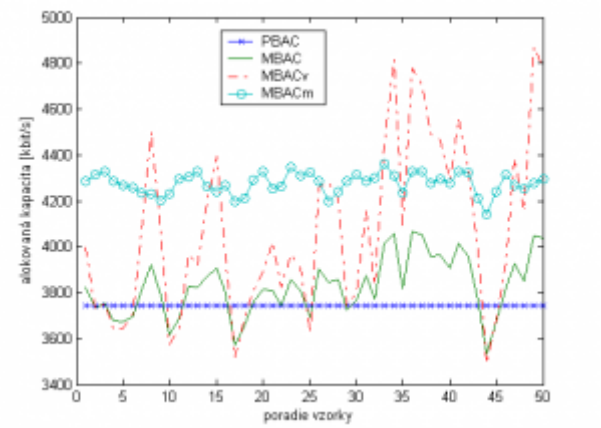


Obr. 4. Závislosť alokovaného pásma od počtu zdrojov.

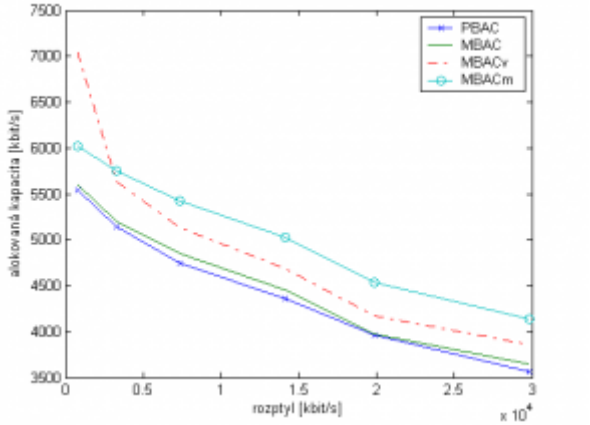
Obmedzenie len pre vyšší počet zdrojov výrazne zužuje pole pôsobnosti algoritmu. V druhom prípade bolo cieľom simulácie poukázať na alokáciu kapacity v čase. Každý časový okamih bol symbolizovaný vzorkou dvadsiatich hodnôt prenosových rýchlostí, ktorú metódy MBAC využívali na meranie. Pre rôzne časové okamihy boli vybrané rôzne vzorky. Meranie prebiehalo pri počte zdrojov 100 a výstupom tohto merania je graf na obr. 5. Ako možno vidieť, splnili sa teoretické predpoklady pre metódy MBACv a MBACm.

Meranie rozptylu pri algoritme (10) je dôvodom, že MBACv lepšie reaguje na momentálne výkyvy rýchlostí počas prenosu dát. Keďže PBAC počas prenosu nemení parametre poskytnuté AC, úroveň alokovanej kapacity je stále rovnaká. Dôsledkom uvedenej vlastnosti je zvyšovanie oneskorenia pre tie pakety, ktoré majú rýchlosť vyššiu ako je táto úroveň. Určitým kompromisom medzi flexibilitou na zmenu rýchlostí a veľkosťou alokovaného pásma predstavuje metóda MBAC.

Nakoľko v troch uvedených metódach sú výpočty založené na parametri rozptylu, tretia simulácia poukazuje na vplyv tohto údaju na výslednú vypočítanú kapacitu. Meranie prebiehalo pri 100 zdrojoch a meniacom sa rozptyle celkovej agregovanej prevádzky. Z obr. 6 možno pozorovať, že všetky metódy s rastúcim rozptylom prevádzky znižujú odhad na celkovú kapacitu. Na základe tohto správania nie je efektívne nasadzovať AC na zdroje s konštantnou prenosovou rýchlosťou. Uvedená vlastnosť sa s výhodou môže uplatniť pre on/off zdroje (VoIP).



Obr. 5. Priebeh alokovanej kapacity v čase.



Obr. 6. Závislosť alokovanej kapacity od rozptylu prevádzky.

4 Záver

V tejto práci boli naštudované a priblížené viaceré mechanizmy na zabezpečenie QoS v sieťach IP. Bola predstavená ich približná architektúra a základné princípy. Dôkladnejšie boli rozobrané predovšetkým metódy riadenia prístupu, ich úlohy a klasifikácia. Posledná časť práce bola zameraná na konkrétne štyri metódy AC a ich simuláciu v prostredí kolísavých prenosových rýchlostí. Boli overené ich teoretické predpoklady a zhodnotené ich výsledky zo simulácií.

5 Referencie

1. BRADEN, R. et al.: Integrated Services in the Internet Architecture: An Overview. RFC 1633, IETF, 1994.
2. BLAKE, S. et al.: An Architecture for Differentiated Services. RFC 2475, IETF, 1998.
3. BRADEN, R. et al.: Resource ReSerVation Protocol (RSVP) – Version 1: Functional Specification. RFC 2205, IETF, 1997.
4. ROSEN, E. et al.: Multiprotocol Label Switching Architecture. RFC 3031, IETF, 2001.
5. FARREL, A.: Network Quality of Service. Morgan Kaufman, 2008. ISBN 9780123745972.
6. PARK, K. I.: QoS in Packet Networks. Springer, 2004. ISBN 0-387-23390-X.
7. KASIGWA, J., BARYAMUREEBA, V., WILLIAMS, D.: Dynamic admission control for Quality of Service in IP Networks. Proceedings of world academy of science, engineering, end technology, Volume8, 2005. ISSN 1307-6884.
8. JAMIN, S., SHENKER, S., ZHANG, L., CLARK, D.: An Admission Control Algorithm for Predictive Real-Time Service (Extended Abstract). Lecture Notes In Computer Science, Vol. 712, 1992, pp. 349 – 356.
9. GEORGULAS, S., TRIMINTZIOS, P., PAVLOU, G., HO, K.: Measurement-based Admission Control for Real-time Traffic in IP Differentiated Services Networks. Proc. ICT 2005, 2005.
10. DAVY, A., BOTVICH, D., JENNINGS, D.: Empirical Effective Bandwidth Estimation for IPTV Admission Control. Real-Time Mobile Multimedia Services, 2007, pp. 125-137. ISSN 0302-9743.
11. TURÁNYI, Z., VERES, A., OLÁH, .: A family of measurement-based admission control algorithms. IFIP Conference Proceedings, Vol. 127, 1998, pp. 153 – 164. ISBN 0-41-

-83730-7.
12. GIBBENS, R. J., KELLY, F. P.: Measurement-based connection admission control. 15th International Teletraffic Congress Proceedings, 1997.

Spoluautorom článku je Ivan Baroňák, Slovenská technická univerzita v Bratislave, Fakulta elektrotechniky a informatiky,
Katedra telekomunikácií, Ilkovičová 3, 812 19 Bratislava