SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE U SPLITU

Kvaliteta usluge u telekomunikacijskim mrežama (DET036)

Predavanja

Toni Jončić

SPECIJALISTIČKI DIPLOMSKI STRUČNI STUDIJ

Sadržaj

PREDAVANJE 1 – Uvod u kvalitetu usluge u telekomunikacijskim mrežama

Pregled stanja današnjih telekomunikacija

Pratimo li udio uporabe starih fiksnih CS mreža u sveukupnim telekomunikacijama, vidimo da njihova uporaba konstantno opada, a da se sve više koriste mobilne mreže i usluge uz značajan rast korištenja širokopojasnog pristupa internetu. Ove značajne promjene na telekomunikacijskom tržištu omogućuje napredak tehnologije, primjerice razvoj bežičnih širokopojasnih tehnologija i tehnologija pokretne mreže te širenje primjene protokola IP.

Samim pogledom na trend događanja jasno nam je da će klasične fiksne CS (Circuit Switched) mreže uskoro potpuno nestati, a razvoj telekomunikacija vodi nas prema takozvanim mrežama slijedeće generacije (NGN -*Next Generation Networks*). koje će se u potpunosti zasnivati na IP tehnologiji.

Konvergencijski procesi u telekomunikacijama

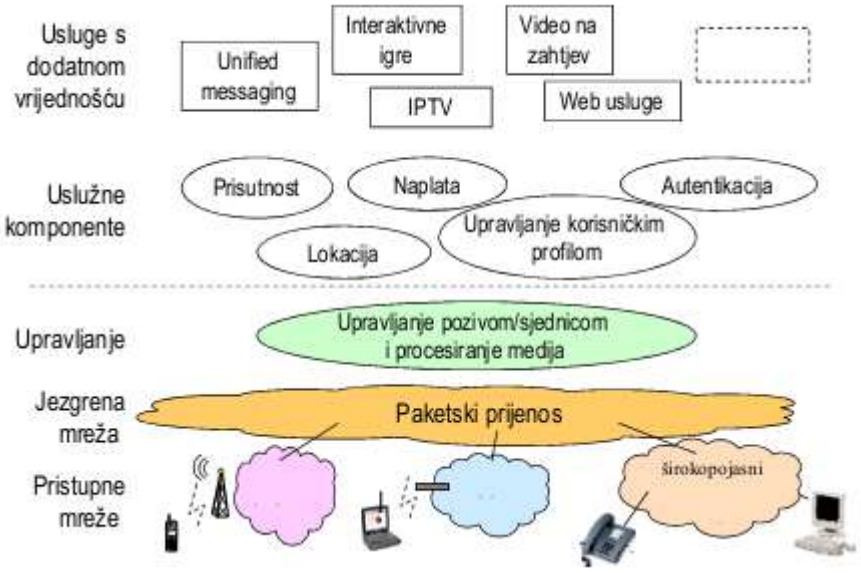
konvergencija = približavanje, put prema nekoj točki

Postoji više različitih pogleda na konvergenciju, a stoga i definicija konvergencije. Primjerice, s **gledišta tehnologije**, konvergencija se definira kao evolucijski proces koji objedinjuje i povezuje telekomunikacije, Internet, informacijsku tehnologiju i elektroničke medije, a s ciljem razvoja naprednih usluga koje koriste različite širokopojasne pristupne tehnologije. Ovdje se konvergencija obično promatra kroz **konvergenciju usluga**, konvergenciju terminala, i konvergenciju mreže. S gledišta medija, konvergencija se definira kao tok sadržaja preko različitih medijskih platformi, suradnja među različitim medijskim industrijama i migracijsko ponašanje publike koja će „učiniti sve da pronađe željenu vrstu zabavnog medijskog doživljaja“. Konvergencija usluga se odnosi na dostupnost usluga s različitih terminala i u različitim mrežama, a da se pri tom koriste standardna ujednačena sučelja koja olakšavaju korištenje usluga. Primjerice, korisnik koristi uslugu trenutnog poručivanja na osobnom računalu ili pokretnom telefonu, a pri tom je očuvana lista njegovih kontakata neovisno o terminalu, dok su grafička sučelja aplikacije vizualno gotovo identična na različitim terminalima. Sljedeći je primjer objedinjavanje govorne, internetske i televizijske usluge preko raznih pristupnih mreža, uz vođenje računa o svojstvima korisnikovog uređaja i pristupne mreže. **Konvergencija terminala** se odnosi na integraciju različitih svojstava i sposobnosti u niz terminala, umjesto korištenja posebnih namjenskih uređaja. Primjerice, današnji su terminali obogaćeni podrškom za različite pristupne mreže te imaju integriranu kameru i MP3 player. Konvergencija terminala nadalje omogućuje jedinstvenu prijavu, identifikaciju i autentifikaciju korisnika, neovisno o uređaju. Kada se govori o **konvergenciji mreža**, podrazumijeva se objedinjena slojevita mrežna arhitektura za pružanje raznovrsnih usluga, npr. sustav IMS omogućuje pružanje višemedijskih usluga u fiksnoj i pokretnoj mreži.(npr. zajednički billing sustav, sustav autentikacije,..itd.)

Važno je uočiti međuovisnost različitih vrsta konvergencije, te je npr. za uslugu objedinjenog poručivanja koja obuhvaća različite oblike komunikacije među korisnicima (e-mail poruke,

kratke tekstualne i govorne poruke) nužno osigurati konvergenciju usluga i mreža, dok je za neometano vertikalno prelaženje među različitim pristupnim mrežama tijekom sjednice nužnapotpora na terminalu i u mreži. Važno je naglasiti i prednosti koje konvergencija donosi korisniku, a to su:

- mogućnost uporabe istog uslužnog okruženja na različitim terminalima (osobna pokretljivost, ista usluga na različitim terminalima) ali i jednog sučelja prema svim uslugama (jedan terminal za pristup svim uslugama),
- združivanje pretplate za usluge fiksne, pokretne i širokopojasne mreže uz objedinjavanje svih troškova na jednom računu uz jednostavniju kontrolu i potencijalno nižu cijenu, i
- jedinstvena „prisutnost“ u objedinjenoj mrežnoj infrastrukturi (npr. jedinstveni broj, jedinstveni spremnik poruka, jedan adresar, kalendar, osobni digitalni sadržaj).



Konvergencijski procesi su prije svega usmjereni razvoju novih naprednih usluga prilagođenih osobnim potrebama krajnjeg korisnika. U takvom okružju, cilj mreža sljedeće generacije je omogućiti ponudu raznovrsnih usluga preko objedinjene infrastrukture za prijenos sadržajnih i upravljačkih informacija, neovisno o načinu pristupa kako je definirano preporukom ITU-T Y.2001. Stoga je definirana nova mrežna arhitektura koja osigurava interoperabilnost s postojećim fiksnim i pokretnim mrežama, kao i otvorenost prema novim pristupnim tehnologijama. Ova mrežna arhitektura omogućuje prijenos različitih sadržaja (npr. govor, podaci, multimedij) na zajedničkom paketskom prijenosu. Važno je istaknuti i motivaciju da usluge u mrežama sljedeće generacije trebaju biti dostupne u svakom trenutku, na svakom mjestu i na bilo kojem uređaju. Stoga je prilagodba usluga korisniku, terminalu i kontekstu od iznimne važnosti za usluge u mrežama nove generacije.

Etablirani mrežni operatori ponukani su na migraciju postojećih mreža prema mrežama nove generacije zbog zastarjele opreme bez mogućnosti kvalitetnog održavanja, ali i zbog pojave

novih konkurentnih davatelja usluga i poslovnih modela. Potencijalne prednosti koje konvergencija donosi mrežnom operatoru su sljedeće:

- pojednostavljena mrežna arhitektura,
- pojednostavljeno upravljanje i održavanje mreže uz smanjenje troškova,
- pojednostavljeno uvođenje novih usluga prilagođenih potrebama korisnika i
- interakcija s vanjskim davateljima usluga bez gubitka kontrole nad vlastitom mrežom uz podršku novih poslovnih modela.

Iz svega gore navedenog razvidno je da će telekomunikacije budućnosti biti u potpunosti IP komunikacije pa ćemo stoga u ovom predmetu isključivo obrađivati problematiku „kvalitete usluga u IP mrežama“.

Tradicijski, Internet Protokol ili IP mreže samo su nudili uslugu *najbolje moguće* („*best effort"*) dostave za IP promet. U takvim mrežama sav promet tretira se jednako. Takav nači rada bio je dovoljno dobar samo na početku razvoja računalnih mreža (Interneta), međutim pojavom prvih aplikacija koje su za svoj rad tražile nekakve uvjete mrežnog transporta podataka, javile su se i potrebe za osiguranjem kvalitete isporuke podatkovnih paketa.

Promatramo li paket koji je Internetom poslan od pošiljatelja do primatelja, mreža nam ne garantira nikavo specificirano vrijeme do kada će taj paket biti isporučen, niti čak da li će biti uopće isporučen ukoliko negdje na putu naiđe na zagušenje.

Brzina isporuke (odnosno kašnjenje paketa) nije veliki problem ukoliko promatramo isporuku npr. E-mail poruke, gdje nam sekunde nisu toliko bitne, međutim ako kod *voice-over-IP* (VoIP) usluge imamo veliko kašnjenje, varijacije kašnjenja ili ako imamo veliki broj izgubljenih paketa, usluga će postati neprihvatljiva.

Stara klasična telefonska mreža sa komutacijom kanala -*Public Switched Telephone Network* (PSTN) ispunjavala je sve zahtjeve za govornom komunikacijom između korisnika i postavila je referencu za razinu govorne usluge. Međutim, kao što joj i samo ime govori, ona je bazirana na komutaciji kanala (*Circuit Switched*- CS) i za svaku pojedinu vezu ima rezerviran zaseban kanal. S jedne strane ovo osigurava vrlo visoku kvalitetu, ali s druge strane pruža i znatno nižu efikasnost iskorištenja kapaciteta u odnosu na IP mreže koje koriste postojeće kapacitete znatno učinkovitije. Za vrijeme prijenosa govora kod komutacije kanala zauzima se jedan cijeli kanal, odnosno čitav kapacitet tog kanala. Za vrijeme tišine (trenutne stanke u razgovoru), kada se ne prenose informacije kapacitet kanala je neiskorišten jer se njime ne mogu prenositi druge informacije osim razgovora između dva korisnika, na taj način dodatno se smanjuje iskorištenost kapaciteta. U IP telefoniji, trenutci tišine odnosno slušanja ili stanki između riječi se ne prenose te se zbog toga značajno dobiva na kapacitetu kanala po kojemu putuju i druge informacije osim između dva sugovornika koji pričaju.

Postoji još jedna velika razlika između PSTN-a mreža i IP mreža. PSTN mreže osmišljene su i izgrađene samo za jednu vrstu usluge, a to je govorna komunikacija. Sa druge strane, **IP mreže su višeuslužne mreže (MSN-*Multi Service Networks*).**To su telekomunikacijske mreže koje pružaju više od jedne vrste usluga putem iste prijenosne infrastrukture, neovisno o prijenosnom mediju.Osim toga, u sebi sadrže ugrađene mehanizme koji osiguravaju zahtijevanu kvalitetu usluge.

To je u suprotnosti s klasičnim mrežama ili mrežama predviđenim samo za jednu vrstu usluge.Iako internetski promet možebiti prenošen telefonskim sustavima, ti sustavi se ne smatraju više uslužnom mrežom, jer nisu dizajnirani s tim ciljem. Glavni cilj višeuslužnih mreža je prijenos informacija na daljinu, bilo da se radilo o govoru,podatku ili videu.

IP QoS parametri

Kvaliteta usluga (QoS) u području telekomunikacija može se definirati kao skup specifičnih zahtjeva koje telekomunikacijska IP mreža (mrežni operater) osigurava korisniku, a koji su neophodni za normalan rad korisnikovih aplikacija.

Korisnici specificiraju zahtjeve u formi liste QoS parametara koje transportna IP mreža mora zadovoljiti kako bi njihove aplikacije mogle normalno raditi.

Najvažnije metrike za definiranje IP razine usluge su:

- kašnjenje
- varijacija kašnjenja
- gubitak paketa
- propusnost
- dostupnost usluge

Budući da različite usluge zahtijevaju različite mrežne kapacitete i različitu kvalitetu, svaka usluga ima različite iznose izgubljenih paketa, širinu prijenosnog pojasa, kašnjenje i varijacije kašnjenja. Navedeni parametri se mogu nazivati mrežnim QoS parametrima ili uslužno specifičnim QoS parametrima jer su vezani za specifičnu uslugu. Također, s obzirom da se radi o parametrima koji direktno utječu na zadovoljstvo korisnika i koji predstavljaju tehničku interpretaciju njegovih zahtjeva za kvalitetom, mogu se svrstati i u ključne QoE (*Quality of Experience*) pokazatelje pri čemu seuzimaju njihove prosječne vrijednosti.

Obzirom da su različite aplikacije imaju različite zahtjeve za kvalitetom usluge (npr. zahtjevi za glasovne, video i aplikacije s kritičnim podacima nisu isti), javila se i potreba za definicijom tzv. **ugovor o razini usluge** - SLA (*service level agreement*).

Ugovor o razini usluge - SLA (*Service Level Agreement*)

Ugovor o razini usluge je alat kojim se stvara međusobno razumijevanje o uslugama i isporuci usluga između davatelja usluga i njihovih korisnika. Njime se određuju očekivanja, razjašnjavaju odgovornosti i stvara objektivna osnova za procjenu učinka usluge.

SLA je proces i proizvod.

U smislu procesa, on je formalno dogovoreno sredstvo pomoću kojega dvije ili više strana unapređuju komunikaciju, grade dugoročne odnose iodređuju očekivanja uslugama, razinama usluge i kvaliteti usluge, odgovornostima svake strane te koracima koje poduzimaju sve strane kako bi osigurale uspješne odnose.

U smislu proizvoda,on je dokument između davatelja usluga i njegovih unutarnjih ili vanjskih korisnika ili između bilo koje dvije ili više strana koje moraju međusobno djelovati kako bi izvršile zadatak i postigle zajednički cilj.

Uvođenjem SLA standardizira se razina usluga, evidentira se i dokumentira razina usluga, uspostavljaju se mehanizmi mjerenja razine usluga na obje strane, stvaraju se temelji za unapređenje razine usluga, uspostavlja se odgovornost u poslovnom procesu, omogućava se lakše planiranje i osiguranje sredstava za resurse, omogućava se veća mobilnost svih sudionika poslovnog procesa, optimizira se funkcioniranje poslovnog procesa, postiže se bolje upravljanje i korištenje kapitalnih resursa, poboljšava se razumijevanje davatelja za korisnikove potrebe I prioritete, postiže se veća konkurencijska prednost pred onim davateljima koji ne koriste ugovore.

Općeniti i eksplicitni SLA ugovori

Vrlo često davatelji usluge (*Internet Service Providers* – ISP) definiraju SLA ugovor vrlo općenito, ukoliko se radi o ponudama za široku populaciju, u kojima pružaju vrlo male ili pak nikakve garancije kvalitete.

Na primjer:„*ako DSL internet vezu nadogradite sa 2 Mbps na 8 Mbps tada možete očekivati da će se usluga koju dobivate poboljšati*.“

Međutim, to ne mora biti slučaj. U ovom primjeru 2 Mbps i 8 Mbps definiraju maksimalnu brzinu usluge koju podržava oprema ISP-a ali DSL usluga se isporučuje preko pristupne mreže koja je za svakog korisnika drugačija i limitira propusnost koju korisnici mogu osijetiti. Vrlo slična priča je i kod mobilnih operatera koji reklamiraju samo maksimalne brzine prijenosa podataka koje su moguće samo ukoliko je na baznu stanicu spojen samo jedan korisnik, koji uz to ima mobilni uređaj koji podržava sve najnovije funkcije.

Kada se rade SLA ugovori za korporacije, oni se **definiraju eksplicitno**!

Definira se minimalna razina usluge, a ona se izvodi iz aplikacijskih zahtjeva.

Npr. mreža koja osigurava jednosmjerno kašnjenje od 500 ms neće moći podržavati govor preko IP-a (VoIP) uslugu koja u najgorem slučaju zahtijeva jednosmjerno kašnjenje manje od 200 ms.

Ukoliko pak za mrežu koja treba prenositi VoIP tražimo da maksimalno jednosmjerno kašnjenje bude manje od 50 ms, što je pak znatno manje od dozvoljenog, mreža će morati biti tako i projektirana pa će se morati koristiti znatno skuplja oprema ili pak nove prijenosne trase, što može za posljedicu dovesti do nepotrebnih troškova.

Iako je uobičajeno da davatelji javnih usluga VPN-a za poslovne organizacije, svoje ponude specificiraju eksplicitno u SLA ugovoru, vrlo rijetko se događa da se u tom ugovoru specificira i oprema samog korisnika, tj. njegova oprema koja podržava rad aplikacija i spoj na mrežu javnog davatelja usluga. Nedovoljno dobre performanse korisničke opreme koja ne može pratiti rad profesionalne opreme davatelja usluga vrlo često uzrokuju razliku između ugvovorenih (i od operatera ponuđenim performansama) i stvarno ostvarenim performansama mreže.

Pored toga, korisnikov tim za mrežnu podršku poslovno-kritičnih aplikacija koji određuje zahtjeve za SLA ugovor vrlo često nije u stanju u potpunosti razumjeti rad samih aplikacija i njihovih limita, što pak onemogućava mrežnim inženjerima osiguranje adekvatne podrške usluge. Razumjevanjem primjena SLA zahtjeva jednako je važno u mreži u poduzeću kao i u mrežnom okruženju davatelja usluga. Važno je razumjeti značenje brojčanih jedinica SLA ugovora.

SLA može biti definiran apsolutnim (eksplicitnim) uvjetima, npr.„u najgorem slučaju jednosmjerno kašnjenje iznosi 100 ms“ ili se pak može definirati statistički sa maksimalnim postotkom gubitka paketa od 0.01%.

U slučaju statističke definicije, definiranje postotka gubitka paketa od 0.01% nije dovoljna informacija da bi se utvrdilo da li usluga može biti podržana na toj mreži.

Trebamo definirati kako se taj gubitak mjeri, te kakav će utjecaj na aplikaciju imati gubitak paketa od 0.01%.

Jedan izgubljeni paket na svakih sto paketa ne može imati značajan utjecaj na VoIP poziv, ali gubitak od 10 uzastopnih paketa od 1000 će uzrokovati grešku u pozivu koja je čujna za krajnjeg korisnika.

Kako bi se uklonile neke od potencijalnih nejasnoća oko SLA definicije, formirana je radna grupa IPPM WG unutar *Internet Engineerins Task Force (IETF)* koja je imala zadaću definirati skup standardnih mjerila i postupaka za precizno mjerenje i dokumentiranje koje se može primjeniti na kvalitetu, svojstva i pouzdanost IP usluga. Uloga IPPM WG bila je dizajn metrike koja se koristi za mjerenja od strane mrežnih operatora te krajnjih korsnika. Njihov cilj bio je definirati mjere koje ne predstavaljaju subjektivnu vrijednosnu procijenu (ne definiraju ″dobar″ ili ″loš″), nego pružaju nepristranu kvantitativnu mjeru učinka. [RFC2330] definira ″okvir za IP svojstva metrike″ unutar IETF pod pretpostavkom da je SLA osiguran od strane mrežnog davatelja usluga za korisnike koji općenito ne koriste IPPM definicije.

Općenito govoreći "kvaliteta usluga" ili „*Quality of Service“* (QoS) izraz je koji se koristi za opisivanje znanosti o inženjerskogom pristupu IP mrežama kako bi ih projektirali za uspješan rad svih aplikacija tretirajući promet različito za svaku aplikaciju, ovisno o njihovim potrebama iz samoga SLA ugovora.

Kvaliteta usluge može biti vrlo značajan faktor na tržištu. Definicija parametara za određivanje kvalitete neke pojedine usluge i njihovo mjerenje u stvarnome radu mreže, neophodni su za pružanje stvarne slike o kvaliteti mreže nekog operatera. Ukoliko su nuđene usluge i cijene između različitih operatera slične, tada će izmjerena kvaliteta usluge imati veliki tržišni utjecaj na odabir pružatelja usluga (operatera) od strane korisnika.

Do prije 15 - 20 godina, došlo je do značajnoga razvoja kvalitete usluge za IP promet, do točke u kojoj su mehanizmi, arhitekture i iskustvo implementacije u potpunosti razvijeniza podršku aplikacijama različitih usluga integrirane IP mreže.

IP je postao tehnologija konvergencije za multimedijske usluge, a time je i QoS jedna od vrućih tema u IP umrežavanjima. Ipak trenutno je to još uvijek jedan od najmanje shvaćenih pojmova s praktične točke gledišta.

Do prije dvadesetak godina, dizajn i implementaciju velikih IP mreža korištenjem protokola usmjeravanja kao što su: OSPF (*Open Shortest Path First*) i BGP (*Border Gateway Protocol*), smatrali su se veoma specijalističkim zadacima, koji su ograničeni samo na mrežne „gurue“. Danas međutim, sa širenjem Interneta i velikih IP mreža, nestalo je mistike povezane s tim tehnologijama, a njihovo razumijevanje se preselio na čitavu Internet zajednicu. Sa druge strane, kakvoća usluge IP prometa se danas tretira kao ekspertna tema, isto kao OSPF i BGP prije dvadeset godina.

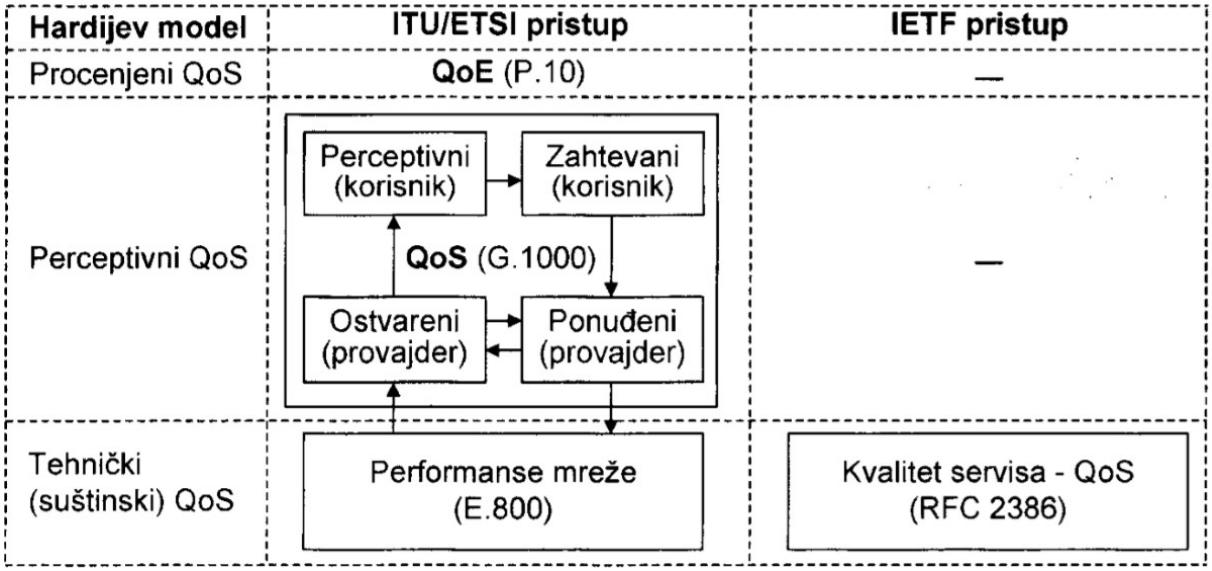
U ovoj skripti istaknuti ćemo značaj IP QoS-a, povezivanjem teorije QoS s primjenom u praksi, od definicije SLA do izvedbenoga detalja projekta i konfiguracije. Opisat će se ključni zahtjevi za primjenu SLA, QoS funkcija i arhitekture kako bi studenti razumjeli pojmove IP QoS, studije slučajeva i primjere korištenja tih koncepata u praksi.

Definicije kvalitete usluge u IP mrežama

Hardijev model kvalitete usluge

William Hardy je 2001. godine definirao opći model kvalitete telekomunikacijske usluge. Taj model objašnjava relevantne aspekte QoS za korisnika i pružatelja usluge, a može poslužiti kao referentni model za objašnjenje terminologije i pristupa koje koriste međunarodne organizacije za standardizaciju: ITU-T, ETSI i IETF. Veza između Hardijevog modela, ITUT/ETSI pristupa i IETF pristupa je prikazana na slici 1-Opći model kvalitete usluge sačinjavaju tri komponente:

- tehnička kvaliteta usluge,
- perceptivna (doživljena) kvaliteta usluge i
- procijenjena kvaliteta usluge.



Slika 1 - Hardijev model QoS, ITU-T/ETSI i IETF pristupi

Tehnički ili **stvarni QoS** se odnosi na karakteristike usluge koje proizlazeiz tehničkih aspekata. Drugim riječima, tehnički QoS je određen projektom telekomunikacijske mreže i načinom realizacije veza, te pristupa mreži. Zahtijevana kvaliteta usluge ostvaruje se pravilnim izborom telekomunikacijskih protokola, mehanizama za garanciju QoS i pridruženih vrijednosti parametara. Ocjena tehničkog QoS se donosi na osnovu usporedbe izmjerenih i očekivanih performansi mreže. Korisnikova percepcija kvaliteta nema utjecaja na ocjenjivanje tehničkog QoS-a.

Perceptivni ili doživljeni QoS odražava iskustvo korisnika u korištenju određeneusluge. Očekivanja korisnika, na koja utječe cijena, iskustvo sa sličnim telekomunikacijskim uslugama i mišljenja drugih korisnika, predstavljaju značajan faktor u ocjeni perceptivnog QoS-a. To znači da različiti korisnici različito opažaju i ocjenjuju uslugu koja ima ista tehnička svojstva.

Procjenjeni QoS dolazi do izražaja kada korisnik odlučuje da li će nastaviti koristiti određenu uslugu. Pored percepcije kvalitete i cijene usluge, značajan faktor procijenjenog QoS-a je i

razina odziva pružatelja usluge na korisničke primjedbe, kao i u smislu obogaćivanja postojećih usluga novom ponudom.

ITU-T/ETSI pristup

ITU-T i ETSI pristupi definiciji kvalitete usluga i QoS terminologiji su u osnovi isti (ITU-T preporuke E.800 [3.4] i G.1000 [3.5], ETSI dokument ETR 003 [3.6]). Obje organizacije usvojile su definiciju prema kojoj se QoS odnosi na "zajednički skup performansi usluga koji određuje nivo zadovoljstva korisnika uslugom“. Iz toga proizlazi da ITU-T/ETSI pristup odgovara perceptivnom QoS iz Hardijevog modela, kao što je prikazano na slici 1-1. Tehnički aspekti QoS-a, odnosno pojam tehničkog QoS-a iz općeg modela odgovara ITU-T definiciji "performanse mreže", koja obuhvaća sve funkcije mreže koje su bitne za realizaciju određene usluge. Performanse mreže se definiraju i mjere pomoću parametara pojedinih komponenata mreže koje učestvuju u procesu realizacije usluge.

ITU-T i ETSI razlikuju četiri komponente koje zajednički sačinjavaju QoS:

1. QoS koji zahtijeva korisnik,
2. QoS koji nudi davatelj usluga (ISP),
3. QoS koji pruža davatelj usluga i
4. QoS koji percipira korisnik (slika 1-1).

Zahtijevi korisnika odražavaju preferencije korisnika za kvalitetom određenih usluga, a mogu biti izraženi formalnim (tehničkim) ili neformalnim opisom. Na kvalitetu usluga koje nudi davatelj utječu strategija davatelja usluga, postojeće tehnologije i standardi, cijena razvoja i implementacije usluga i drugi faktori. QoS koji nudi davatelj usluga je izražen skupom parametara i pridruženih vrijednosti koje su razumljive širokom krugu različitih korisnika (na primjer, "godišnja raspoloživost usluge je 99,95%"). Skup parametara QoS-a je definiran ITU-T preporukom E.800. Nivo kvalitete usluge koji realno ostvaruje davatelj usluga izražava se pomoću istog skupa parametara. Usporedba vrijednosti parametara ponuđenog i ostvarenog QoS je jedna od komponenata za ocjenjivanje doživljenog QoS-a. Doživljeni QoS predstavlja konačnu ocijenu korisnika o kvaliteti dobivene usluge, izvedenu na osnovu usporedbe sa zahtijevanim nivoom QoS-a.

Iskustvena kvaliteta usluge–QoE

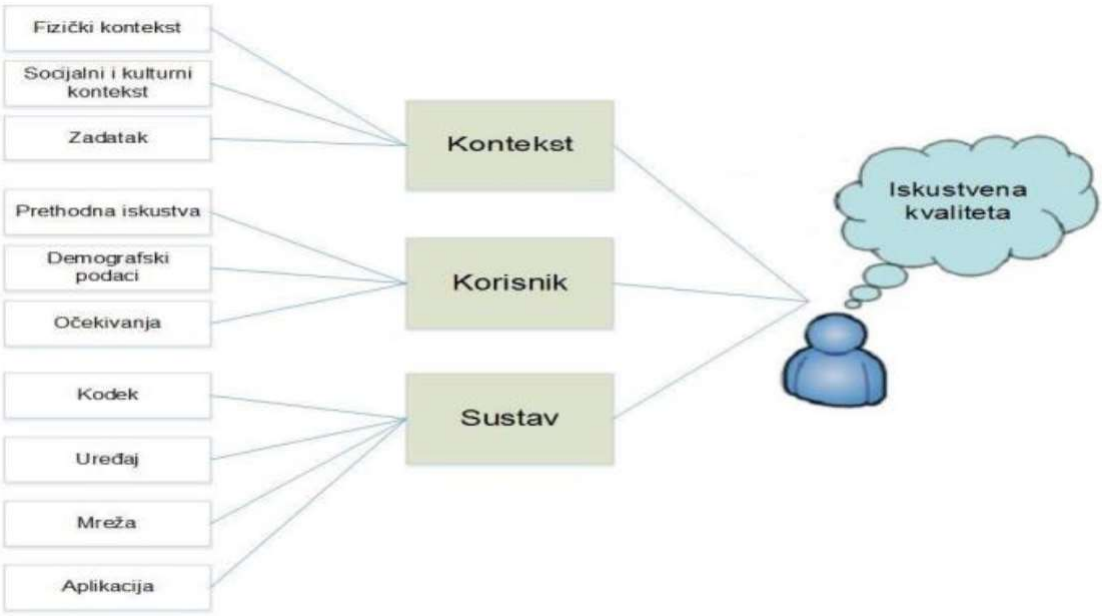
Iskustvena kvaliteta usluge relativno je novi koncept koji se bavi mjerenjem korisničkog zadovoljstva korištenjem određene usluge ili proizvoda. Javlja se u području telekomunikacija. To je korisnički usmjeren koncept u multidisciplinarnom području koji pokušava shvatiti korisničku percepciju kvalitete usluge kako bi se povećalo zadovoljstvo korisnika uslugom.Većina predloženih modela iskustvene kvalitete temelje se na određenom broju faktora koji utječu na percipiranu kvalitetu usluge od strane korisnika, a koji proizlaze iz sustava, konteksta korištenja usluge ili korisnika. Nemoguće je definirati model za mjerenje iskustvene kvalitete kojibi vrijedio za sve telekomunikacijske usluge, ali moguće je definirati pojedine modele za evaluaciju iskustvene kvalitete za različite tipove usluga. Iskustvena kvaliteta je subjektivna mjera zadovoljstva krajnjeg korisnika korištenjem određenog proizvoda ili usluge. Koncept iskustvene kvalitete razvijen je kao nadopuna kvalitete usluge QoS. Standardizacijsko tijelo ITU-T (*International Telecommunication Union – Telecommunication Standardization Sector*) u preporuci E.800, [19]definira kvalitetu usluge

kao "kolektivni utjecaj performansi usluge koji određuju stupanj zadovoljstva krajnjeg korisnika uslugom". Istraživanja kvalitete usluge na području telekomunikacija bila su usmjerena na ispitivanja o utjecajima objektivnih, mjerljivih mrežnih parametara i karakteristike pružane usluge kao što su način kodiranja podataka, kašnjenje, gubitak paketa. Moorsel je uveo pojam iskustvene kvalitete kao nove metrike povezane s korisničkim iskustvom i doživljajem prilikom korištenja telekomunikacijske usluge. Iskustvena kvaliteta i kvaliteta usluge razliku se po subjektivnim utjecajima na korisnika. Standardizacijsko tijelo ITU-T proširilo je preporuku E.800 definirajući kvalitetu usluge kao "sveukupnost karakteristika telekomunikacijske usluge koje zadovoljavaju potrebe krajnjeg korisnika te usluge" te se obraća posebna pozornost na kvalitetu usluge percipiranu odstrane korisnika (QoSP–*QoS Perceived*). Standardizacijsko tijelo ITU-T u proširenju P.10 preporuke G.100 definira iskustvenu kvalitetu kao "sveukupnu prihvatljivost aplikacije ili usluge, subjektivno percipiranu od strane krajnjeg korisnika", a standardizacijsko tijelo ETSI definira ju kao "mjerilo uspješnosti korištenja telekomunikacijske usluge ili proizvoda temeljeno na objektivnim i subjektivnim psihološkim mjerama".
Iskustvena kvaliteta u jednoj je od zadnjih predloženih definicija istraživačke zajednice opisana kao "stupanj zadovoljstva ili iritiranosti (*annoyance*) korisnika aplikacije ili usluge; ona proizlazi iz njegovih očekivanja obzirom na korist i/ili uživanje u aplikaciji ili usluzi kao rezultat osobnosti korisnika i trenutnog stanja". Prema navedenim definicijama može se zaključiti da je došlo do pomaka u perspektivi kvalitete usluge kao tehnički orijentiranog koncepta usmjerenog prema korisniku, koji osim dijela tehničkih performansi u obzir uzima i kontekst korištenja usluge, ali i samog korisnika,pri čemu nastaju složeni parametri iskustvene kvalitete.

Vrednovanje iskustvene kvalitete

Vrednovanje iskustvene kvalitete treba se temeljiti na utjecajnim faktorima koji se mogu kontrolirati i mjeriti. Za vrednovanje iskustvene kvalitete koriste se dvije metode; subjektivno i objektivno vrednovanje. Najčešći načini provođenja subjektivnog vrednovanja su anketiranje korisnika i subjektivna ispitivanja u testnim okruženjima. Detaljnim pregledom utjecaja parametara na iskustvenu kvalitetu korisnika omogućena je manipulacija i kontrola nad parametrima. Ukoliko se ispitivanje ponavlja, stupanj pouzdanosti dobivenih rezultata može se povećati jer provođenjem eksperimenata više puta dolazi do potvrde zaključaka ispitivanja. Ovakav način vrednovanja iskustvene kvalitete ima određene nedostatke pa su rezultati istraživanja uglavnom nepouzdani jer uvjeti stvarnog okruženja većinom ne odgovaraju uvjetima testne okoline. Ispitivanja u kontroliranim uvjetima uglavnom su dugotrajna i skupa. Vrijeme i troškovi istraživanja, te pouzdanost podataka dobiveni su na način vrednovanja iskustvene kvalitete putem *crowdsourcinga* kod kojega se podrazumijeva evaluaciju usluge sa strane povećeg broja Internet korisnika. Kod subjektivnih ispitivanja najčešće se koristi **MOS (*Mean Opinion Score*)**, ljestvica kvantificiranja korisničkog iskustva. MOS nije najbolje rješenje za vrednovanje iskustvene kvalitete budući da korisnici u većini slučajeva imaju različite interpretacije ocjena, a ponekad se dogodi da više korisnika isto ocjeni različita iskustva.S aspekta subjektivne iskustvene kvalitete nemoguća je kvantifikacija ocjene kvalitete usluge jer korisnici u većini slučajeva svoje (ne)zadovoljstvo uslugom izražavaju opisima kao što su dobro, loše, odlično, itd. Ponekad ni aspekt korisnika nije u stanju kvalitativno opisati zadovoljstvo korištenom uslugom. Iz tog razloga iskustvena kvaliteta se često nastoji vrednovati pomoću modela i objektivnih mjerenja. Ocjena iskustvene kvalitete koja je dobivena objektivnim mjerenjem ima pouzdanost koja ovisi o definiciji pravilnog modela za određenu uslugu. Kako bi se definirao pouzdani model vrednovanja iskustvene kvalitete

potrebni su mjerljivi parametri koji utječu na iskustvenu kvalitetu korisnika i koji su vezani uz različite dijelove usluge i koji su različiti za svaku uslugu. ITU predlaže podjelu utjecajnih faktora na objektivne faktore koji se odnose na kvalitetu usluge (npr. parametri usluge i mreže) i subjektivne, tj. ljudske faktore (npr. korisnička očekivanja, emocije). Na slici 2. definirani su utjecajni faktori koji su podijeljeni u tri skupine: faktori sustava (sve karakteristike sustava koje utječu na iskustvenu kvalitetu korisnika), korisnički faktori (sve karakteristike korisnika koje utječu na njegovu subjektivnu ocjenu kvalitete usluge) i kontekstni faktori (trenutni faktori iz okolinei sustava prisutni za vrijeme korištenja usluge)



Slika 2: Utjecajni faktori na iskustvenu kvalitetu korisnika

PREDAVANJE 2 - Mjerenja i značaj IP QoS parametara

Mrežno kašnjenje

Kod ugovora na razini usluge (SLA) mrežno kašnjenje općenito je definirano u smislu:

jednosmjernog kašnjenja za ne-prilagodljive i vremensko-kritične aplikacije kao što su VoIP i video, te u smislu

povratnog kašnjenja ili povratnog vremena (RTT) za prilagodljive aplikacije kao što su one koje koriste TCP protokol (Transmission Control Protocol) [RFC739].

Jednosmjerno kašnjenje karakterizira vremenska razlika između slanja i primanja IP paketa po definiranoj putanji mreže. Mjerilo za mjerenje jednosmjernog kašnjenja definirano je [RFC2679] od strane IETF.

RTT karakterizira vrijeme između prijenosa IP paketa od točke do točke prema odredištu te potvrde o primitku paketa od odredišta. Mjerilo za mjerenje RTT definirano je [RFC2681] od strane IETF.

Jednosmjerno kašnjenje se mjeri rijeđe od povratnog kašnjenja jer staze između izvora i odredišta mogu biti asimetrične. Put usmjeravanja ili obilježja staze od izvorišta do odredišta mogu biti različiti od puta usmjeravanja ili obilježja iz odredišta natrag prema izvoru.

Podjela kašnjenja po uzroku nastajanja:

Propagacijsko kašnjenje

Propagacijsko kašnjenje je vrijeme potrebno za pojedinačno putovanje paketa od izlaznog sučelja usmjernika vezom preko prijenosnog medija do ulaznog sučelja odredišnog usmjernika. Brzina širenja signala, tj. brzina putovanja paketa prijenosnim medije određena je brzinom svijetlosti, pa samo propagacijsko kašnjenje ovisi o udaljenosti između uređaja i o iskoristivosti prijenosnog medija. Ukupno propagacijsko kašnjenje na putu čine zbroj propagacijskih kašnjenja na svim sastavnim dijelovima prijenosne trase. Propagacijsko kašnjenje je oko 4 ms na 1000 km kroz koaksijalne kabele i oko 5 ms na 1000 km za optička vlakna.

U praksi, mrežne veze nikada ne slijede zemljopisno najkraći put između točaka koje povezuju. Međuovisnost duljine trase i zračne udaljenosti točaka možemo procijeniti slijedećim aproksimacijama:

- Zemljopisna udaljenost D (zračna linija) između dvije krajnje točke prijenosne trase.
- Duljina samih prijenosnih trasa (R) mora biti veća od udaljenosti zračne linije.

Staza duljine R može se procijeniti iz zemljopisne udaljenosti D pomoću izračuna od (*International Telecommunication Union* – ITU) preporuka [G.826], koja je sažeta u ovoj tablici.

D	R
D < 1000 km	R = 1.5 * D
1000 km s=d=s 1200 km	R = 1500 km
D > 1200 km	R = 1.25 * D

Tablica 1: *Procjena duljine trase u odnosu na zemljopisnu udaljenost točaka*

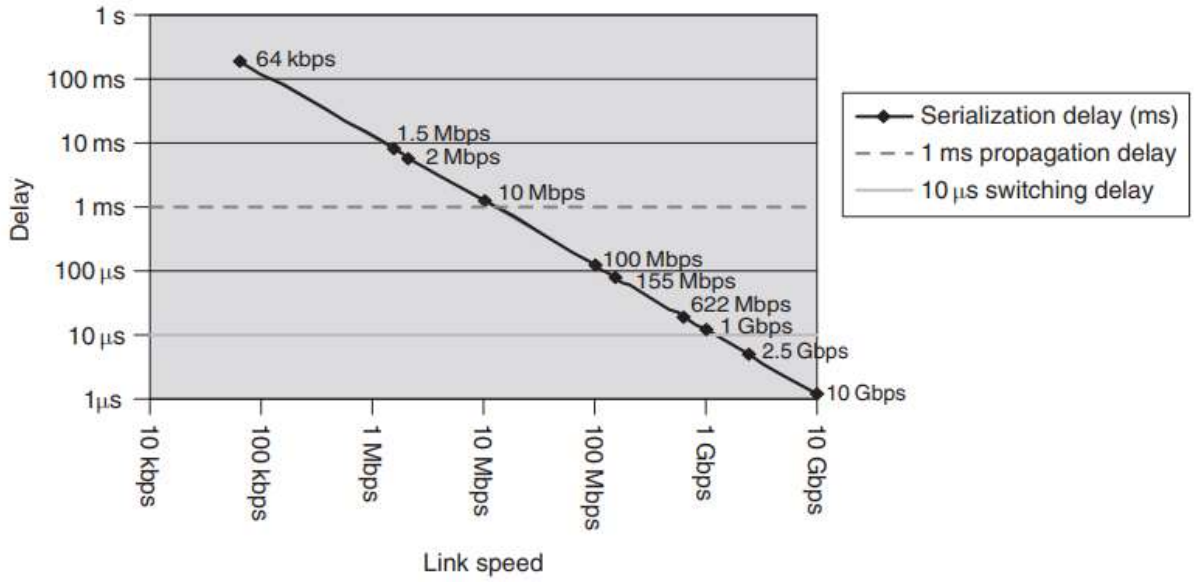
Jedini način kontrole propagacijskog kašnjenja veze je kontrola usmjeravanja na fizičkom linku, koja se može kontrolirati na 2 ili 3 sloju ISO-OSI modela. Ako je propagacijsko kašnjenje na linku vrlo veliko, moguće je da je usmjeravanje veze na 2 sloju mreže duže nego što bi trebalo biti, a moguće ga je smanjiti preusmjerenjem veze. Alternativno, promjenom topologije mreže i dodavanjem više direktnih veza možemo smanjiti propagacijsko kašnjenje na putu.

Kašnjenje prospajanja (*Processing delay*)
Kašnjenje kod prospajanja (obrade zaglavlja paketa) nastaje u usmjerniku kao vremenska razlika između primanja paketa na dolaznom sučelju usmjernika i čekanja paketa u upravljačkom programu prema izlaznim sučeljima. Kašnjenje prospajanja na usmjernicima visokih performansi može se generalno smatrati zanemarivim za vanjske usmjernike gdje se prospajanje provodi u hardveru, kašnjenje prospajanja tipično je reda od 10^{-20} po paketu. Čak i za implementaciju softverski baziranog usmjernika, tipično kašnjenje prospajanja bi trebalo biti samo 2-3 ms. Malo se može učiniti za kontrolu kašnjenja prospajanja bez promjene softvera ili hardvera usmjernika. Kašnjenja prospajanja uobičajeno su znatno manje veličine od ukupnog kašnjenja s kraja na kraj mreže pa nisu toliko kritična.

Kašnjenje raspoređivača (*Queing delay*)
Kašnjenje raspoređivača je definirano kao razlika vremena između čekanja paketa na izlaznim sučeljima raspoređivača i generiranja paketa na izlaznom sučelju. Ovo kašnjenje nastaje korištenjem algoritama za raspoređivanja kod reda čekanja paketa u upravljačkom programu (queing), a koji je pak funkcija kapaciteta čekanja i ponuđenog prometnog opterećenja i profila.

Kašnjenje raspoređivača kontrolira upravljanje prometnim opterećenjem primjenomodgovarajućeg mehanizma čekanja i raspoređivanja.

Kašnjenja serijalizacije (*Transmission delay*)
Kašnjenje serijalizacije je vrijeme potrebno za generiranje paketa na izlaznom sučelju (jedan po jedan bit paketa), a ovisi o brzini veze i veličini paketa.



Slika 1: Kašnjenje serijalizacije za paket od 1500 bajta

Kašnjenje serijalizacije je proporcionalno veličini paketa a obrnuto proporcionalno brzini veze:

$$\textit{Kašnjenje serijalizacije} = \frac{\textit{veličina paketa}}{\textit{brzina veze}}$$

Serijalizacijsko kašnjenje općenito se može smatrati zanemarivim za brzinu veze iznad 155 Mbps (STM-1/OC3) poput veza jezgrene mreže, ali može biti značajno za veze manje brzine. Serijalizacijsko kašnjenje za paket veličine 1500 bajta na vezama od 64 kbps do 10 Gbps prikazano je na slici iznad. Serijalizacijsko kašnjenje može biti značajano za veze niže brzine. Serijalizacijsko kašnjenje je fizičko ograničenje i stoga ne postoji način kontroliranja serijalizacijskog kašnjenja, osim promjenom brzine veze.

Varijacije kašnjenja paketa (*Jitter*)

Varijacijom kašnjenja paketa se općenito opisuje razlika jednosmjernog kašnjenja za dva uzastopna paketa, kao što je definirano [RFC3393] u IETR u praksi, međutim varijacija kašnjenja paketa se također može mjeriti kao varijacija kašnjenja sa poštivanjem nekih referentnih mjerila kao što su prosječna ili minimalna kašnjenja. Varijacija kašnjenja paketa odnosi na jednosmjerno kašnjenje pa pojam povratnog vremena varijacije kašnjenja paketa nema smisla. Može biti uzrokovana raznim razlozima poput nesavršenosti izvora referentnog takta, vanjskih elektromagnetskih smetnji, itd. Ova veličina standardno se definira pri sklapanju SLA ugovora jer neke aplikacije mogu biti osjetljive na nju.

Neke aplikacije kao one što koriste TCP uglavnom nisu osjetljive na smetnje. Aplikacije koje su osjetljive na varijacije kašnjenja koriste *spremnike za uklanjanje varijacija kašnjenja* kako bi trasformirali promjenjivo mrežno kašnjenje u stalno kašnjenje na odredištu.

Gubitak paketa

Gubitak paketa karakterizira ispuštanje paketa koje se javlja između definirane mrežne ulazne točke i definirane mrežne izlazne točke. Paket poslan od mrežneulazne točke smatra se izgubljenim ako ne stigne na mrežnu izlaznu točku unutarodređenog vremenskog razdoblja.

Metrika za mjerenje stope jednosmjernog gubitka paketa (PLR) je definirana [RFC2680] od strane IETF.

Osim izmjerenih stopa gubitka, u nekim aplikacijama ključni parametar koji može utjecati na promatranu izvedbu od strane krajnjeg korisnika je gubitak uzorka ili gubitak distribucije. Isti postotak gubitka može rezultirati značajno različitompercepcijom izvedbe dajući dva različita gubitka distribucije. Stoga [RFC3357] uvodi neke dodatne metrike koje opisuju gubitke obrazaca:

- ″period gubitka″ definira učestalost i trajanje gubitka (*gubitak praska*) nakon što počne.
- ″udaljenost gubitka″ definira razmak između razdoblja gubitka

Gubitak paketa može biti uzrokovan brojnim čimbenicima:

- ***Zagušenost.*** Kad se javlja zagušenost čekanje u redu se povećava i paketi se odbacuju. Gubitak uslijed zagušenja kontrolira upravljanje prometnim zagušenjem i primjena odgovarajućeg mehanizma raspoređivanja.
- ***Pogreške na nižim slojevima***. Pogreške bita na fizičkom sloju mogu se javiti zbog buke ili gušenja u prijenosnom kanalu što može uzrokovati odbacivanje paketa. Većina IP transportnih protokola kao što su UDP (*User Datagram Protocol*) [RFC768], imaju cikličku zaštitu (CRC) ili paritetni zbroj za otkrivanje pogreški. Kad se pogreške događaju a zbroj je ispravan okviri će biti odbačeni. Stoga, za pakete koji putuju preko mreža sa takvim mogućnostima greške će rezultirati gubitkom paketa. Svaki paket će stići ispravan ili uopće neće stići, iako postoji nekoliko iznimaka u ovom slučaju. U praksi, stvarna stopa pogrešaka (BER koja se također naziva *bit error ratio*) variraju ovisno o osnovi koriste li tehnologije 1 ili 2 sloj koji su različiti za različite dijelove mreže :
  - ✓ Na vlaknu baziran optički link može podržati BER od $1*10^{-13}$
  - ✓ Sinkrona Digitalna Hijerarhija (SDH) ili Sinkrona Optička Mreža (SONET) usluge obično nude BER od $1*10^{-12}$
  - ✓ Tipična E1/T1 zakupljena linija podržava BER od $1*10^{-9}$
  - ✓ Institut inženjera elektrotehnike i elektronike (IEEE) donose standarde za lokalne i gradske mreže [802-2001] precizira maksimalni BER od $1*10^{-8}$
  - ✓ Tipična asinkrona digitalna pretplatnička linija (ADSL) usluga podržava BER od $1*10^{-7}$
  - ✓ Satelitske usluge podržavaju BER od približno $1*10^{-6}$

Za tehnologije na slojevima veza koje su općenito sklone visokim stopama greški uobičajena je podrška nekih mehzanizama pouzdanosti slojeva veze kao što su FEC (*Forward Error Correction*) kako bi se u nekim slučajevima oporavile od grešaka. Međutim ako tehnologije prvog ili drugog sloja ne mogu pružiti potrebnu podršku BER za stopu gubitka paketa (PLR) koje zahtijevaju IP aplikacije onda se za ispravljanje pogrešaka moraju koristiti protokoli viših slojeva ili aplikacija.

- ***Kvarovi mrežnih elemenata***. Kvarovi na mrežnim elementima mogu prouzročiti gubitke paketa dok se ne obnovi veza od pogreške na mrežnom elementu. To je rezultiralo periodima gubitka koje ovise o temeljnim mrežnim tehnologijama koje se koriste. Sa razvojem ″običnog″ IP (ne MPLS) nakon pogreške na mrežnom elementu,čak iako postoji alternativni staza doći će do gubitaka povezanosti koja uzrokuje gubitak paketa dok unutarnji usmjerivački protokol poveznika (IGP) ne konvergira. U dobro dizajniranim mrežama vrijeme IGP konvergencije završava u nekoliko stotina milisekunda. Ako ne postoji alternativna staza onda će se gubitak povezanosti ponavljati sve dok staza ne bude popravljena. Takvi ispadi mogli bi nam koristiti za definiciju postotaka gubitaka za uslugu, a ona najćešće iznosi definiranu raspoloživost za uslugu . Kada alternativna staza postoji gubitak povezanosti na sljedećem elementu mreže može biti znatno smanjen kroz korištenje tehnologija kao što su MPLS prometno inženjerstvo (TE), brzo preusmjeravanje (FRR) [RFC4090] ili IP brzo preusmjeravanje (IPFRR), koja je tehnologija lokalne zaštite koja omogućava povezivanje i brzo obnavljaljanje veze i kvarova na čvorištima obično unutar 50 ms. Istovjetne tehnike mogu se koristiti na drugom sloju kao što je automatska zaštita prospajanja (APS) za SONET i zaštitu multipleks dijela za SDH.
- ***Gubitak u aplikacijama krajnjih sustava***. Gubitak u aplikacijama krajnjih sustava se može dogoditi zbog poplava u prijamnom spremniku. Poplave se događaju kada se spremnik prepuni, a paketi i dalje dolaze koji stoga ne mogu čekati u spremniku. Poplave mogu utjecati na sve vrste programa. Ispod granice obično utječu na aplikacije u realnom vremenu kao što je VoIP i video te kada je spremnik prazan kada kodek mora uzeti uzorak i to se efektivno realizira kao izgubljeni paket. Gubitak zbog poplava u spremnicima može se spriječiti pravilnim dizajnom mreže i primjenom krajnjih sustava.

Ovisno o primjeni prijenosnog protokola ili aplikacije, postoji potencijalno veliki broj tehnologija koje se mogu upotrijebiti za zaštitu paketa uključujući ispravljanje pogrešaka te retransmisiju.

Širina pojasa i propusnost

IP usluge obično se prodaju sa definiranom širinom pojasa gdje „širina pojasa“ često odražava kapacitet pristupne veze na drugom sloju. Propusnost (*troughput)* je stvarno ostvarena širina pojasa tj brzina protoka bita (b/s).

"Propusnost" *(troughput) je maksimalna količina podataka u jedinici vremena koju neka veza ili cijela staza može pružiti nekoj aplikaciji ovisno o trenutnoj iskoristivosti staze, korištenim protokolima i operativnim sustavima, te mogućnostima i opterećenju koje ima krajnji korisnički uređaj.*

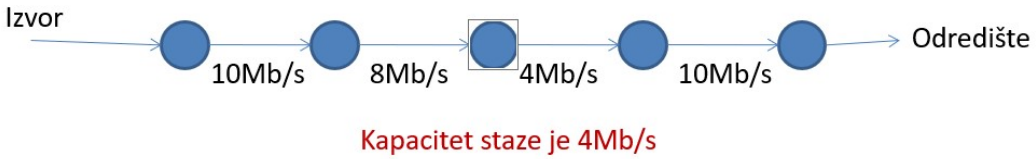
Kada se koristi u kontestu umrežavanja ″širina″ koja se izvorno koristi za opisivanje elektromagnetskih frekvencija, potencijalno može imati niz različitih značenja s obzirom na kapacitet veze, mreža ili usluga za prijenos prometa ili podataka.

Dakle kako bi se izbjegla konfuzija definirali smo neke više specifične pojmove :

- ***Kapacitet veze***. Kapacitet veze je mjera koliko se bita po sekundi može prenijeti vezom s tim da kapacitet veze treba uzeti u obzir na 2 i 3 sloju.
  - ✓ Kapacitet vezena 2. sloju je obično konstantan te je funkcija kapaciteta fizičkog medija (kapacitet 1.sloja) uz posebno kodiranje korišteno na 2.sloju. Međutim, neke tehnologije kao što su ADSL 2/2+ su prilagodljive po brzini pa stoga kapcitet 1.sloja može varirati ovisno o razini šuma i interferencije.
  - ✓ Kapacitet veze na 3 sloju (IP kapacitet veze) je funkcija kapaciteta veze na 2 .sloju. Drugi sloj koristi enkapsulaciju, a 3. sloj veličinu paketa. Kapacitet IP veze može biti izveden za specifičnu veličinu IP paketa od dostupnog kapaciteta veze na 2. sloju u bitima po sekundi.

  Kapacitet veze se također naziva još i *širina pojasa veze* ili *brzina veze*

- ***Klasifikacija kapaciteta***. U sustavima koji koriste QOS mehanizme, promet se može svrstati u nekoliko konstitutivnih klasa i različiti QOS zahtjevi mogu biti osigurani za različitu klasifikaciju prometa. Gdje klasa ima definiranu minimalnu propusnost, to se zove *klasa kapaciteta* i može biti također poznata kao *klasa propusnosti*.
- ***Kapacitet staze ili puta***. Kapacitet staze određuje minimalni kapacitetpojedinačne veze na stazi između definirane mrežne ulazne točke i definirane mrežne izlazne točke koja se sastoji od niza usmjernika i čvorova međusobno povezanih linkovima. Kapacitet staze također može biti zvan kao *propusnost staze*



- ***Obujam prijenosnog kapaciteta(Bulk Transfer Capacity - BTC)*** . Obujam prijenosnog kapaciteta (BTC) je mjerenje dostižnog protoka podataka korisnika između izvora i odredišta. [RFC3148] određuje okvir za definiranje empirijske metrike kapaciteta obujma.

BTC = preneseni podaci / proteklo vrijeme.

BTC je učinkovita mjerilo za tokove podataka koji previše ne variraju u sveme volumenu pri određenoj stopi propusnosti (u bitima po sekundi) kako bi zagušenja svijestan transportni sloj veze mogao prijeći preko staze od izvorišta do odredišta. ″Zagušenja svijestan″ u ovom kontestu odnosi se na prijenosni sloj tehnologije koja prilagođava svoju brzinu slanja, ovisno o tome što je trenutno primljeno kako bi se pokušala povećati maksimalna propusnost. TCP veza je primjer takve zagušenja svijesne veze na transportnom sloju.

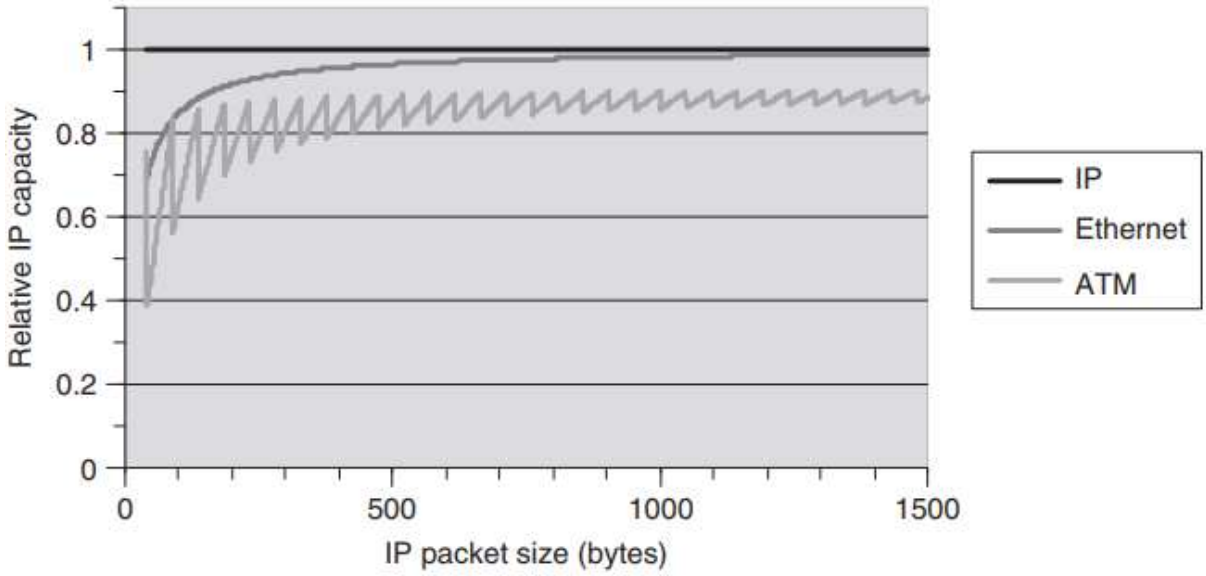
BTC je jasno ograničen kapacitetom veze, ali na njegatakođer utječe niz drugih faktora kao što je gubitak paketa i RTT, stoga jevažno imati na umu da BTC može biti znatno niži nego kapacitet veze koji jenaveden u SLA.

BTC se ne odnosi na neprilagodljive usluge (nema prilagođenja brzine slanja). Za takve usluge njihova dostižna propusnost ne može biti metrički značajna ali ipak može biti izvedena od kapaciteta staze i dozvoljene stope gubitka za usluge.

Dakle, jasno je da dosegnuta propusnostza usluge možda neće biti ista kao definirana propusnost staze. Sljedeći odijeljci uzimaju u obzir dodatne čimbenike koji dodatno otežavaju odnos između ″propusnosti″ i „postignute propusnosti“.

Umetanje na drugom sloju

Kapacitet usluge ovisi o dostupnome IP kapacitetu, a ovaj pak ovisi o 2. sloju veze.
2. sloj korisiti enkapsulaciju, a 3. sloj veličinu paketa.



Slika 2: Relativni IP kapacitet za različite medije drugog sloja

Enkapsulacija na 2 sloju dodaje različite veličine zaglavlja za svaki paket, zaglavlja se umeću sa perspektive IP usluga koje koriste kapacitet 2. Sloja, a koji nije dostupan na 3 sloju. Na trećem sloju (kao i na 2. Sloju) zaglavlja se dodavaju za svaki IP paket, a dostupnost IP kapaciteta ovisi o veličini IP paketa. Slika 2 pokazuje relativni IP kapacitet za Ethernet i ATM

veze i kako kapacitet relativno varira ovisno o veličini IP paketa. Kao što vidimo sa slike 2, raspoloživi IP kapacitet može značajno varirati ovisno o umetanju na 2 sloju.

Za Ethernet, umetanje broja bajta po IP paketu na 2. sloju je konstantna bez obzira na veličinu paketa. Umetanje 2 sloja relativno se smanjuje u odnosu na raspoloživi IP kapacitet kako se veličina IP paketa povećava. Tj. sve je manji udio sistemskih bita u odnosu na informacijske bite koje želimo prenijeti. To nije slučaj za ATM, gdje se IP paket segmentira u ćelije, a ćelijsko opterećenje ovisi o broju ćelija koje pak ovise o veličini paketa. Stoga, iako se trend umetanja na 2 sloju smanjuje u odnosu na dostupni IP kapacitet kako se veličina IP paketa povećava, povećanje od jednog bajta u veličini paketa može rezultirati dodatnim ATM ćelijama, što rezultira u povećanju relativnog umetanja.

Neke usluge koriste prometni oblikovatelj koji se primjenjuje na pristupnim linkovima kako bi smanjili dostupan kapacitet linka, međutim, oblikovatelji i raspoređivači mogu se ponašati različito, ovisno o tome da li oni prikazuju propusnost u smislu veličine paketa 3 sloja ili oni također uključuju sva umetanja sa 2 sloja.

Uzeti ćemo u obzir za primjer, jednostavna dva reda čekanja (gdje red označava klasu prometa), gdje raspoređivač za red čekanja minimalne propusnosti definira na3 sloju X=Y=50%. Raspoređivač za red X čeka da primi 100 bajta informacije i onda doda bite okvira. S veličinom IP paketa od 100 bajta za čekanje X i 1000 bajta za čekanje Y uz predpostavku da 2 sloj umeće 26 bajta po paketu (kao što je slučaj sa ethernet v2) , izmjereni omjer propusnosti X:Y na 3 sloju je (10*100) : (1*1000) = 50:50, dok je omjer mjerenja na 2 sloju (10*126) : (1*1026) = -55:45.

Obrnuto, uz pretpostavku iste veličine paketa i umetanja ali sa redom čekanja minimalne propusnosti X=Y=50% definiranom na 2 sloju, rezultiralo omjeru propusnosti na 3 sloju = (100*1026):(1000*126) =~ 45:55.

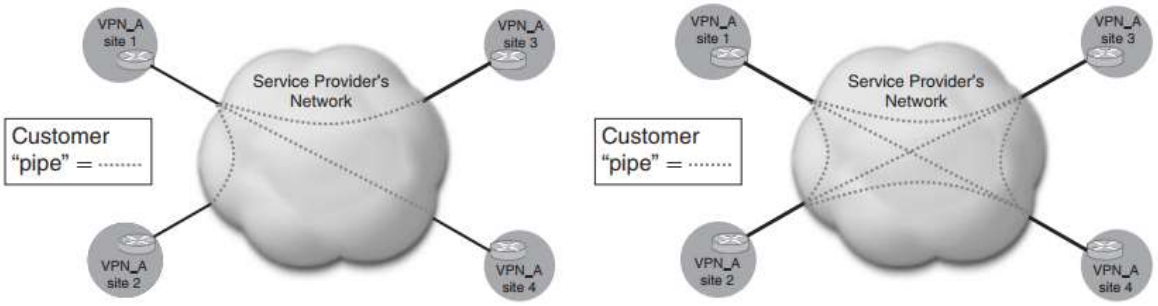
U nekim slučajevima, postoje ograničenja nametnuta od 1 sloja i tehnologija 2 sloja, što naravno definira umetanje koje je uzeto u obzir u određenoj SLA definiciji. U drugim slučajevima možda ne postoji definitivan odgovor da li umetanje na 2 sloju treba uzeti u obzir:

- Proračun za umetanje na 2 sloju u implementacijama stvarnih usmjernika može biti različit kada npr. mehanizmi fragmentacije na 2 sloju umeću dodatne bajtove paketu koji je u redu čekanja
- Neke SLA usluge su definirane bez umetanja na 2 sloju dok druge uzimaju u obzir proračun umetanja
- Arhitekture IETF integriranih usluga (Intserv) i diferenciranih usluge (Diffserv) ne definiraju proračun umetanja na 2 sloju.

Bez obzira na usvojeni pristup SLA specifikacije moraju jasno definirati koji troškovi se uzimaju u obzir i na koji sloj primjenjuju jamstvo propusnosti. To posljedično utječe na troškove pa QOS funkcije kao što su raspoređivanje, oblikovanje ili utvrđivanje kriterija kvalitete treba uzeti u obzir.

VPN tehnologija tuneliranja

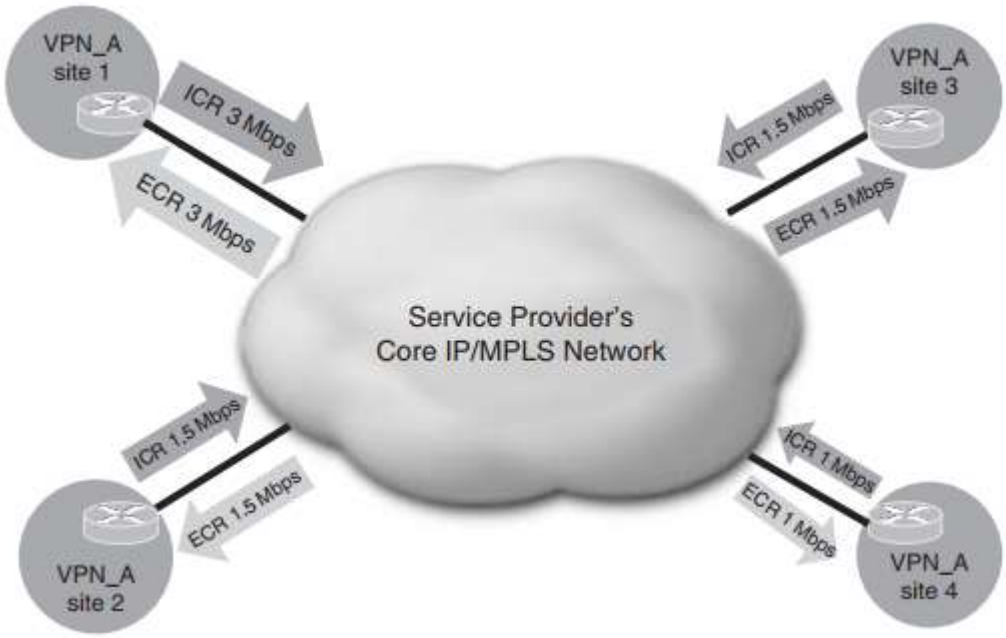
Razmatramo mrežu koja je spojena na četri mjesta (#1, #2, #3, #4), ovo bi mogao biti 2. sloj virtualne privatne mreže (VPN) ostvaren tehnologijama kao što su ATM, Frame-relay ili iznajmljenim vodovima. Bez obzira koja se tehnologija koristi, lokacije mogu biti međusobno razmještene i povezane preko središnje (*hub)* lokacije ili bi mogle biti povezane međusobno svatko sa svakim.



Slika 3: VPN mreža povezna u *hub* (lijevo) i svatko sa svakim (desno) koristeći ″pipe model″.

U oba slučaja prikazana na slici 3, svaki zakupljeni vod ili virtualni krug (VC) može imati definiranu SLA obvezu. Ova vrsta propusnosti točka-točka naziva se tuneliranje, a povezivanje točka-točka pruža izolaciju između svojstava svakog ″tunela″. Kako se broj lokacija unutar VPN mreže u svaki-sa-svakim konfiguraciji povećava tako osiguranje takve veze može postati glomazno. Na primjer, međusobna povezanost između n lokacija zahtijeva n(n-1)/2 priključaka. 100 lokacija će zahtijevati 100*99/2 = 4950 takvih tunela. Veze točka-točka mogu biti neučinkovite s obzirom na korištenje utemeljenog kapaciteta. Na primjer, lokacija #1 možda će imati 1 Mbps virtualni kanal (VC) pripremljen za svaku lokaciju #2, #3 i #4 (ukupno 3Mbps). Ako VC na lokaciji #2 nije zauzet, ovaj neiskorišteni kapacitet sa lokacije #2 ne može se ponovno koristiti za promet između lokacije #1 i lokacije #3 te lokacije #3 ili #4. Kapacitet do 1Mbps od/do lokacije #1 će biti neiskorišten.

Korištenjem MPLS tehnologije možemo kreirati VPN koji implicitno pruža povezivost svatko sa svakim između lokacija unutar VPN, međutim, ovo dovodi do pitanja kako definirati SLA između mjesta unutar VPN koje pružaju višespojnu povezivost, kada nemate odgovarajući tunel između tih lokacija? Sa modelom tuneliranja, SLA možemo definirati na osnovi veza točka-točka između lokacija, SLA se definira u smislu tuneliranja sa svake lokacije do VPN mreže davatelja usluga. Iz perspektive kapaciteta, tuneliranje za svaku lokaciju je definirano u smislu ulazne izvršne brzine (ICR) prema davatelju usluge i izlazne izvršne točke (ECR) od davatelja usluga, kako je prikazano na slici 4. Promet između dvije lokacije koje imaju ICR ugovor na lokaciji izvora te ECR ugovor na lokaciji odredišta osigurana je povezanost sa kraja na kraj. ICR/ECR može biti definirana sa jednom klasom na svakom lokaciji ili u kontekstu Diffserv usluge može biti ponuđena po klasi i po osnovnoj lokaciji.



Slika 4: Povezivanje svatko sa svakim u VPN mreži koristeći ″hose model″

Hose model SLA može pružiti prednosti statističkog multipleksiranja dok *pipe* model SLA ne može. Na primjer, ako lokacija #1 ima ICR i ECR od 3 Mbps taj kapcitet bi se mogao koristiti za komunikaciju sa bilo kojom od lokacija #2, #3 i #4, ako nije bilo prometa na lokaciji #2 neiskorišteni kapacitet bi se potencijalno ponovno mogao koristiti za promet između lokacije lokacije #1 i lokacije #3 ili #4. Posljedica toga je da *hose model* SLA također potreban da bi se napravila odredba za posredovanje između ICR i ECR između različitih lokacija. Na primjer, ICR za lokaciju #1 može biti 3Mbps, međutim, dostupan kapacitet za lokaciju #4 će biti ograničen ECR od lokacije #4, što je 1Mbps. Stoga, hose model SLA treba uzeti u obzir u slučajevima gdje se mogući gubitak propusnosti događa zbog nagomilavanja korisničkog prometa. Ako lokacije #2, #3 i #4 pokušaju generirati promet sa svih ICR-ova (koji iznose 4 Mbps) na lokaciju #1, njihov ukupno dostupan kapacitet će biti ograničen ECR-om na lokaciji #1 koji je brzine samo 3 Mbps.

Očuvanje slijeda protoka

IP tehnologija nam ne garantira da se paketi dostavljaju u redoslijedu po kojem su poslani. Kao što je definirano u IETF od [RFC4737], ako su paketi u protoku numerirani sekvencijalno u redoslijedu u kojem su bili poslani paket koji je stigao sa rednim brojem manjim od svog prethodnika bio bi definiran kao pogrešan te bi bio ponovno poslan. Na primjer, ako su paketi u sekvencijalnom broju slijedova poprimili poredak 1, 2, 3, 4, 7, 5, 6, 8, 9, 10 tada će paketi sa brojem 5 i 6 biti ponovno poslani.
Najjednostavnija veličina po kojoj se mjeri važnost ponovnog slanja ili retransmisije je omjer ponovnog slanja, što je omjer ponovno poslanih paketa koji su pristigli u odnosu na ukupan broj primljenih paketa. Brojne druge metrike za kvaniticiranje važnosti retransmisije definirane su u [RFC4737].

Zbog štetnog utjecaja koje retransmisije mogu imati kod nekih aplikacija, obično se prihvaćaju dva ključna dizajna koji predstavljaju „najbolje prakse“ za spriječavanje ponovne retransmisije unutar toka:

- Važno je da se bilo koje IP balansiranje opterećenja preko više putova unutar mreže izvode po razini protoka paketa tako da **svi paketi unutar toka slijede isti put**. Ovo balansiranje opterećenja obavlja se preko algoritma ECMP (*Equel Cost Multipath*). ECMP algoritmi obično obavljaju *hash* funkcije kako bi se utvrdilo koji od putova će paket prijeći, gdje *hash* funkcija koristi 5-torku IP protokola, izvornu IP adresu, odredišnu IP adresu, izvorišni UDP/TCP port, odredeišni UDP/TCP port
- QOS dizajn i algoritmi moraju osigurati da se paketi istog protoka uvijek primaju po istom redoslijedu. Ovo je temeljni princip integrirane usluge i diferencirane usluge QOS arhitekture.

Raspoloživost

Raspoloživost za IP usluge je obično definirano na jedan od ova dva načina, bilo kao raspoloživost mreže ili raspoloživost usluga

Raspoloživost (dostupnost) mreže

Raspoloživost mreže je definirana kao dijelić vremena u kojem je mrežna povezivost dostupna između određene mrežne uzlazne točke i određene mrežne izlazne točke. Raspoloživost može biti jednosmjerna i dvosmjerna. Dvosmjerna povezivost je ono što je bitno za većinu IP aplikacija tako da izvor može poslati paket na odredište te potom čekati odgovor. Metrika za mjerenje povezivanja definirana je od [RFC2678] u
IETF. Kod mrežne raspoloživosti treba uzeti u obzir i nedostupnost zbog planiranih zastoja koja je uzrokovana rasporedom održavanja mreže kao i ispadi zbog mrežnih kvarova. Nedostupnost koja proizlazi iz mrežnih kvarova ovisi o mrežnim tehnologijama koje se koriste. Raspoloživost mreže može se procijeniti izračunavanjem raspoloživosti svakog pojedinog elementa mreže, a zatim kombiniranjem raspoloživosti u seriji ili paralelno prema potrebi pomoću slijedeće formule :

Raspoloživost komponenti

Raspoloživost (A) pojedine komponente je udio vremena za koje će uređaj raditi :

$$A = \frac{\text{vrijeme rada}}{\text{ukupno vrijeme}} = \frac{MTBF}{MTBF+MTTR}$$

Gdje je:

MTBF = prosječno vrijeme između kvarova

MTTR = prosječno vrijeme potrebno za otklanjanje kvara

Neraspoloživost komponenti

Neraspoloživost (U) pojedine komponente je udio vremena za koje uređaj neće raditi:

$$UA = \frac{\text{vrijeme bez rada}}{\text{ukupno vrijeme}} = \frac{MTTR}{MTBF + MTTR} = 1 - A$$

Raspoloživost komponenti u seriji

Raspoloživost kompnenti { a, b, c, ...} u seriji (A) je dana :

$$A_s = [\, A(a) \times A(b) \times A(c) \times \ldots]$$

Raspoloživost komponenti u paraleli

Raspoloživost komponenti { a, b, c, ...} u paraleli je dana :

$$A_p = [\, 1 - (\, U(a) \times U(b) \times U(c) \times \ldots)]$$

Za većinu aplikacija sama mjera raspoloživosti mreže nije dovoljna, tj. ne govori nam mnogo. Npr. za VoIP, raspoloživost mreže može biti vrlo velika, ali ukoliko postoji veliko kašnjenje paketa između dva VoIP krajnja uređaja sama aplikacija postaje neupotrebljiva jer kada VoIP paketi kasne u razgovoru između dviju stranaka govor postaje nerazumljiv.

Raspoloživost usluge

Raspoloživost usluge definira se kao dio vremena kada je usluga dostupna između određene ulazne točke i određene izlazne točke i to unutar SLA definiranih granica parametara za uslugu.

Raspoloživost usluge može se definirati neovisno o mrežnoj raspoloživosti u kojem slučaju raspoloživost usluga ne može prelaziti mrežnu raspoloživost ili se može definirati kao odnos samo kada se mreža smatra dostupnom.

Raspoloživost mreže može obuhvatiti performanse aplikacija kao i performanse mreže. Na primjer, raspoloživost mreže može obuhvaćati dodijelivanje imena hostova (DNS server) i vremena transakcije ovisno o kašnjenju mreže i performansama web servera. Tu može biti preklapanja između definicija rasploloživosti mreže ili usluge i definicija drugih SLA parametara.

Na primjer, razmotrit ćemo dvije klase prometa, A i B.

Klasa A podržava kašnjenje SLA koje je navedeno sa 90 percentila (P90) te kašnjenja paketa do 10 ms što znači da 90 od 100 paketa mora biti isporučeno unutar tog vremena te P99 kašnjenje od 15 ms.

Klasa B ima P75 kašnjenje od 10 ms s P99 zaostatkom od 30 ms.

Ovaj SLA mogao bi biti izražen manjim kašnjenjem vezano sa klasama A i B ali sa istom raspoloživosti. Klasa A ima kašnjenje od 15 ms sa 9.9 % raspoloživosti usluge, dok klasa B ima kašnjenje od 30 ms s 9.9% raspoloživosti usluge.

Alternativno, ovaj SLA bi mogao biti izražen sa istom granicom kašnjenja ali sa većom raspoloživosti za klasu A nego za B. Klasa A ima kašnjenje od 10 ms s 90% raspoloživosti usluge dok klasa B ima kašnjenje od 10 ms s 75% raspoloživosti usluge.

Kvaliteta doživljaja (*Quality of Experience* – QoE)

Osim metrike već opisane u ovom poglavlju koja definira karakteristike mreže postoje dodatne metrike čiji je cilj kvantificirati doživljaje aplikacija koristeći mrežu. Ove metrike definiraju percepciju primjenih performansi doživljene iz perspektive krajnjeg korisnika koja je također poznata kao korisnička ″ kvaliteta doživljaja ″ (QOE – Quality of Experience).

Za IP bazirane glasovne i video aplikacije QOE je spoj metrika koje ovise o kvaliteti kodera koji se koristite te isporučenoj kvaliteti usluge od IP mreže i kvaliteti dekodera koji se koristi. QoE ciljevi ne definiraju izravno kašnjenje, smetnje i gubitke te karakteristike koje mreža treba osigurati nego određene aplikacije koristeći definirani koder/dekoder.

QoE metrikom može se mjeriti subjektivno ili objektivno.

Subjektivno mjerenje oslanja se na krajnjeg korisnika po procijeni njihove percepcije kvalitete usluge.

Objektivno mjerenje koristi mjerenja karakteristika primljenog toka a moguće i prijenosnog toka kako bi se zaključila subjektivna kvaliteta koju doživljava krajnji korisnik.

Postoje QoE metrike definirane za on-line igre, glasovne i video aplikacije:

Glasovne

- *Subjektivna mjerenja*. **MOS (*Mean opinion score*)** su dobro ustrojen nacrt koji nam pruža numeričku mjeru kvalitete glasovnog poziva na odredištu. MOS je službeno testiran za subjektivna mjerenja koja su definirana od ITU [P.800] i određuju se koristeći veliki broj ljudskih slušatelja koji sudjeluju u skupu standardnih testova. Kod subjektivnog ocjenivanja kvalitete, definirani tekst čita se preko komunikacijskih medija te se prijemna kvaliteta ocjenjuje od strane slušatelja pomoću ljestvice : izvrstan (5), dobar (4), prosječan (3), prolazan (2) i loš (1). Srednja vrijednost MOS-a izračunava se aritmetičkom srednjom vrijednost svih pojedninačnih rezultata. Tipična javna telefonska mreža (PSTN) za govorne usluge ima MOS od 4.3, dok mobilne telefonske usluge obično imaju MOS između 2.9 i 4.1.
- *Objektivna mjerenja*. Postoji nekoliko preporuka koje je dao ITU koje pružaju metode za objektivno praćenje kvalitete glasa i koje se također mogu koristiti za procijenu MOS-a.
  - ✓ ITU P.862 [P.862] definiraju perceptivnu promjenu kvalitete govora (PESQ), te je puna referenca (gdje su potpuni podatci o oba prenesena i primljena audio signala dostupni kada se određuje kvaliteta zvuka) za objektivne metode za predviđanje subjektivne MOS kvalitete kod usluga telefonije.
  - ✓ ITU G.107 [G.107] definira tzv. ″E model″ koji koristi brojne razine prijenosnih parametara za procijenu kvalitete prijenosnog sustava kako bi se procijenili učinci na uslugu telefonije. Primarni izlaz iz E modela je ″faktor procijene″ R pomoću kojeg dolazimo do procjene MOS-a za pozive koje koriste taj prijenos usluga.

Video

- *Subjektivna mjerenja.* Glavni pojmovi subjektivnog mjerenja video kvalitete su isti kao i za MOS za glasovne komunikacije. Većina utemeljenih shema testiranja subjektivnog videa u svjetskim programima DCSQS (*Double Stimulus Quality scale)* postupak definiran u ITU specifikacijama [BT.500]. Alternativna tehnologija koju Europska radiodifuzijska unija (EBU) definirala zove se SAMVIQ (Subjektivna procijena metodologije za video kvalitetu).
- *Objektivna mjerenja*. Većina postavljenih ciljeva za video kvalitetu definirana je u ITU-T standardom J.144 i Q.144. Ovo pruža smjernice o perceptivnom

  mjerenju kvalitete videa za uporabu aplikacija digitalne kabelske televizije kada je dostupna puna referenca signala videozapisa.

On-line igranje

[DICK] definira MOS metriku za klasificiranje kvalitete percepcije igračevog igranja

PREDAVANJE 3 - SLA zahtjevi aplikacija

Različite aplikacije imaju različite SLA zahtijeve:

- Pretjerani gubitak paketa ili kašnjenje može otežati podržavanje aplikacija u realnom vremenu, iako precizan prag ″prekomjerno″ ovisi o pojedinim aplikacijama.
- Vrijednost gubitka paketa ili mrežnog kašnjenja raste različito pri uporabi različitih protokola prijenosnog sloja za održavanje visoke propusnosti.

Kako bi razlikovali ove utjecaje trebali bi imati potrebnu minimalnu razinu razumjevanja kako se aplikacije i protokoli ponašaju kada se mrežne karakteristike mijenjaju. Samo uz pomoć takvog razumjevanja mrežni inženjer može, koristeći QoS mogućnosti mreže, osigurati podržavanje SLA zahtjeve aplikacija.

Dakle, ovo predavanje ima cilj osigurati minimalnu razinu razumjevanja zajedno sa pružanjem reference za daljne detalje o aplikacijama i pojašnjenjima protokola. Osim toga, razumijevanjem kako se aplikacije i protokoli ponašaju kada se SLA karakteristike mijenjaju moguće je razumjeti gdje implementacija QOS mehanizma ne može biti dovoljna da bi mogli zadovoljiti SLA zahtijeve. Isto tako, da bi razumjeti utjecaj koji aplikacija ima na mrežu ili na druge aplikacije važno je razumjeti kakav je profil aplikacijskog prometa. Za određivanje prometnog profila aplikacije treba definirati barem prosječnu stopu aplikacijskih zahtjeva ili karakteristiku „praska zahtijeva“ u određenom vremenskom intervalu.

Neke aplikacije imaju konstantnu brzinu prijenosa (CBR – *Constant Bit Rate*) što znači da će karakteristika prometa biti relativno ista tijekom bilo kojeg vremenskog intervala.

Ostale aplikacije mogu se opisati kao promjenjive brzine prijenosa (VBR – *Variable Bit Rate*), gdje je karakteristika praska prometa relativno veća preko manjeg vremenskog intervala.

Iako postoji previše aplikacija da bi ih sve opisali, razmotrit ćemo najčešće aplikacije ili vrste aplikacija koje nameću najoštrije zahtijeve SLA na mreži. U praksi, većina aplikacija koje imaju eksplicitne SLA zahtijeve pasti će u jednu od sljedećih kategorija koji su slični jednoj od ovih opisanih kategorija :

- govor preko IP (VoIP)
- video stream
- video konferencije
- TCP aplikacije usredotočene na propusnost
- interaktivne podatkovne aplikacije
- on-line ili mrežno igranje

Govor preko IP (VoIP)

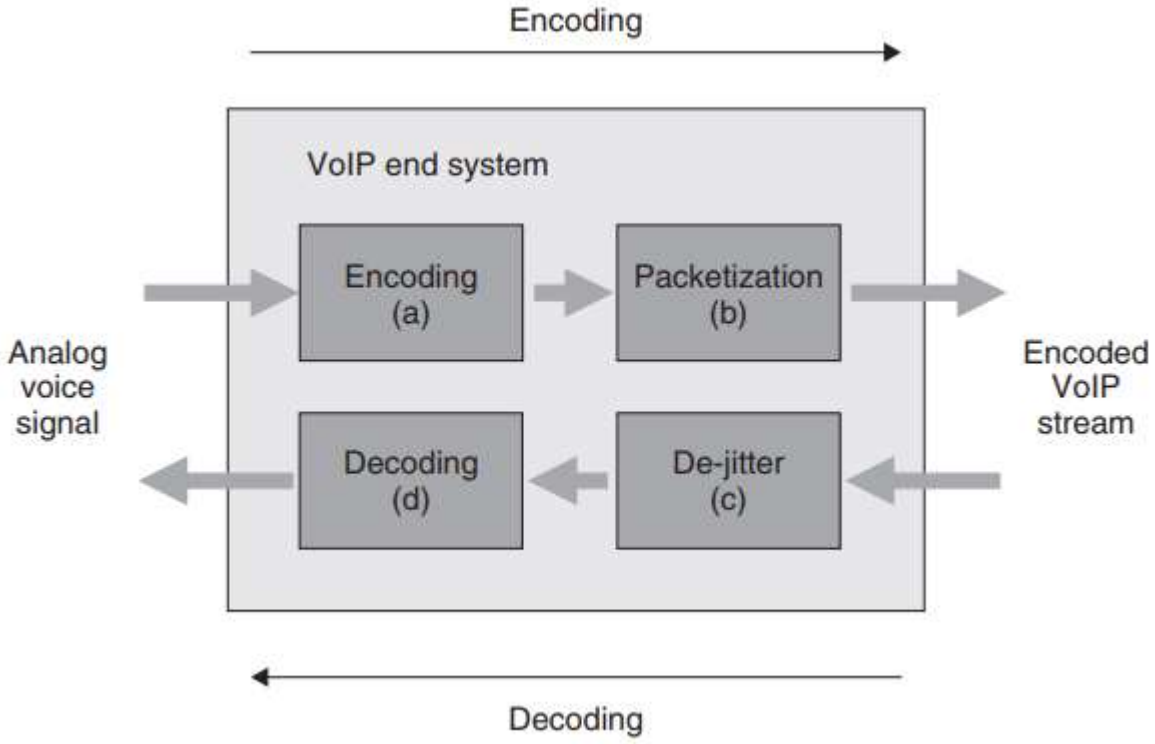
Govor preko IP (VoIP) najčešće se prenosi kao digitalno kodirani *stream* koristeći protokol za usluge u realnom vremenu (RTP – *Real-Time Protocol*) [RFC3550] preko UDP protokola.

RTP je protokol na transportnom sloju koji nam omogućava dostavu VoIP streamova od pošiljatelja do primatelja. Signalizacijski protokol kao što je protokol za uspostavu sjednice (SIP) [RFC3261] može se koristiti za postavljanje RTP nositelja *stream*-a i odrediti medijske formate koji će se koristiti.

Ključni čimbenici (prema kojima se postavljaju SLA ograničenja kao što je kašnjenje i gubitak) su VoIP koderi koji se koristi za kodiranje signala i određuju specifične detalje na implementaciji krajnjih sustava.

Na primjer, neki kodeci mogu biti manje tolernatni na gubitke od drugih dok loša implementacija krajnjih sustava može biti manje tolerantna na smetnje. VoIP kodeci pretvaraju analogni glasovni signal u digitalni *bit stream* do pošiljatelja i pretvaraju ga natrag u analogni audio signal u prijamniku. Najviše korišteni kodeci su definirani od strane ITU-T a to su G.71x i G.72x standardi. Najjednostavniji valno-bazirani kodeci kao što je to definirao ITU standardom G.711 koriste pulsno kodnu modulaciju (PCM) gdje se analogni signal uzorkuje u redovitim razmacima a uzorci se kvantiziraju u niz diskretnih vrijednosti za proizvodnju kodiranog digitalnog signala. Napredniji kodeci, koji su definirani od ITU standardom G.726 koriste **adaptivno diferencijalni PCM (ADPCM).** ADPCM pretviđa sljedeći uzorak iz prethodnih uzoraka a zatim kvantizira samo razliku između stvarne vrijednosti uzorka i predviđanja, dakle, ADPCM proizvodi manju brzinu bita od PCM-a, a pruža nam jednaku (ili bolju) kvalitetu zvuka. Kodeci kao što su ITU G.729 i ITU G.723 koriste kompliciranije tehnike kao što su Algebarsko Kodno Pobuđeno Linearno Predviđanje (ACELP). ACELP siječe uzorkovani ulazni signal u blokove uzoraka, ti blokovi ili okviri koji su obično 20 ms obrađuju se kao cijelovite jedinice. U obradi okvira, koder koristi tehniku koja se naziva analiza-pa-sinteza kako bi se utvrdilo koji ulazni parametar kada prođe kroz sintezirani filtar bi rekonstruirao govor najbliži izvornom govoru signala. Koder zatim koristi kodne riječi s referentnih ulaza na filter a referenca je poslana na dekoder koji dijeli iste kodne riječi i koji primjenjuje odgovarajuće ulaze na istu sintezu filtera za rekonstrukciju govora.
Kodeci raspoloživi za VoIP razlikuju se u složenosti i u propusnosti što im je potrebna i u percepciji dostavljene kvalitete poziva od strane krajnjeg korisnika.

Algoritmi koji su složeniji mogu pružiti bolju kvalitetu zvuka (ili slike), ali uslijed duže obrade uvijek uvode veće kašnjenj te su manje otporni na gubitke!!!



Slika 1: VoIP komponente kašnjenja krajnjih sustava

Slika prikazuje funkcionalne komponente u VoIP krajnjim sustavima koji doprinose kašnjenju. Neki kodeci smanjuju kompresiju kako bi se smanjila širina pojasa potrebna za VoIP pozive, što neminovno dovodi do gubitka detalja od originalnog signala, stoga se općenito zahtijeva bolja kvaliteta poziva i veća propusnost ili širina pojasa koja će biti zahtijevana po pozivu.

ITU-T kodek	Tip kodeka	Max. kašnjenje kodeka (ms)	Brzina (bps)	Interval paketizacije (ms)	pps	Veličina payloada (bytes)	Veličina IP pkt (bytes)	IP bps
	PCM	0.375	64000	10	100	80	120	96000
G.711	PCM	0.375	64000	20	50	160	200	80000
G.711	PCM	0.375	64000	30	33.33	240	280	74659
G.723.1	ACELP	97.5	5300	30	33.33	20	60	15998
G.723.1	ACELP	97.5	5300	15	16.67	40	80	10669
G.723.16	ADPCM	0.375	16000	10	100	20	60	48000
G.723.16	ADPCM	0.375	16000	20	50	40	80	32000
G.723.16	ADPCM	0.375	16000	30	33.33	60	100	26664
G.726.24	ADPCM	0.375	24000	10	100	30	70	56000
G.726.24	ADPCM	0.375	24000	10	50	60	100	40000
G.726.24	ADPCM	0.375	24000	10	33.33	90	130	34663
G.726.32	ADPCM	0.375	32000	10	100	40	80	64000
G.726.32	ADPCM	0.375	32000	20	50	80	120	48000
G.726.32	ADPCM	0.375	32000	30	33.33	120	160	42662
G.726.40	ADPCM	0.375	40000	10	100	50	90	72000
G.726.40	ADPCM	0.375	40000	20	50	100	140	56000
G.?m40	ADPCM	0.375	40000	30	33.33	150	190	50662
G.728	LD-CELP	1.875	16000	10	100	20	60	48000
G.728	LD-CELP	1.875	16000	20	50	40	80	32000
G.728	LD-CELP	1.875	16000	30	33.33	60	100	26664
G.729A	CS-ACELP	35	8000	10	100	10	50	40000
G.729A	CS-ACELP	35	8000	20	50	20	60	24000
G.729A	CS-ACELP	35	8000	30	33.33	30	70	18665

Slika 2: Karakteristike VoIP kodeka

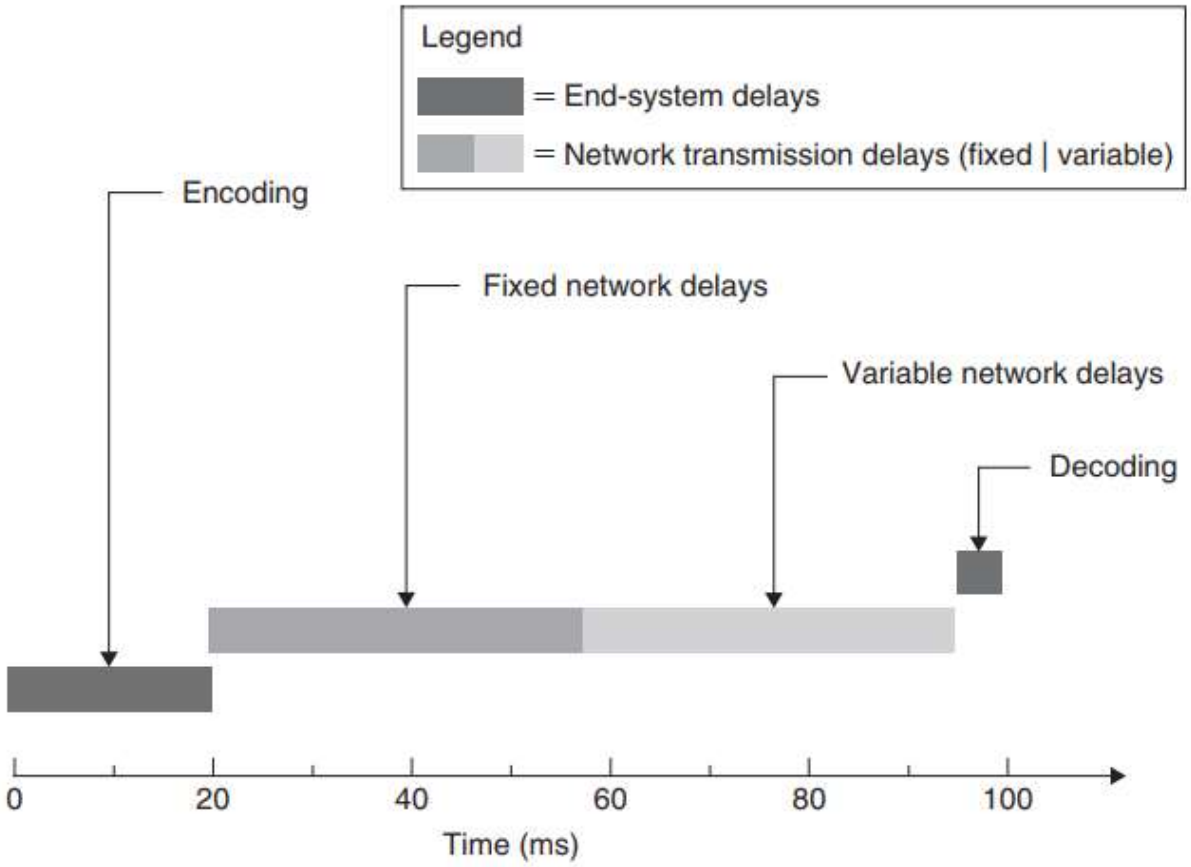
U sljedećem poglavlju proučavati ćemo utjecaj raličitih SLA metričkih parametara na VoIP aplikacije.

VoIP: Utjecaj kašnjenja na kvalitetu govora

Za VoIP je važno jednosmjerno kašnjenje sa kraja na kraj. Ako je kašnjenje veliko tada sudionici teško razlučuju razliku između prirodne pauze u govoru i kašnjenja unutar sustava. Ako dođe do greške kašnjenja sustava za vrijeme pauze u razgovoru ovo kašnjenje se može uzeti kao njihov znak za početak govora dok će u međuvremenu njihove riječi stići na drugi kraj tako da slušatelj sa druge strane može početi razgovarati s time da se normalni protokol razgovora ne prekida. Preveliko kašnjenje sa kraja na kraj također može umanjiti učinkovitost mehanizama koje se koristi za poništenje jeke. Kako bi pružio smjernice u dizajniranju mreža za podršku govorne usluge (VoIP) ITU-T je specificirao G.114 koji koristi E-model da bi procijenio učinak kašnjenja govora i kvalitete prijenosa. Preporuka G.114 sugerira da je maksimalno jednosmjerno kašnjenje s kraja na kraj od ~150ms granica koja osigurava da će korisnici biti zadovoljni za većinu aplikacija telefonije. Veća kašnjenja također mogu biti prihvatljiva ali sa posljedicom smanjenja zadovoljstva korisnika, a kašnjenje veće od 400 ms općenito se smatra neprihvatljivim, kao što je prikazano u tablici ispod

Ear-to-mouth kašnjenje (d)	R faktor	Objektivni MOS
D < 150 ms	80-89	5
150 ms < D <250ms	70-79	4
250 ms – D 325m-	60-69	3
325 ms < D < 425 ms	50-59	2
D > 425 ms	90-100	1

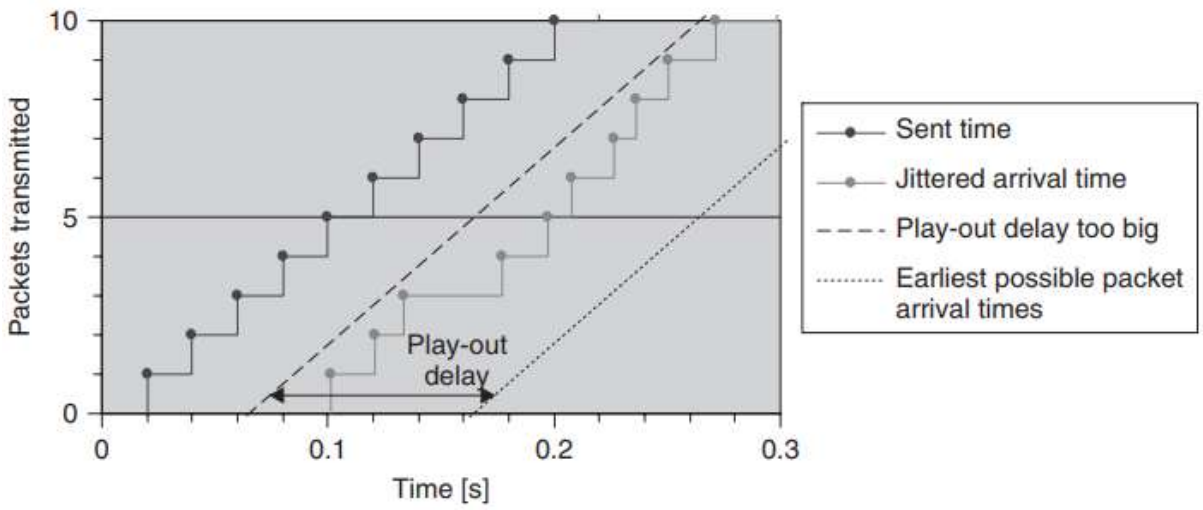
Mrežno kašnjenje je samo jedna komponenta kašnjenja koja utječe na VoIP poziv. Dakle, nakon što je utvrđeno maksimalno prihvatljivo kašnjenje za određene VoIP usluge, mrežni QoS dizajn bi trebao uzeti u obzir ovaj proračun te ga razdijeliti na razne dijelove mrežnog kašnjenja (propagacijsko kašnjenje kroz jezgrenu mrežu (*backbone*), raspored kašnjenja zbog zagušenja i serijalizacijsko kašnjenje kod pristupne veze) i kašnjenje krajnjih sustava (zbog VoIP kodeka i smetnji u spremniku). Primjer vremenske skale na slici 3 pokazuje dijelove kašnjenja koje utječu na kašnjenje VoIP usluga koristeći tipičnu vrijednost za svaku komponentu. Kašnjenje kodeka ovisi o vrsti kodeka koji se koristi. Tablica na slici 2 navodi maksimalno teoretsko jednosmjerno kašnjenje uvedeno od kodeka povezanih sa obradom. U praksi VoIP krajnji sustavi mogu imati dodatno kašnjenje od 5 - 20 ms ovisno o specifičnoj primjeni. Jednosmjerno mrežno kašnjenje od 35 – 150 ms obično je usmjereno na visoku kvalitetu VoIP usluga kako bi se osiguralo da se kašnjenje do 150 ms može dostići. Kako bi se osigurale ove vrijednosti neophodno je u mreži koristiti QoS mehanizme. Veće kašnjenje može biti tolerirano za niže kvalitete usluge.



Slika 3: VoIP: komponente kašnjenja ear-to mouth

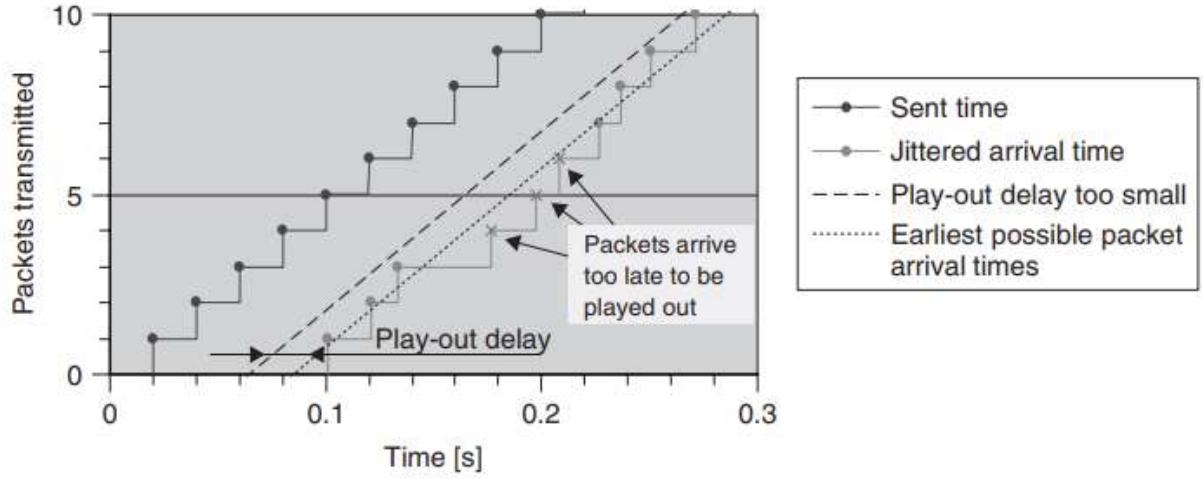
VoIP: Utjecaj varijacija kašnjenja - *jitter*

Uobičajena je zabluda da gubitak paketa ima veći utjecaj na kvalitetu VoIP poziva od mrežnog kašnjenja. Aplikacije koje su osjetljive na gubitak paketa, kao što je VoIP, koriste spremnike za otklanjanje varijabilnog kašnjenja kako bi izbjegle gubitke u zakašnjelom dolasku paketa i redosljedu dolasku paketa. Dekodiranje primljenog signala **sinkroni je proces** i stoga se podaci moraju pohraniti u dekoder, te dekodirati točno onim redosljedom kojim su i slani, te u jednakim vremenskim razmacima. **Spremnici za poništavanje smetnji uklanjaju varijabilno mrežno kašnjenje paketa ipretvaraju ga u fiksno kašnjenje na odredištu krajnjih sustava. To se vrši pomoću sa naše strane namjerno umetnutog dodatnog kašnjenja kako bi se eliminirale varijacije.** Ako se vremenski pragovi spremnika za regulaciju kašnjenja postave proizvoljno kao na slici 4 to može nametnuti nepotrebna velika kašnjenja te tako postaviti stroža ograničenja za karakteristiku transportne mreže (što znači da je nam je proračun earto-mouth kašnjenja dostupan za raspodijelu na mrežu limitiran) ili pak može utjecati na kvalitetu VoIP usluga.

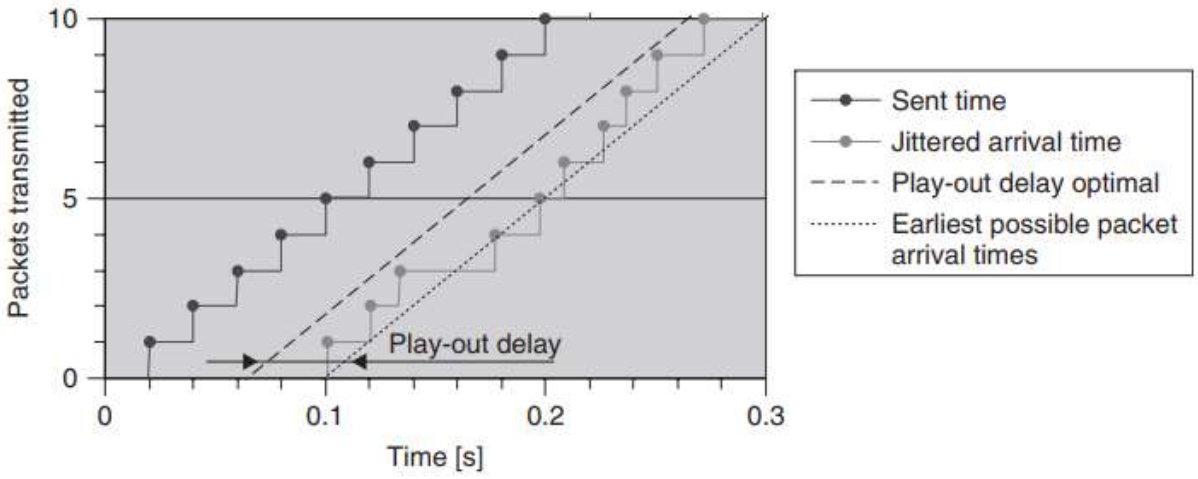


Slika 4: Preveliko unešeno kompenzacijsko kašnjenje spremnika za VoIP

Druga situacija je pak ako je vremenski prozor kod spremnika za otklanjanje smetnji kašnjenja premali da bi u njega upao zakašnjeli paket. Tada može doći do pojave presporog dolaska paketa do dekodera, tzv. *underflow* - situacija kada je spremnik prazan (jer paket koji kasni još nije stigao) u trenutku kada kodek treba uzeti uzorak, Takva situacija karakterizira se kao izgubljeni paket što je prikazano na slici 5



Slika 5: Premalo unešeno kompenzacijsko kašnjenje spremnika za VoIP



Slika 6: Optimalno kompenzacijsko kašnjenje spremnika za VoIP

Većina VoIP krajnjih sustava koriste adaptivne spremnike za uklanjanje smetnji čiji je cilj prevladati ove probleme dinamičnim podešavanjem vremenskog prozora
(ubačenog kašnjenja) na najnižu prihvatljivu vrijednost kao što je prikazano na slici 6. Dobro dizajnirani prilagodljivi algoritmi spremnika za uklanjanje kašnjenja neće ograničavati dizajn mreže.

VoIP: Utjecaj gubitka paketa na kvalitetu govora

Prikrivanje gubitka paketa (PLC – Packet Loss Concealment) je tehnika koja se koristi za maskiranje izgubljenih ili odbačenih VoIP paketa. Za razumjevanje PLC-a je potrebno razumjeti utjecaj koji ima gubitak paketa na kvalitetu VoIP poziva. Metoda prikrivanja gubitka paketa ovisi o vrsti kodeka koji se koristi. Jednostavni načini prikrivanja gubitka paketa je ponavljanje prethodno dobivenog uzorka. Ovu metodu koriste kodeci poput G.711 (PLC za G.711 je definiran u G.711 Dodatak I). Ovakva metoda maskiranja izgubljenog paketa može se primjeniti jer osim za ubrzano promijenjive dijelove govora, govorni signal je stacioniran i predvidljiv. Ova tehnika može biti učinkovita za prikrivanje gubitka uzorka otprilike od 20 ms. Interval paketizacije određuje veličinu uzoraka sadržanih u jednom paketu. Uz pretpostavku da imamo interval od 20 ms pakiranja paketa, gubitak dva ili više uzastopnih paketa će rezultirati primjetnom propadanju kvalitete glasa. Iz perspektive mrežnog dizajna, važno je imati na umu da planom možemo koristiti i intervale paketizacije od 30 ms, ali za danu vrijednost gubitka paketa moglo bi rezultirati uočljivo gorom kvalitetom poziva nego u intervalu paketizacije od 20 ms. Sa 30 ms intervala PLC neće biti u mogućnosti učinkovito prikriti gubitak jednog paketa. Stoga, tu nepromijenjenost dizajna mreže treba uzeti u obzir. Veći interval paketizacije može povećati propusnost VoIP poziva (ima relativno manje IP zaglavlje zbog toga što se više uzoraka provodi u jednom paketu), ali isto tako može rezultirati nižom kvalitetom poziva za određeni postotak gubitka.

Male brzine okvirno-baziranih kodeka poput G.729 i G.723, koriste sofisticiranije PLC tehnike, koje mogu prikriti od 30 – 40 ms gubitka s ″podnošljivom″ kvalitetom. Prikrivanje postaje problematično s kratkim fonetskim jedinicama u jeziku – gdje 30 ms uzorka može biti više od polovice jedne fonetske jedinice, a naknadni uzorci ne mogu pružiti dovoljno informacija o izgubljenom uzorku kako bi se omogućilo da se učinkovito prekrije. Slično kao

i za valno bazirane kodeke, ako je interval paketizacije veći od gubitka koji PLC algoritam može umetnuti, tada PLC neće biti u mogućnosti učinkovito prekriti gubitak jednog paketa.

Dakle, da sumiramo, utjecaj koji gubitak paketa ima na VoIP, s prikladnomodabranim intervalom paketizacije (20 – 30 ms ovisno o tipu kodeka koji se koristi)period gubitka paketa može biti skriven ali razdoblje gubitka od dva ili više uzastopnihpaketa može dovesti do primjetne degradacije kvalitete govora. Veličina vremenskog prozora za otklanjanje kašnjenje zbog udaljenosti, za određenu uslugu, izbor je davatelja usluga. Podržavajući VoIP usluge, bitno je da se razumije kakav utjecaj ovi ciljevi imaju na dizajn mreže u praksi, uzeti ćemo u obzir utjecaj mogućih uzoraka gubitka paketa prethodno definirano u odjeljku 1.2.3 :

- *Zagušenost.* Kada zagušenost utječe na VoIP promet, javljaju se redovi čekanja i VoIP paketi se odbacuju. Mrežni inženjer mora osigurati da se uzastopni paketi od jednog VoIP poziva ne odbacuju. Iz tog razloga, mrežna podrška za VoIP dizajnirana ja da eliminira zagušenja, te da su raspoloživi kapaciteti za VoIP promet u stanju nositi se sa vrhuncem ponuđenog VoIP prometnog opterećenja. Kako bi VoIP paketima taj kapacitet ostao zagarantiran koriste se QOS mehanizmi
- *Pogreške na nižim slojevima.* Kao što smo prije opisali, pogreške bita na fizičkom sloju mogu uzrokovati da paket bude odbačen zbog provjera na slojevima veza ili prijenosnom sloju. Dakle, bitske pogreške će obično

  rezultirati gubitkom cijelog paketa, što znači da će svaki paket stići ispravan ili uopće neće stići. QOS mehanizam ne može nam pomoći kod grešaka bita uslijed smetnji na fizičkom sloju. Tamo gdje temeljna mrežna prometna infrastruktura ne može zadovoljiti ciljeve malih gubitka bita (a samim time i cijelih paketa) na daljinu koje zahtijevaju VoIP usluge, biti će nam biti potrebna PLC tehnologija. Pogledajmo na primjer, tipični ponuđeni BER za usluge iznajmljenih linija od $1*10^{-9}$ i pretpostavljeni slučajni raspored pogreški, da svaka pogreška uzrokuje gubitak paketa (BER=PLR) i da G.711-20ms kodek

  koji se koristi proizvodi pakete od 200 bajta na 50 pps rezultat PLR bi bio

  $1*10^{-9} * 200 * 8 =$ **$1,6 * 10^{-6}$** Bez PLC-a to bi dovelo do efektivnog gubitka paketa od 1/(1.6*10 * 50pps* 60) sekunda = 208 minuta, što je bolje od tipičnih uslužnih ciljeva, koji imaju redoslijed od jednog izgubljenog zvučnog artefakta svakih 30 minuta. Upotreba PLC interpolacija još bi popravila tu karakteristiku
- *Greške elemenata mreže*. Greške na elementima mreže mogu uzrokovati gubitke paketa sve do ponovnog uspostavljanja veze oko palog elementa mreže. Rezultat gubitka ovisi o mrežnoj tehnologiji koja se koristi. U „običnoj“ IP (ne MPLS) mreži, čak i u dobro dizajniranim mrežama gdje je vrijeme IGP konvergencije 100 ms, gubitak paketa nakon greške na mrežnom elementu je previše značajan da bi se prikrio i to rezultira zvučnim smetnjama. Tamo gdje je implementiran MPLS TE FRR ili ekvivalentne tehnike, gubitak povezanosti nakon greške na mrežnom elementu je unutar 50 ms, te će PLC uglavnom moći nadoknaditi rezultantni gubitak paketa.

- *Gubitak u aplikacijama krajnjih sustava*. Gubitak uslijed underflows (nedovoljne brzine dolaska) i poplave paketima može se spriječiti pažljivim dizajniranjem krajnjih sustava.

U praksi, mreže koje podržavaju VoIP trebale bi biti dizajnirane tako da postotak gubitka VoIP paketa bude blizu nule. Planiranje kvalitetnih pristupnih veza, kapaciteta na cijeloj trasi, proračun brzina i umetnutog kašnjenja svih elemenata te upotreba QOS mehanizama trebalo bi osigurati da nema izgubljenih paketa zbog zagušenja. Ukoliko dođe do gubitka paketa, utjecaj gubitka treba smanjiti na prihvatljivu razinu koristeći PLC tehniku.

VoIP: Utjecaj propusnosti

VoIP kodeci obično proizvode tok podataka konstantne brzine (*stream*), s propusnosti koja je prikazana na slici 1.6. Konverzcijski govor sadrži oko 0.5% tišine, a to se može iskoristiti za smanje tražene brzine prijenosa (prosječnu propusnost koja se koristi za poziv). Funkcija suzbijanja „tišine“ koja je također poznata kao *VAD – Voice Activation Detection*, spriječava prijenos „tihih“ paketa. Potiskivanje tišine postaje aktivno kada se otkriju razdoblja tišine od mikrofona koje prelaze utvrđene granične vrijednosti. Mreža koja podržava VoIP obično se dizajnira da gubitak VoIP paketa bude blizu 0% i stoga su dizajnirane tako da zagušenje bude što manje iz perspektive VoIP prometa. To znači da raspoloživi kapacitet za VoIP promet mora biti u stanju nositi se maksimalnim prometnim opterećenjem za ponuđeni VoIP promet. U praksi se susrećemo sa slijedećim problemima. Čak i ako je VoIP kapacitet pripremljen za podršku maksimalnog opterećenja, VoIP usluga može biti statistički planirana. Na primjer. Uzmimo pretpostavku da neka veza može podržati maksimalno 30 istodobnih VoIP poziva osiguravajući i da su ciljevi kašnjenja, smetnji i gubitaka uvijek ispunjeni za taj broj poziva. U realnoj praksi, samo dio od ukupnog broja korisnika u nekom trenutku obavlja pozive koji traju određeno vrijeme. Stoga mnogo više od 30 krajnjih korisnika može biti podržano projektiranom vezom koristeći statističko mulipleksiranje. Ako više od 30 korisnika bude pokušalo uspostaviti pozive na vrhuncu prometnog korištenja, VoIP opterećenje može prelaziti raspoloživost VoIP kapaciteta. U tome slučaju usluge svih poziva u tijeku mogu biti degradirane. Ako je vjerojatnost takvog događa dovoljno visoka, onda može biti potreban pristup sustavu kontrole da se ograniči broj VoIP poziva koji istovremeno može biti postavljen kako raspoloživi kapacitet nikad ne bi bio premašen u praksi. Također treba obratiti pažnju na uporabu kodeka sa manjim bitskim brzinama. Oni nam omogućavaju da kroz neki komunikacijski kanal postavimo više VoIP kapaciteta, ali oni troše znatno više vremena za kodiranje i dekodiranje, pa nam ograničavaju uslugu uslijed povećanja kašnjenja.

Video prijenos (*stream*)

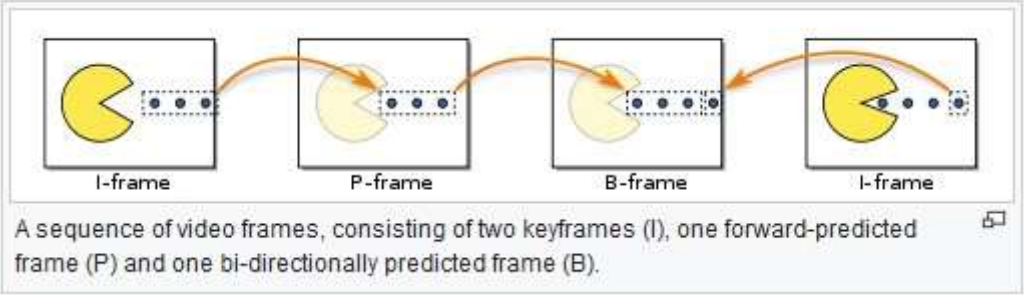
Kod *video stream* aplikacija, klijent zahtijeva primanje videa koji je pohranjen na poslužitelju (server). Serveri šalju *stream* videa klijentu koji započinje gledati video prije nego što su svi podaci video streama primljeni. Video stream se koristi i za „emitiranje“ video kanala, koji se često isporučuju preko IP mreže većem broju korisnika (multicast) ili pak za video na zahtjev (VOD – Video On Demand), koje se isporučuje preko IP mreže pojedinom korisniku(unicast).

Video stream baziran na IP najčešće se prenosi kao tok podataka kodiran MPEG (Motion Picture Expert Group) standardom i prenosi se koristeći RTP preko UDP načina prijenosa.

MPEG definira kodiranje koje se koristi za stvarni video stream, dok [RFC2250, RFC 2343, RFC, 3640] standardi definiraju kako će se za usluge u realnom vremenu (realtime) ti kodirani video i audio podaci oblikovati za prijenos pomoću RTP protokola. RTP je protokol prijenosnog sloja, koji obavlja isporuku toka podataka od pošiljatelja do primatelja. MPEG odbor je radna grupa Međunarodne Organizacije za Standardizaciju/Međunarodne Elektrotehničke Komisije (ISO/IEC) koja radi na razvoju standarda za digitalni audio i video. MPEG je odgovoran za proizvodnju brojnih standarda koji se mogu koristiti za IP usluge uključujući MPEG-2 (dio videa koji je isti kao u ITU-T standardu H.262), koji se koristi za kodiranje kvalitetnog video signala kod usluge digitalne televizije. Novi MPEG- 4 AVC (Advanced Video Coding) standard koji je dizajniran za audio i video kodiranje nudi potencijalno dvostruko smanjene brzine od MPEG-2 za usporedivu kvalitetu video reprodukcije. MPEG koder pretvara i komprimira video signal u niz slika ili okvira. Uglavnom postoji samo mala količina promjena između uzastopnih okvira pa je moguće komprimirati odašiljanje na način da video signal emitira samo značajne razlike. Postoje tri različite vrste MPEG okvira koje se koriste za vrijeme odašiljanja videa:

- „I“ okviri (*frame*). Unutarnji ili „I“ okviri nose kompletni video okvir i kodiraju se bez pozivanja na druge okvire. Na početku kodiranja postavljaju reverencu za rad P i B okvira. Periodički se ponovno generiraju kako bi osvježili referencu ili u situacijama kada se slika vrlo brzo mjenja te je P i B okviri ne mogu dovoljno precizno pratiti.

- „P“ okviri. Prediktivno kodirani ili P- okviri kodirani su pomoću prijedloga kompezacija Zahtjevaju predhodno dekodirani P-okvir kako bi uspostavili referencu. Mogu sadržavati podatke same slike kao i vektor pokreta ili kombinaciju oba podatka. U verziji H.264, mogu koristiti reference na više predhodno dekodiranih okvira. Uobičajeno je d aim je veličina 10-30% u odnosu na povezane I-okvire.
- ″ B ″ okviri. Dvosmjerni ili ″B″ okviri koriste prethodne i slijedeće okvire za postavljanje svoje reference. B-okviri pružaju daljnu kompresiju, a veličina im je oko 5-15% veličine od povezanih I-okvira.



Slika 7: Način korištenja I,P i B okvira

Okviri su raspoređeni u grupu slika ili GOP, na primjer, Europski PAL (Phase Alternating Line) MPEG-2 video format koristi GOP veličine 15, dok Sjeverna Amerika NTSC (National Television system committe) format koristi GOP veličine 18.

Brzina okvira za PAL je 25 sličica u sekundi (fps) a za NTCS je 29.97 slika u sekundi. Svaki GOP obično će kodirati (15/25) = ~(18/30) = ~0.6 sekundi videa. Postoji mnogo mogućih GOP struktura i sastava I, P, B okvira untar GOP koji je određen formatom izvornog video signala, i propusna ograničenja u kodiranju video streama (koji određuje potreban omjer kompresije), a možda i ograničenja na kašnjenje kodiranja/dekodiranja. Svaki GOP ima jedan I-okvir, i obično 2 do 14 P-okvira i 2 do 10 B-okvira. Ispravna GOP struktura može se opisati po broju okvira u GOP (GOP veličina) i razmak P-okvira unutar GOP. Tipična GOP struktura veličine 15 sličica i Pokvira razmaka od 3 (označeno kao 15/3 GOP strukture) prikazana je ispod:

$$B_1 B_2\ I_3\ B_4 B_5 P_6 B_7 B_8 P_9 B_{10} B_{11} P_{12} B_{13} B_{14} P_{15}$$

GOP struktura prikazana je gore u redu zaslona. Kako bi se omogućilo predviđanje unatrag, koder ponovno šalje okvire iz zaslona kako bi se B-okviri prenijeli nakon prethodnog i slijedećeg okvira reference. Rezultat okvira poslanih u dekoder je :

$$I_3 B_1 B_2 P_6 B_4 B_5 P_9 B_7 B_8 P_{12} B_{10} B_{11} P_{15} B_{13} B_{14}$$

Ovo ponovno slanje unosi kašnjenje i na kodiranje i na dekodiranje ovisno o brojuuzastopnih B-okvira.Za razliku od VoIP-a gdje je je kodek implementacije vrlokonkretno definiran, sa video stream postoji značajan prostor za varijacije uspecifičnom načinu na koji MPEG stream može biti kodiran, čak i za jednu vrstukodiranja. Specifična GOP struktura za kodiranje video streama može imati velik utjecaj na gubitak paketa, kašnjenje i propusnost usluge do prijamnika.

Video prijenos (*stream*) – Utjecaj kašnjenja

Kod video streming-a ono što nas zanima je jednosmjerno kašnjenje i *jitter* paketa od video servera do prijemnog uređaja.

To kašnjenje direktno utječe na interaktivnost krajnjeg korisnika tj. utječe na tzv. „*finger-to-eye*“ kašnjenje koje se očituje u trenutku kada korisnik mjenja kanal koji prati. To je vrijeme potrebno da nakon odabira novog kanala na daljinskom upravljaču dobijemo sliku tog kanala na ekranu.

Kako bismo bolje shvatili utjecaj kašnjenja, razmotriti ćemo zasebno nekoliko vrsta video streaming aplikacija.

Broadcast Video Service (IPTV) – uglavnom koristi multicast odašiljanje. Jednosmjerno kašnjenje kod ove vrste aplikacija uzrokuje nestanak slike sa TV uređaja za vrijeme promjene kanala (channel change time).

Uglavnom se pokušava postići da ovo vrijeme bude unutar 1-2 sekunde. Pretpostavimo da se IPTV usluga pruža putem set-top box (STB) gdje nam svaki kanal predstavlja drugu multicast adresu.

Ukupno vrijeme kašnjenja sastavljeno je od nekoliko komponenti:

- *Kašnjenje daljinskog upravljača i STB procesuiranja zahtjeva*. Nakon prijema komande za promjenom kanala iz daljinskog upravljača, STB izdaje zahtjev za napuštanje jedne multicast grupe (IGMP) i zahtjev za pretplatu na drugu multicast grupu. Ovo tipično traje nekoliko destetaka milisekundi, ali mi ćemo uzeti najgori slučaj od 50ms.

- *Mrežno kašnjenje*. Ovdje govorimo o kašnjenju IGMP zahtjeva između STB i prvog multicast svjesnog mrežnog elementa. Ovo kašnjenje se sastoji od kašnjenja serijalizacije, prospajanja, čekanja u redu i propagacijskog kašnjenja. Mrežni QoS mehanizmi su uključeni kako bi se osiguralo da IGMP poruka ne bude odbačena od mreže i da bude prioritizirana u redovima čekanja. Ovo kašnjenje tipično iznosi ispod 100ms.

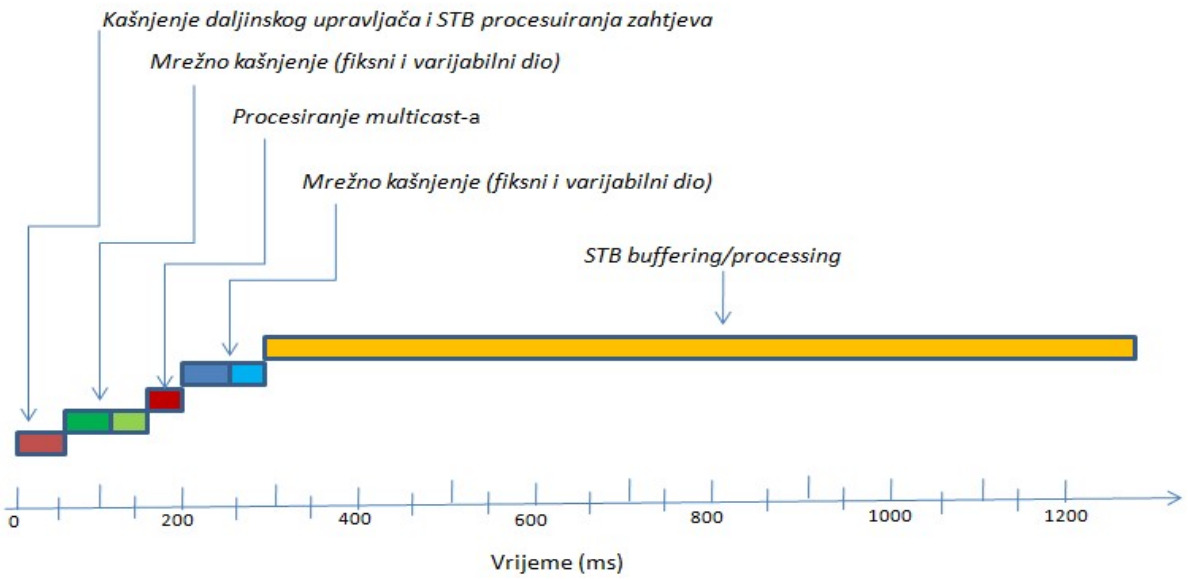
- *Procesiranje multicast*-a. Kada prvi multicast svjesni mrežni element zaprimi IGMP poruku za napuštanje multicast grupe, on prestane odašiljati pakete prema prijemnom sučelju. Kada zaprimi IGMP poruku za učanjenje u drugu multicast grupu, on počinje slanje paketa drugog kanala (uz uvjet da na tom uređaju već stižu paketi traženog kanala. Ukoliko ne stižu, pokreće se multicast signalizacija prema mrežnom elementu na koji paketi tog multicasta stižu). Ovo kašnjenje obično iznosi nekoliko desetaka milisekundi, a mi smo za ovu prezentaciju uzeli najgori slučaj kašnjenja od 100ms.

- *Mrežno kašnjenje*. Ovo je mrežno kašnjenje koje treba multicast paketima da stignu do STB-a. Tipično iznosi ispod 100ms.

- *STB buffering/processing*. Potrebno je prikupljanje određenog broja paketa u ulazni spremnik prije nego što počne dekodiranje samog video toka. Ovdje imamo nakupljanje nekoliko vrsta kašnjenja.

    - Kašnjenje u spremniku za otklanjanje jitter-a,

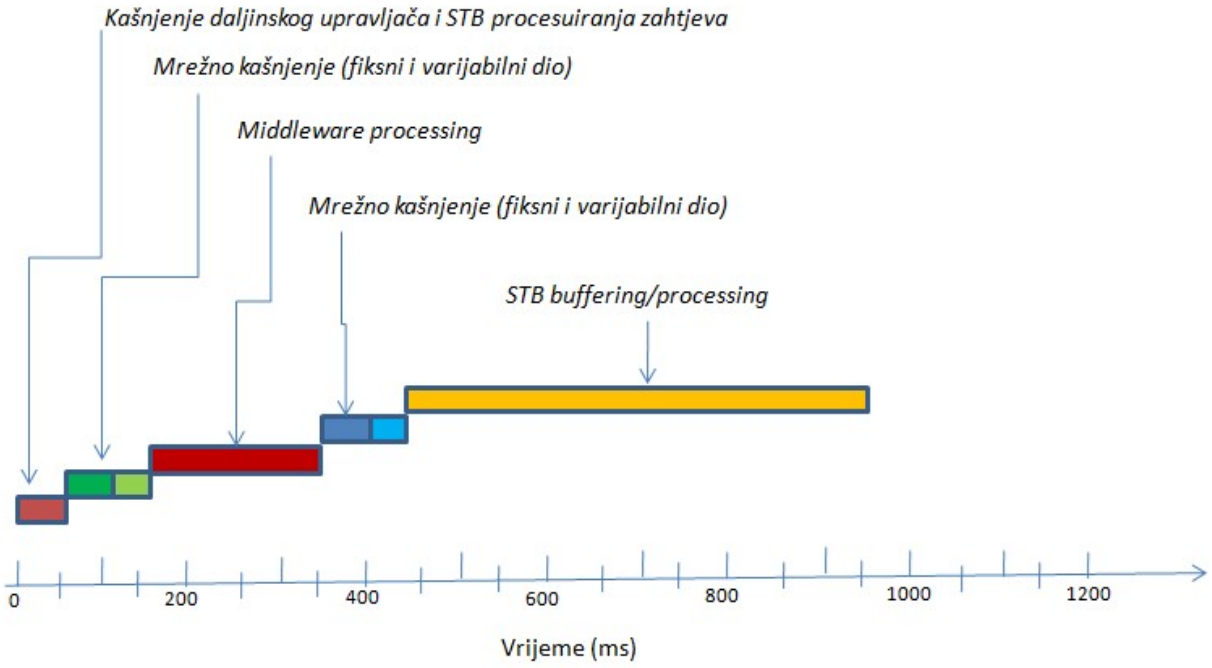
- FEC – tj. kašnjenje retransmisije kod sustava koji imaju zaštitu od mrežnog gubitka paketa,
- Dekripcijsko kašnjenje – STB periodički dobiva dekripcijske ključeve kako bi mogao de-kriptirati pakete,
- kašnjenje ulaznog spremnika MPEG dekodera,
- Kašnjenje IBB okvira – dekoder treba čekati dok ne zaprimi IBB sekvencu prije nego započne dekodiranje. Za 15/3 GOP strukturu, ovo kašnjenje je tipično oko 650ms.



Slika 8: Komponente kašnjenja kod Broadcast videa (IPTV)

„Video na zahtjev“ (*Video-on-demand*).

- Ova usluga koristi unicast adresiranje umjesto multicasta.
- Ovdje se umjesto kašnjenja multicasta javlja kašnjenje izazvano opremom koja obrađuje zahtjev za video-on-demand tzv. *Middleware processing*. Tipčno iznosi nekoliko stotina milisekundi.
- Kod VOD-a (Video-on-demand) razlikuje nam se i STB buffering/processing kašnjenje. Za razliku od broadcasta gdje STB treba čekati I-okvir prije nego što započne dekodiranje video signala, ovdje se IBB sekvenca odmah šalje kao prva informacija, pa je STB kašnjenje smanjeno i tipično traje oko 500ms.



Slika 9: Komponente kašnjenja kod „Video na zahtjev“ usluge

Video prijenos (*stream*) – Utjecaj varijacija kašnjenja (*jitter)*

- Digitalni video dekoderi imaju vrlo malu toleranciju na jitter od svega **+-500ns** za dekodiranje videa bez vidlivih odstupanja.
- Tako oštri zahtjevi ne mogu se zadovoljiti u običnim IP mrežama, pa se koriste spremnici za eliminaciju varijacija kašnjenja tj. za pretvaranje varijabilnog kašnjenja u **stalno** tvz. *Play-out buffers*.
- Ovi spremnici moraju biti optimalno dizajnirani kako bi zadovoljili i najveća kašnjenja signala.
- Kapacitet spremnika mora biti barem 100ms veći od najveće varijacije kašnjenja koju očekujemo.

Video prijenos (*stream*) – Utjecaj gubitka paketa

- Svaki MPEG okvir prenosi se kao tok MPEG-TS paketa koji su tipično dugi 188 bajtova, a svaki IP paket nosi od 1 do 7 MPEG-TS paketa.
- Jedan dekodirani MPEG okvir obuhvaća nekoliko IP paketa. Ukoliko ne bi koristili tehnike za oporavak od gubitka paketa, gubitak samo jednog IP paketa bio bi vidljiv na kvaliteti reprodukcije videa jer bi uzrokovao gubitak cijelog MPEG okvira.
- Gubitak I-okvira uzrokuje vizualnu smetnju u reprodukciji sve dok se ne primi slijedeći I-okvir.
- Gubitak P-okvira uzrokuje smetnje na nekoliko slijedećih okvira, a
- Gubitak B-okvira uzrokuje smetnje samo u tom jednom okviru.

Veće GOP strukture pružaju nam veću kompresiju signala, tj. uz jednaku bitsku brzinu možemo slati video veće kvalitete, ali u slučaju gubitka paketa – greška u reproduciranom signalu znatno je veća. Također je i veći utjecaj na interaktivnost korisnika tj. povećava se kašnjenje kod prebacivanja kanala na daljinskom upravljaču.

Gubitci paketa mogu nastati iz slijedećih razloga:

- Usljed zagušenja na trasi
- Usljed grešaka na nižim slojevima
- Usljed kvara nekog od elemenata na trasi
- Usljed gubitka koji je nastao u aplikacijskom krajnjem sustavu

Gubitak paketa usljed zagušenja na trasi

Mreže koje podržavaju video prijenose trebale bi biti potpuno otporne na zagušenja, te se paketi zbog toga ne bi trebali gubiti, tj. instalirana širina pojasa trase trebala bi zadovoljiti potrebe u vršnim opterećenjime, a za svaki slučaj još se primjenjuju i sustavi kontrole pristupa i rezervacije resursa.

Gubitak paketa usljed grešaka na nižim slojevima (*Lower layers errors*)

To su gubici paketa koji nam nastaju usljed nesavršenosti veza (npr. loši kontakti žica ili smetnji izazvanih vanjskim utjecajem na naš prijenosni vod). Obzirom da govorimo o fizičkom

sloju, a veze su jako duge i sačinjene od više komponenata, ove gubitke nikada u praksi ne možemo izbjeći. Postoje različite trasportne tehnologije. Neke su otpornije, a neke manje otporne na gubitke u fizičkom sloju. Svaka od tih tehnologija ima definiranu neku statističku vrijednost PLR-a koju treba zadovoljavati, pa je to također potrebno uzimati u obzir kada se dizajnira mreža za neku uslugu, u ovom slučaju za video prijenos.

Ciljana **udaljenost gubitka** paketa odabir je svakog davatelja usluga, ali u praksi se pokazalo da se oni uglavnom odlučuju za udaljenost gubitka od **jedne vidljive smetnje u sat vremena (kako je to definirao i DVB standard za IPTV)**.

Idemo sada pogledati što to u realnosti znači.

Pretpostavimo da imamo 3.7Mb/s MPEG tok sa 1356-bajtnim paketima (jer jedan IP paket nosi do 7x188 bajta videa u svakom paketu, + 40 bajta za RTP, UDP i IP zaglavlje) što nam pak daje tok od približno 350 paketa u sekundi.

Za ovakav tok paketa i uz odaljenost gubitka od jednog sata možemo izračunati ciljani maksimalni dozvoljeni PLR koji za ovaj slučaj iznosi ne više od

1/(350pps*60min*60sec)= oko $1*10^{-6}$

Sada pogledajmo kako se taj cilj odražava na dizajn mreže. Prvenstveno ćemo gledati utjecaj gubitaka paketa na nižim mrežnim slojevima, tj. gubicima usljed samih fizičkih prijenosnih medija.

Uzmimo za primjer **SONET/SDH** prijenos koji nam nudi BER bolji od $1*10^{-12}$ i pretpostavimo da imamo slučajnu distribuciju gubitka i da svaki gubitak bita uzrokuje gubitak cijelog paketa. Ovo bi rezultiralo sa PLR-om od

$1*10^{-12}$*1356*8(bita za jedan bajt)= približno $1*10^{-8}$

Što bi rezultiralo gubitkom jednog paketa svakih 79 sati, što je znatno bolje od traženog.

Ali idemo sada pogledati kako bi to izgledalo za **DSL linije** koje nam pružaju BER od $1*10^{-7}$.

Ovdje nam PLR izgleda:

$1*10^{-17}$*1356*8(bita za jedan bajt)= približno $1*10^{-3}$

Što bi rezultiralo gubitkom paketa svake 3 sekunde – što je pak znatno lošije od traženog.

Obzirom da se greške na fizičkom sloju ne mogu izbjeći, uvode se dvije metode za ispravke tih grešaka.

- Foreward Error Correction
- Retransmisija u realnome vremenu

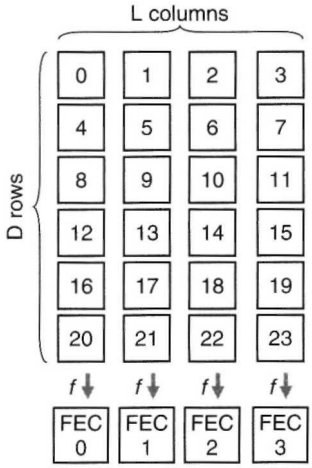
Foreward Error Correction, tj. sustav oporavak gubitka paketa, temelji se na redundanciji i ugrađuje se u tok bita prometa, a uloga mu je da prepozna grešku i da rekonstruira paket kako bi se izbjegla retransmisija paketa.

Profesionalni-MPEG Forum [PRO-MPEG] objavljen u pravilniku o postupanju (COP) broj 3 predlaže plan temeljen na pristupu definiran u RFC 2733 [RFC 2733] koji se određuje FEC mehanizmom za zaštitu RTP prijenosa od izgubljenih RTP paketa. U MPEG-Pro Forum shemi, XOR operacije izvode se na bloku paketa raspoređenih u matrici od D redova i L stupaca za generiranje redundantnih pariteta paketa. Unutar prijemnika, FEC informacije se koriste za oporavak od gubitaka paketa unutar FEC bloka.

Struktura matrice koja oblikuje FEC blokove utječe na

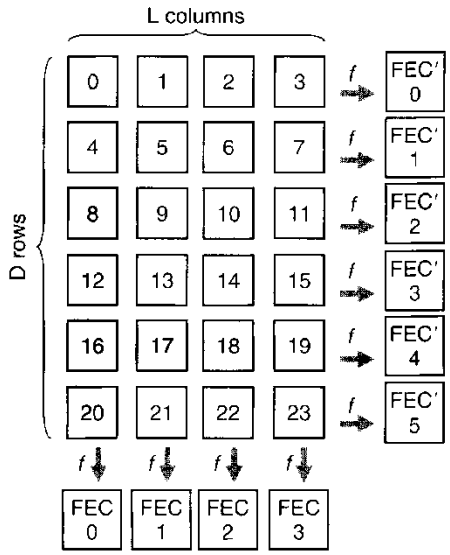
- veličinu „gubitak praska“ od kojeg nas FEC množe zaštititi,
- propusnost povezanu s FEC prijenosom i
- kašnjenjem uzrokovano FEC mehanizmom.

Dakle, važno je da se FEC parametri mogu konfiguruirati da odgovaraju zahtjevima određene usluge, uzimajući u obzir karakteristike temeljne mreže.



Slika 10: Profesionalni-MPEG Forum COP 3 1D FEC

Pro-MPEG Forum sustav omogućuje obje jednodimenzionalne (1D) FEC, kao što je prikazano na Slici xxx, i dvodimenzionalni (2D) FEC, kao što je prikazano na Slici xxx.



Slika 11: Profesionalni-MPEG Forum COP 3 2D FEC

FEC informacije se prenose u posebnom toku paketa (za 1D FEC) ili tokovima (za 2D FEC) u video nositelju.

Jednodimenzionalni FEC je u mogućnosti da ispravi 1 pogrešku u FEC bloku i ima pretek (*overhead*) L/(L ·D).

Dvodimenzionalna shema je u mogućnosti od gubitka praska oporaviti L pogrešaka unutar FEC bloka i ima pretek (dodavanje zalihosnih podataka) (L + D)/(L ·D).

Dodatno kašnjenje koje unose obje sheme je vrijeme potrebno za prijenos L ·D dodatnih paketa. Veća D vrijednost smanjuje pretek na račun povećanja dodatnog kašnjenja.

Na primjer, uz pretpostavku 3,7 Mb/s MPEG-2 prijenos koji se sastoji od ~ 350 paketa u sekundi, a svaki paket s 1356 bajta nosivosti:

❖ Korištenje jednodimenzionalnog FEC s L = 4 i D = 6 pruža mogućnost oporavka od 1 pogreške u 24 paketa, a unosi se 4/(4 ·6) ≈17% preteka informacija i uzrokuje se 24/330 ≈72 ms dodatnog kašnjenja zbog FEC procesuiranja.

Uz pretpostavku PLR od 1 $\cdot 10^{-3}$(prethodno izračunatom tipičnom PLR-uza ADSL), sa slučajnom distribucijom gubitka paketa, vjerojatnost nepopravljivoga gubitka (tj. 2 izgubljena paketa) unutar 24 bloka paketa (1 $\cdot 10^{-3} \cdot 24$) ·(1 $\cdot 10^{-3} \cdot 23$) ≈6 $\cdot 10^{-4}$; to rezultira gubitkom udaljenosti od ~5 sekundi, što je još nekoliko redova veličine lošije od ciljane vrijednosti.

❖Za usporedbu, korištenjem dvodimenzionalnog FEC s L = 4 i D = 6 pruža mogućnost oporavka od gubitka praska 4 pogreške u 24 paketa, dok se unosi (4 + 6)/(4 ·6) ≈42% preteka i 24/330 ≈72 ms dodatnog kašnjenja zbog FEC procesuiranja.

[1] It is noted that the delay due to the FEC processing operation for a matrix size of $m \cdot n$ reduces in absolute terms as the rate of the encoded MPEG stream increases, because the time to transmit m · n packets reduces accordingly.

Uz pretpostavku PLR od $1 \cdot 10^{-3}$, vjerojatnost nepopravljivog gubitka (tj. 5 izgubljenih paketa) unutar bloka od 24 paketa je $(1 \cdot 10^{-3} \cdot 24) \cdot (1 \cdot 10^{-3} \cdot 23) \cdot (1 \cdot 10^{-3} \cdot 22) \cdot (1 \cdot 10^{-3} \cdot 21) \cdot (1 \cdot 10^{-3} \cdot 20) \approx 5 \cdot 10^{-9}$; što rezultiraudaljenosti gubitka većoj od ~155 sati, što je za nekoliko redova veličine bolje od ciljane vrijednosti.

Retransmisija u realnom vremenu.

Prijenosi medijskih podatakakoji koriste RTP su donekle otporni na gubitke, u prijemnicima mogu koristiti mehanizme definirane za protokol upravljanja RTP (također poznat kao RTCP) koji javljaju pošiljatelju statistiku zaprimljenih paketa i time omogućuju pošiljatelju da prilagodi svoje odašiljanje. Dodatne tehnike su definirane u IETF, koje se šire osnovne mogućnosti RTCP kako bi se omogućile brže povratne informacije o gubitku paketa od prijemnika do pošiljatelja [RFC 4584], kako bi izgubljeni paketi mogu biti ponovno odaslani [RFC 4588]. Unutar određenog vremenskog okvira, prijamnici mogu otkriti nedostatak nekog paketa po rednim brojevimai prijavit te pakete nazad pošiljatelju koristeći RTCP negativna potvrde prijema (NACK-ovi), koji retransmitira izgubljene pakete.

Retransmisija u realnom vremenu je reaktivni sustav, koji ponovo šalje samo one pakete koji su izgubljeni, stoga nastaje minimalni pretek širine pojasa. Nedostatak ovog pristupa je, da se dodaje kašnjenje jednakoRTT (*Round Trip Time*)između prijemnika i retransmisijskog izvora, na potencijalne najgore slučajeve kašnjenja do kojih paket inače može doći. Dakle, u stvarnom vremenu retransmisija je izvediva samo u slučajevima u kojima RTT između prijemnika i izvora može biti mala, kako bi se izbjeglo povećanje vremena promjene kanala ili smanjuje VOD odaziva.

Treba napomenuti, međutim, da neki krajnji video sustavi onemogućuju UDP provjeru (*UDP checksum*), ili koristite "UDP-lite" [RFC 3828], tako da će paketi sa bitima greške biti primljeni uključujući i pogrešne bite, a to temelje na pretpostavci da je bolje primiti paket sa nekim pogrešnim bitom nego uopće ne primiti cijeli paket. Trenutno, međutim, ne postoji dovoljno podataka o performansama takvih implementacija da bi se moglo odrediti kakav utjecaj to ima na primljene video usluge u praksi.

Kvar mrežnoga elementa.

Kvar mrežnoga elementa može izazvati gubitke paketa do ponovnog uspostavljanja veze oko pokvarenog mrežnog elementa. Rezultirajući period gubitaka ovisi o vrsti mrežnih tehnologija koje se koriste. U "običnoj" IP (tj. ne-MPLS) mreži, čak i u dobro osmišljenoj mreži gdje je IGP vrijeme konvergencije ispod sekunde, gubitci paketa nastali usljed kvara mrežnog elementa su toliki da ih ni jedna gore opisana tehnologija zaštite ne može prikriti.

Na primjer, pretpostavimo gubitak veze od 500 ms i utjecaj na 3,7 Mb/s MPEG-2 video tok od 350 paketa u sekundi, ~ 175 paketa će biti izgubljeno zbog prekida veze.

Čak i ako koristimo MPLS TE FRR ili ekvivalente tehnike, koje skraćuju gubitak povezanosti usljed kvara mrežnog elementa na manje od 50 ms, gubitak paketa može biti previše značajan da se mogao prikriti korištenjem bilo koje od predhodno opisanih tehnika.

Na primjer, pretpostavljajući gubitak veze od 50 ms i utjecaj na 3,7 Mb/s MPEG-2 video tok od 350 paketa u sekundi, ~ 18 paketa će biti izgubljeno zbog prekida veze.

Tamo gdje je utjecaj mrežnih ispada takav da se ciljana udaljenost gubitka za video usluge ne može ispuniti, mogu nam pomoći tehnike uporaba redundantnih tokova podataka. Dostupne tehnike su bazirane na prostornoj ili vremenskoj redundanciji.

Prostorna redundancija tokova – tehnika se bazira na slanju dva toka podataka po dvije različite fizičke trase između izvora i prijemnika. Osiguravanje potpuno različitih fizičkih trasa za te tokove podataka može se ostvariti uporabom MPLS TE tehnika. U normalnom radu, prijemnik će primati po dvije kopije svakog paketa, od kojih će jedna biti odabrana za reprodukciju. Ukoliko dođe do prekida veze na jednoj trasi, prijemnik će nastaviti primati pakete sa druge trase i video prijenos će biti neprekinut. Ovakve tehnike umeću 100% preteka (*overhead*) na potrebnu širinu pojasa jer u stvarnosti šalju dva ista toka po dvije trase, a također moraju uključiti kašnjenje u prijemniku koje u najmanjem slučaju mora biti jednako najvećoj razlici prijenosnog kašnjenja između te dvije trase (u praksi to može biti zanemarivo)

Vremenska redundancija tokova – tehnika se bazira na razbijanju toka podataka u blokove, gdje se svaki pojedini blok šalje dva puta i to sa vremenskim pomakom. Razmak između istih blokova podataka mora biti takav da je veći od vremena oporavka mreže od kvara. U normalnom radu, prijemnik će unutar nekog vremenskog prozora primiti obje kopije bloka podataka od kojih će jedna biti izabrana za reprodukciju. U slučaju kvara nekog mrežnog elementa, barem jedna kopija bloka će stići do prijemnika. Ova tehnika također unosi 100% preteka na širinu pojasa (jer se informacija šalje dvaput). Međutim, ova tehnika ne mora nužno uzrokovati povećanje „*finger-to-eye*“ kašnjenja ukoliko se koristi samo u jezgrenoj mreži, a ne skroz do korisničkog krajnjeg uređaja.

Video prijenos (stream) – Utjecaj propusnosti

Zahtjevana širina pojasa za video prijenos ovisi o video formatu, video dekoderu i GOP strukturi. Postoje 4 glavna video formata koja se koriste:

SD (Standard Definition)

- američki NTSC (480 vertikalnih linija sa 720 piksela, te 29.97 okvira/s) i
- europski PAL sustav (576 linija sa 720 piksela, te 25 okvira u sekundi)

HD (High Definition) – imamo 2 formata.

- 720p: 720 x 1280 sa 50 i 60 okvira u sekundi
- 1080i: 1080 x 1920 sa 25 i 30 okvira u sekundi

Common interchange format (CIF). Ovo je format niže definicije za širokopojasne video aplikacije poput video konferencije.

- 240i: 240 x 352 (NTSC baziran)
- 288i: 288 x 352 (PAL baziran)

Quarter CIF (QCIF) – namjenjen za prikaze na mobilnim uređajima

- NTSC baziran 120 x 176
- PAL baziran 144 x 176

MPEG dozvoljava da video tok bude kodiran varijabilnom brzinom bita koja nam pruža konstantnu kvalitetu video prikaza ili da bude kodiran konstantnom brzinom bita što nam daje varijabilnu kvalitetu video reprodukcije.

FORMAT	MPEG-2	MPEG-4 AVC
LD QCIF	100-200 kb/s	50-100kb/s
LD CIF	0-5-1 Mb/s	2-3Mb/s
SD 4CIF	3-4Mb/s	2-3Mb/s
HD	15-20Mb/s	10-15Mb/s

Treba biti svjestan da veće GOP strukture, koje kao rezultat imaju smanjenje potrebne širine pojasa za jednaku kvalitetu reprodukcije videa, sa druge strane utječu na veću ranjivost u slučaju gubitka paketa, a također i na vrijeme promjene kanala na TV uređaju.

Što se tiče samog projektiranja mrežnih kapaciteta, oni moraju biti dovoljni da osiguravaju 0% gubitka paketa usljed zagušenja. To znači da kapacitet video veza mora biti dovoljan da u vršnim satima opterećenja može prenjeti promet, a bez da uzrokuje dodatna kašnjenja u isporuci paketa ili jitter. Kao što smo naveli i kod VoIP-a, ovo ne znači da se ne može imati

više pretplatnika (jer statistički gledano, neće baš svi istovremeno koristiti uslugu), ali u tom slučaju potrebno je koristiti mehanizme kontrole pristupa usluzi o kojima će biti više riječi u nastavku.

Video prijenos *(stream*) – Utjecaj nepravilnog redosljeda prijema paketa

Veliki broj krajnjih sustava za reprodukciju videa u realnom vremenu nema mogućnost preslagivanja paketa koji nisu stigli po redosljedu, pa to dovodi do gubitka paketa.

Video Konferencije

- uspostavljaju se koristeći SIP ili H.323 protokol.
- Bez obzira koja metoda se primjenjuje, uređaji međusobno dogovore koje kodeke će koristiti za sjednicu i sve ostale parametre.
- U tipičnom slučaju, rezerviraju se odvojeni kanali za glas i video i određuje se koje UDP portove će koristiti RTP protokol za trasport.
- SLA zahtjevi su slični onima potrebnim za VoIP uslugu koju smo već objasnili.
- Video formati za prijenos slike znatno su niže kvalitete od one koja se koristi za broadcast IPTV-a. Ovdje se uglavnom koriste kodeci MPEG2/H.262 ili MPEG-4 AVC/H.264 sa ograničenom širinom pojasa i sa 10 okvira u sekundi.
- Kod lošijih performansi mreže (kašnjenja), ovdje se mogu pojaviti razlike između zvuka i slike, tj. da zvuk i slika nisu sinhronizirani.
- Dozvoljena razlika u kašnjenjima između audio i video toka iznosi **80ms** i smatra se da je nezamjetna.

PREDAVANJE 4 - Propusno fokusirane TCP aplikacije

Da bi se shvatio utjecaj koje metrike poput mrežnog kašnjenja i gubitka paketa imaju na TCP [RFC 793] prvo moramo razumjeti osnovna načela rada TCP protokola. TCP ima za cilj osigurati pouzdan i učinkovit transportniprotokolni sloj na vrhu IP-a.

Četiri ključna mehanizma osiguravaju rad TCP protokola:

1. dvosmjerno uspostavljanje sjednice
2. pozitivnu potvrdu s retransmisijom
3. kliznu prozorsku potvrdu za kontrolu protoka između pošiljatelja i primatelja
4. Kontrolu zagušenja, za postupanje s gubicima koji se javljaju između pošiljatelja i primatelja.

Sljedeći odjeljci daju pregled tih mehanizama

Dvosmjerno uspostavljanje sjednice

TCP je spojno orijentirani transportni protokol, koji uspostavlja sjednice između dva krajnja TCP sustava prije nego što započne prijenos podataka. TCP uspostava sjednice oslanja se na "trostruko rukovanje" ("three-way handshake").Zamislite dva TCP krajnja sustava A i B, u kojoj je A inicijator TCP sjednice za B.

1. A prvo šalje TCP segment prema B sa sinkronizacijskim bitnim (SYN) skupom koji predstavlja prvi dio„trostrukog rukovanja“, a segment je TCP podatkovna jedinica prenesena u IP paketu.
2. Za nastavak uspostave TCP sjednice, B odgovara slanjem segmenta sa SYN i potvrdnim (ACK) bitovima natrag premaA.
3. Završni segment u rukovanju je još jedan ACK, koji je poslan od A do B kako bi potvrdili da je sjednica uspješno uspostavljena.

Tijekom uspostave sjednice, pregovara se o više parametara uključujući maksimalnu veličinu segmenta (MSS) i veličini prozora, o kojima će se raspravljati u sljedećim poglavljima, te hoće li se koristiti eksplicitna obavijest o zagušenju (*Explicit Congestion Notification*).

Pozitivna potvrda s retransmisijom

Kako bi se osigurao pouzdan i učinkovit prijenos podataka između TCP krajnjih sustava, čak i ako je osnovna mreža nepouzdana, TCP koristi tehniku poznatu kao "pozitivna potvrda s retransimisijom". Ta tehnika zahtijeva da primatelj šalje potvrdu (ACK) nazad pošiljatelju o primitku TCP segmenta. U najjednostavnijem mogućem modelu, pošiljatelj vodi evidenciju o svakom segmentu kojeg šalje i čeka ACK za prethodni segment prije slanja sljedećeg. Pošiljatelj također pokreće retransmisijski brojač kada šalje segment. Ako ACK nije primljen prije isteka vremena, pošiljatelj ponovno šalje već poslani segment, pod pretpostavkom da je prethodni izgubljen. TCP je dvosmjerni transportni protokol, što znači da jedna TCP sjednica može podržati prijenos podataka u oba smjera. Dakle, poruke potvrde prijama (ACK-ovi) iz jednog TCP krajnjeg sustava na drugi mogu sekombinirati sa segmentima podataka koji se šalju u suprotnom smjeru.

Uspostava kliznog prozora

TCP proširuje osnovni model „pozitivne potvrde s retransmisijom“ dodavanjem koncepta „potvrde kliznog prozora“ koji omogućuje pošiljatelju da šalje višestruke pakete prijemniku, prije čekanja na ACK poruku potvrde prijema. Shema „potvrde kliznog prozora“ koristi se odstrane TCP za kontrolu protoka, tj. podešavanje brzine prijenosa od pošiljatelja, tako da ne prelazi kapacitet prihvata podataka prijemnika.

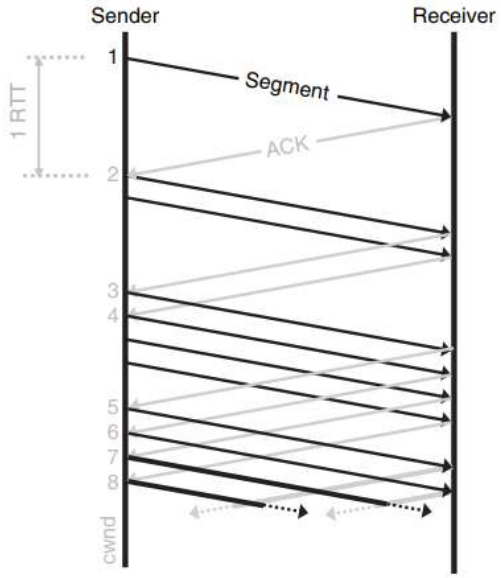
Svaki TCP krajnji sustav obznanjuje u TCP zaglavlju maksimalnu veličinu prozora (awnd) kojeg su spremni prihvatiti unutar iste sjednice. „Širina prozora“ ili broj od X paketa znači da pošiljatelj može imati do X nepotvrđenih segmenata. Ako je pošiljatelj primio ACK za segment Y, tada pošiljatelj može poslati do Y + X segmenta prije primitka ACK za segment Y + 1. Obzirom da možemo imati nekoliko paketa u prijenosu između pošiljatelja i primatelja s konceptom kliznog prozora, stoga kako bi pratili izgubljene i duplirane segmente TCP dodjeljuje redni broj za svaki segment. Ako je jedan (ili više) paketa u prijenosu odbačen ili resekvenciran, na dolasku u prijemniku će se pojaviti segment „van redosljeda“. To uzrokuje da prijemnik odmah generira ACK (duplikat ACK) za posljednji segment uspješno primljen u nizu.

Kontrola zagušenja

TCP također provodi kontrolu zagušenja, kako bi se izbjegao "kolaps zagušenja" mreže. Kontroliranjem TCP sjedniceomogućava se njeno prilagođenje trenutnim prometnim uvjetima na mreži, kako bi se pokušala povećati propusnost za svaku sjednicu. To također održava iravnopravan odnos između sjednica. Da bi se to postiglo, veličina prozora TCP nije statički određen, već se koristi niz dinamičkih tehnika [RFC 2581] za podešavanje veličine prozora. Glavne tehnike koje se koriste su: “spori start”, “izbjegavanje zagušenja”, “brza retransmisija” i “brzi oporavak”.

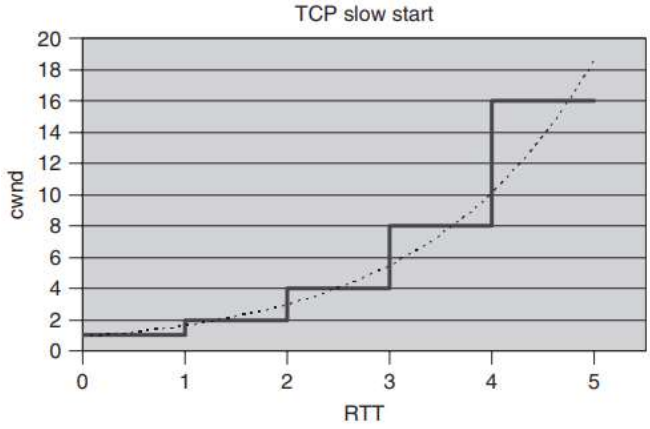
„Spori start“

Algoritam *sporog starta* ima za cilj kontrolirati brzinu kojom pošiljatelj odašilje segmente u mreži na početku sjednice kako bi se smanjila vjerojatnost da će sjednica poslati previše segmenata i doprinijeti zagušenju u mrežnim elementima na putu. Da bi se to postiglo, *sporistart* primjenjuje ograničenje veličine prozora kojeg nazivamo „prozor zagušenja“ (cwnd). Kada se uspostavlja nova sjednica, cwnd se postavlja na veličinu od samo jednog segmenta. Nakon svake primljene ACK poruke, cwnd se povećava za jedan segment.Pošiljatelj može poslati samo onoliko segmenata koliko je određeno trenutnimminimumom awnd i cwnd (tj. MIN [awnd, cwnd]), prije nego zaprimi slijedeću ACK potvrdu prijema. Na primjer, ako pošiljatelj u sporom startu sa cwnd postavljenom na jedan, pošalje jedan segment.Nakon primitka prve ACK potvrde, povećava cwnd na dva i šalje još dva segmenta. Kada mu stignu ACK potvrde o isporuci oba odaslana segmenta, cwnd je povećan na četiri kao što je prikazano na slici 1.



Slika 1: TCP "*spori start"*

Dakle, „*spori start"* daje eksponencijalni rast cwnd s RTT kao što je prikazano na slici 2



Slika 2: TCP "*spori start*" – eksponencijalni rast brzine

Razlog zašto se ovaj koncept zove „*spori start"* je zato što je spor u odnosu na originalne implementacije TCP koji nisu poznavale koncept cwnd i pokretale su slanje putem maksimalne veličine prozora na početku sjednice.

"Izbjegavanje zagušenja"

U nekom trenutku, kapacitet nekog mrežnog elementa na putu između pošiljatelja i primatelja može biti prekoračen, odnosno dolazi do zagušenja i kao posljedica paketi mogu biti odbačeni. TCP (bez podrške za ECN) tretira mrežu kao "crnu kutiju", u smislu da se ne oslanja na neko određeno ponašanje mreže pri svome obavljanju kontrole toka (kako bi se utvrdilo stanje dostupne propusnosti mreže i da li je došlo do zagušenja). TCP se isključivo oslanja na svoje mehanizme za implicitno određivanje izgubljenih paketa i to: TCP istekom vremena za potvrdu prijema (*TCP timeouts)* ili prijem duplikata ACK poruke. Kada se utvrdi gubitak paketa unutar sjednice, TCP reagira pozivajući se na sljedeći algoritam, koji koristi dodatnu varijablu koja se zove *prag sporog starta* (ssthresh):

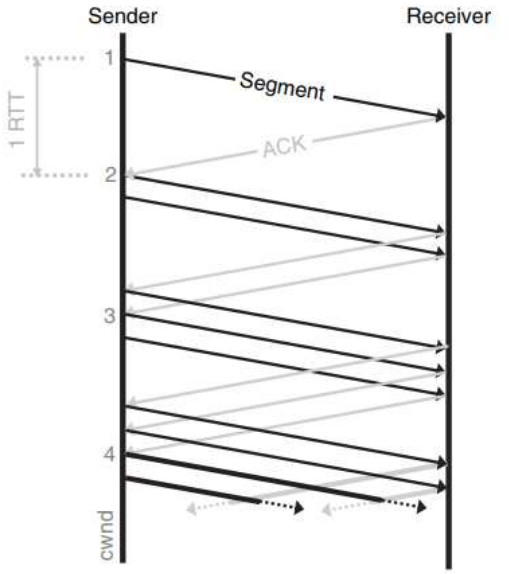
Ssthresh se postavlja na veću vrijednost od: ili 2 segmenata ili jedne polovice veličine prozora prije nego je došlo do zagušenja (npr MAX [2, MIN [awnd, cwnd]). Cwnd je zatim prepolovljen za svaki eventualni slijedeći gubitak, stoga ako se gubitak nastavlja, stopa prijenosa se smanjuje eksponencijalno.

Osim toga, ukoliko je zagušenje indicirano *TCP timeout-om (istekom vremena za potvrdu)*, cwnd se postavlja na jedan segment.

Kada se zaprimi slijedeća ACK poruka:

- Ako je cwnd manji ili jednak ssthresh-u, poziva se algoritam *spori start* kao što je gore opisano dok veličina prozora ne bude jednaka ssthresh, odnosno polovici veličine prozora u trenutku kada je došlo do zagušenja.
- Kad je cwnd veći od ssthresh-a, poziva se sljedeći algoritam za *izbjegavanje zagušenja*.

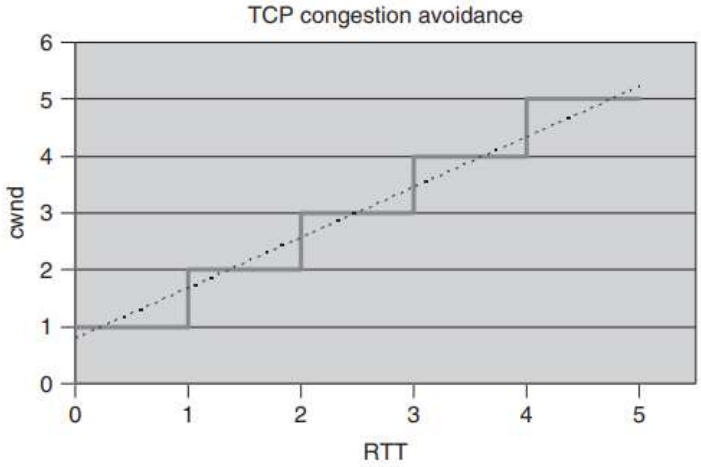
Algoritam izbjegavanja zagušenja definira da svaki put kada je ACK primljen, cwnd se povećava za veličinu segmenta /cwnd. Na primjer, ako pošiljatelj u sporom startu sa cwnd postavljenom na jedan, pošalje jedan segment, kada primi prvu ACK poruku povećava cwnd na dva i šalje još dva segmenta. Kada su sljedeća dva segmenta primljena, cwnd je povećan na tri, kao što je prikazano na slici 1.19.



Slika 3: TCP *izbjegavanje zagušenja*

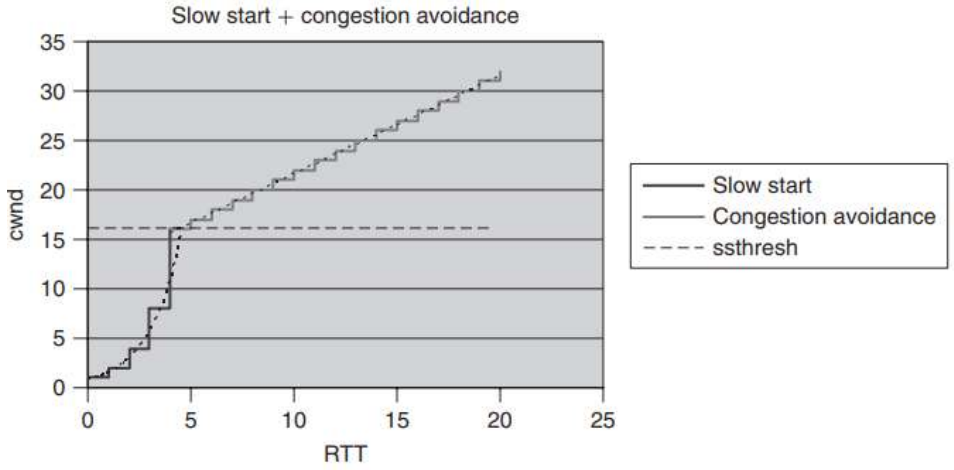
Povećanje cwnd je ograničeno na najviše jedan segment u svakom RTT bez obzira koliko je ACK primljeno u tom intervalu, dok spori start povećava cwnd za broj primljenih ACK unutar RTT. Stoga, algoritam *izbjegavanja zagušenja* daje linearni rast cwnd, u usporedbi s eksponencijalnim rastom sa algoritmom *spori start*.

Razmotrimo primjer prikazan na slici 1.21. U trenutku t = 0, uspostavljena TCP sjednica doživi istek vremena *(timeout*) kad je cwnd = 32 segmenata. Ssthresh je postavljen na 16 segmenata i cwnd se smanjuje na 1 segment. Cwnd se zatim povećava sa *sporim startom* dok se ne izjednači ssthresh. Zatim se poziva algoritam *izbjegavanje zagušenja*.

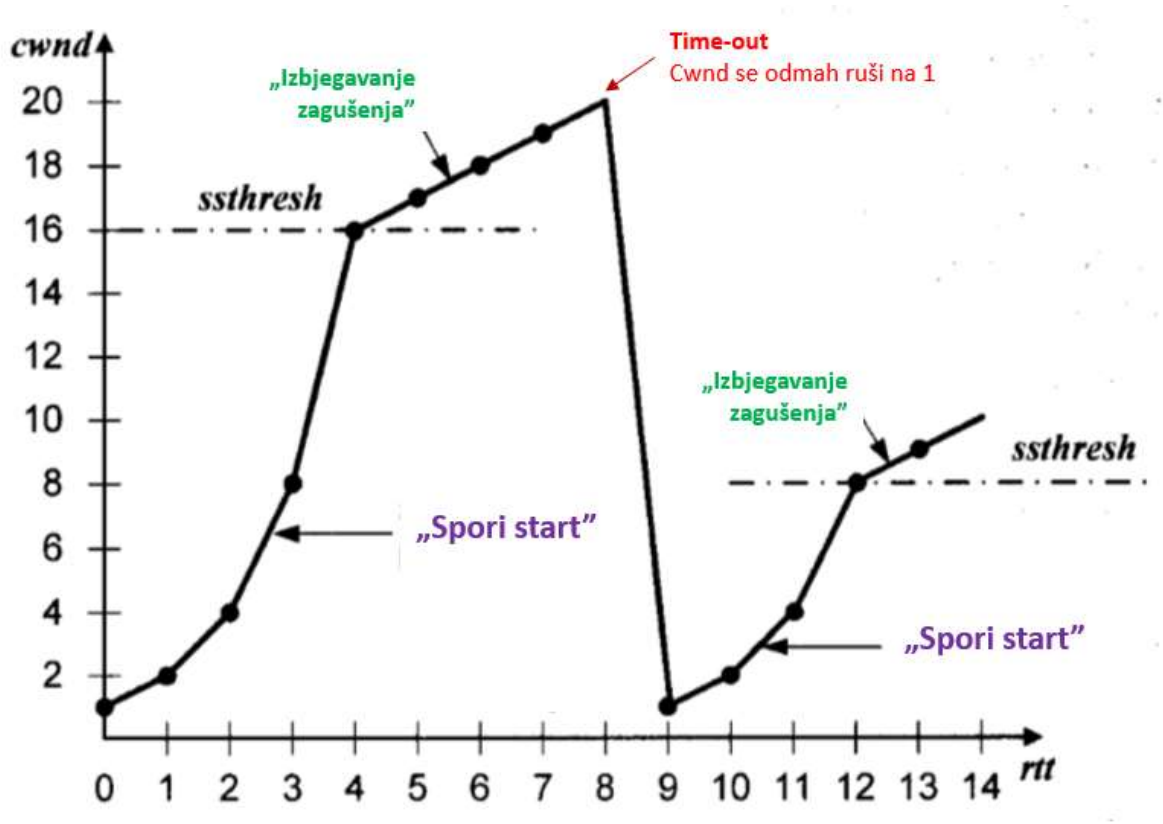


Slika 4: TCP izbjegavanje zagušenja

Kao što se može vidjeti na Slici 1.21, cwnd eksponencijalno raste sa RTT dok ne bude jednak ssthresh; Iznad ssthresh cwnd raste linearno s RTT.



Slika 5: Primjeri sporog starta i izbjegavanja zagušenja.



Slika 6: Tipičan izgled TCP prometne karakteristike – oblik „pile".

"*Brza retransmisija*"

Brza retransmisija je poboljšanje performansi prethodno opisanih mehanizama, koji određuje ponašanje pošiljatelja kada su primljeni dupli ACK-ovi. Kad pošiljatelj primi duple ACK, ne zna je li ACK uzrokovan izgubljenim segmentom ili segmentom sa rednim brojem izvan slijeda,pa stoga čeka da primi još mali broj dvostrukih ACK prije reakcije. Ako su dva ili manje dupla ACK-a primljena zaredom, pretpostavlja se da je došlo do primitka segmenata van slijeda. Ako su tri ili više dupla ACK-a primiljena, to se uzima kao znak da se segment izgubio i algoritam *brze retransmisije* definira da u ovom slučaju pošiljatelj treba ponovno poslati nedostajeći segment, bez čekanja isteka vremena ponovne transmisije (*TCP timeouts*).

"*Brzi oporavak*"

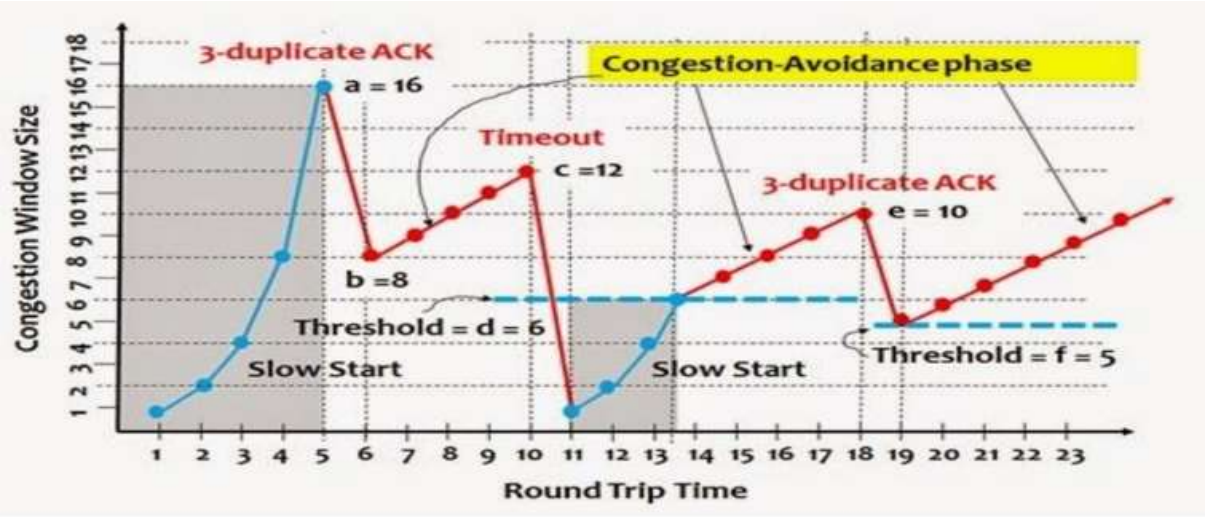
Brzi oporavak je dodatno poboljšanje performansi, što omogućuje veću propusnost pri umjerenim zagušenjima. Brzi oporavak definira da nakon što "*brza retransmisija*" ponovo pošalje nedostajeći segment, treba pristupiti algoritmu "*izbjegavanje zagušenja*" umjesto "*sporog starta*".

Podrška za razne tehnike kontrole zagušenja u TCP knjižnici je evoluirala tijekom vremena i tu je općenita sehma imenovanja koja potječe iz BSD (Berkeley UNIX) implementacije TCP knjižnice koja daje taksonomiju za evoluciju TCP knjižnice.

- 4.2BSD (1983) bio je prvo široko dostupno izdanje TCP/IP.
- Tahoe: 4.3BSD Tahoe izdanje (1988) uključuje spor start, izbjegavanje zagušenja i brzi ponovni prijenos.
- Reno: 4.3BSD Reno izdanje (1990) dodana podrška za brz oporavak.
- Vegas: Vegas TCP knjižnica (1994) dodana podrška za dodatne opreme opisanih u [BRAKMO], čiji je cilj poboljšati TCP propusnost u odnosu na prethodne knjižnice.
- NewReno: Nova Reno TCP knjižnica (1999) dodaje podršku za poboljšanja za algoritam brzog oporavka opisanog u [RFC 3782].

U novije vrijeme, [RFC 3390] određuje povećanje dopuštene gornje granice TCP početne veličine prozora od jednog ili dva segment(a) na između dva i četiri segmenta. Ova promjena smanjuje broj RTT-ova potrebne za dovršetak neke transakcije. Mnoge e-mail i web stranice transakcije su manje od 4 kilobajta, stoga će veći početni prozor smanjiti vrijeme prijenosa podataka da samo jednog RTT-a.

Postoje dodatne suptilnosti u implementacijama TCP - pogledajte [Stevens, RFC 2581] - No, detalji koje smo do sada naveli su dovoljni za razumijevanje učinaka koje mrežne značajke kao što su kašnjenje i gubitci imaju na TCP i koji se detaljno objašnjeni u sljedećim poglavljima



Slika 7: Tipičan izgled TCP prometne karakteristike uz "Brzi opravak".

TCP: Utjecaj kašnjenja

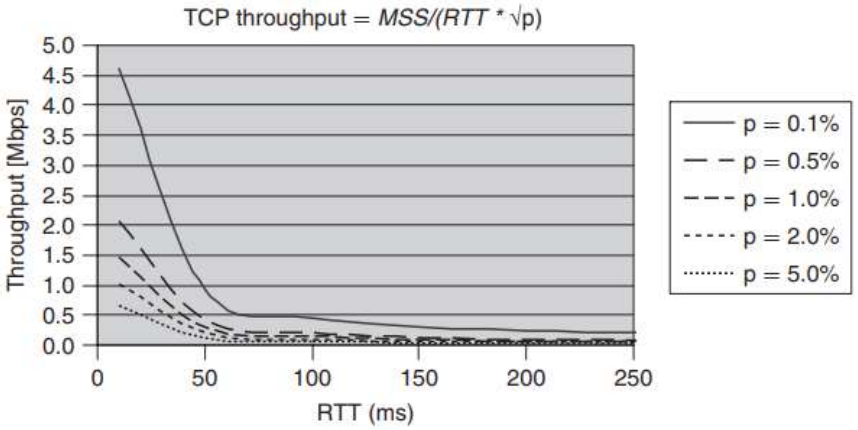
Za TCP, važna metrika je kašnjenje RTT između TCP krajnjih sustava. Maksimalan broj segmenata bez potvrde prijema (*unacknowledged*) koje TCP pošiljatelj može imati ograničena je veličinom prozora. Dakle, za određeni RTT između pošiljatelja i primatelja, maksimalno moguća TCP propusnost sjednice biti će određena veličinom prozora · MSS/RTT, gdje je MSS maksimalna veličina segmenta. To je količina podataka koja je poslana, ali još nije potvrđen njihov prijem, a obično se naziva TCP "veličina leta" (*flight size*) [RFC 2581] ili "veličina cijevi" (*pipesize*).

Dakle, TCP sesijska propusnost je obrnuto proporcionalna RTT.

[MATHIS] pokazuje da je maksimalna teoretska dostižna TCP propusnost za jednu sesiju varira u ovisnosti od RTT i gubitak paketa u tom odnosu gdje je p je vjerojatnost gubitka paketa:

$$TCP\_throughput = \frac{MSS}{RTT \times \sqrt{p}}$$

Graf na slici 1.22 koristi taj odnos da prikaže teoretski kako maksimalna TCP propusnost za jednu TCP sesiju varira u ovisnosti od RTT za TCP maksimalnu veličinu segmenta (MSS) od 1460 bajtova.



Slika 8: TCP propusnost kao funkcija RTT

Primjećeno je da će postignuta TCP propusnost u praksi ovisiti o nizu drugih čimbenika, koji se razlikuju od mreže do mreže uključujući:

- životni vijek TCP sesije. Dugotrajne sesije će imati više prilika da otvore svoje maksimalne veličine prozora nego kratkotrajne sjednice ako dođe do zagušenja:
- specifično ponašanje korištenih krajnjih sustava u prisutnosti zagušenja. Za TCP-temeljene aplikacije to ovisi o TCP knjižnici koja se koristi
- Ponašanje bilo kojeg routera u prisutnosti zagušenja, npr. odbacivanje kraja ili RED
- Osim toga, može se vidjeti na slici 6 da čak i ako postignuta propusnost je blizu teoretskog maksimuma, na niskim RTT-ovima i niskim vjerojatnostima gubitka paketa, propusnost sjednice je ograničena na nekoliko megabita u sekundi.

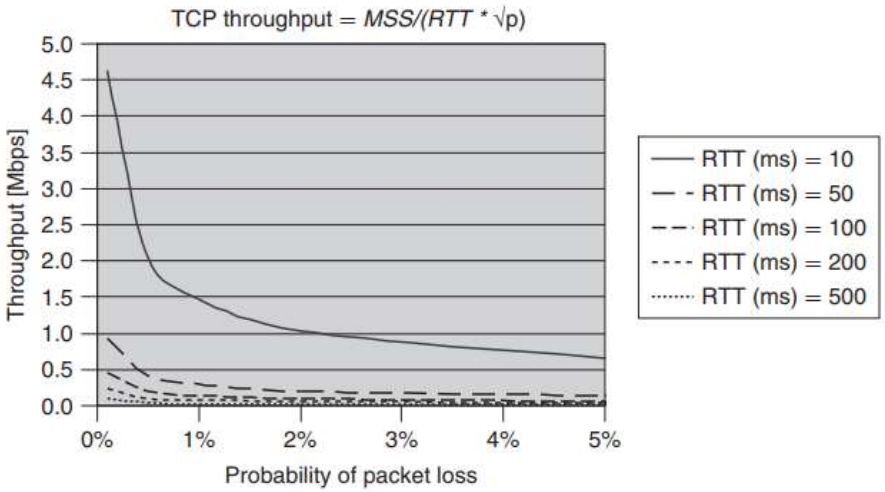
Za neke visoko propusno aplikacije te granice mogu biti pretjerano ograničavajuće;. Jedan takav zahtjev je „Grid računalstvo“ [BAKER] gdje su geografski distribuirani računalni resursi umreženi da djeluju kao jedinstveno računalo. Bilo je brojnih prokušaja (iako ni jedna opcijajoš uvijek nijeušla u širu uporabu) kako bi se unaprijedo TCP u smislu znatno većepropusnosti jedne sjednice. Dva takva koncepta su "Brzi TCP" [Cheng] i "TCP visoke brzine" [RFC 3649].

TCP: Utjecaj varijacije kašnjenja

Same varijacije kašnjenja nemaju značajan utjecaj na TCP. Jedini utjecaj na TCP očituje su u tome što su varijacije kašnjenja sastavni dio kašnjenja, a što pak može utjecati na propusnost kako je opisano u prošlom odjeljku.

TCP: Utjecaj gubitka

TCP ima mehanizme koji osiguravaju da se izgubljeni paketi ponovno šalju. Međutim, [MATHIS] pokazuje da se teoretski maksimum TCP propusnosti smanjuje kao inverzijakorijena vjerojatnosti gubitka paketa. Graf na slici 1.23 koristi tu povezanost da pokaže kako teoretski maksimalna postignuta TCP propusnost za jednu TCP sjednicu varira u ovisnosti o gubitku paketa za maksimalnu veličinu TCP segmenta (MSS) 1460 bajtova.



Slika 9: TCP propusnost kao funkcija gubitka paketa

Kao što je već navedeno, postoji niz faktora koji će utjecati na postignutu TCP propusnost u praksi.

TCP: Utjecaj propusnosti

U prethodnim poglavljima je opisano kako postignuta propusnost za TCP sjednicu ovisi o vjerojatnosti gubitka paketa i postignutom RTT, kao i nizu praktičnih čimbenika. Osim toga, postignuta propusnost za TCP sjednicu će očito biti ograničenai od strane raspoloživih kapaciteta na putu između izvora i odredišta.

Dakle, važno je napomenuti da stvarna postignuta TCP propusnost za jednu TCP sjednicu može biti znatno manja od ugovorene širine pojasa osigurane za uslugu.

TCP: Utjecaj paketa stiglih van redoslijeda

Većina korištenih TCP implementacija će podržati funkcionalnost*brze retransmisije*, a time će se interpretirati prijem tri uzastopna dvostruka ACK kao pokazatelj gubitka paketa i ponovno će poslati sljedeći paket te usporiti njihovu brzinu slanja pozivajući se na *algoritam izbjegavanja zaušenja*. Iz tih razloga paketi koji su pristigli van redosljeda unutar TCP prometa mogu imati značajan utjecaj na TCP propusnost.

[LAOR] pokazuje da je za TCP promet sa stopom od samo 0,04% paketa koji su pristigli van redosljeda, postignuta aplikacijska propusnost može se smanjiti do 74% u odnosu na propusnost postignutu bez grešaka u redosljedu paketa. Dakle, greške u redosljedu prijema paketa treba izbjegavati zbog mogućeg utjecaja na TCP propusnosti.

Interaktivne podatkovne aplikacije

Interaktivne aplikacije ovise o pružanju odgovora krajnjem korisniku u realnom vremenu. Kako se posebne implementacije interaktivnih podatkovnih aplikacija mogu razlikovati, također se razlikuje i utjecaj koji mrežne karakteristike kao što su kašnjenje imaju na njih. Dakle nije moguće dati definitivne smjernice, već je potrebno razmotriti glavne čimbenike koji utječu na SLA zahtjeve u potpori interaktivnim podatkovnim aplikacijama.

Ciljano vrijeme odziva za takve interaktivne aplikacije ovisno je o ljudskim faktorima; [DOHERTY] pokazuje ekonomsku vrijednost brzih vremena odgovora na interaktivne aplikacije. Robert B. Millerov rad iz 1968. na "vijeme odziva u komunikaciji čovjek-računalo" opisao je tri vremenska praga odziva za ljudsku pozornost, [1] kojih su dva još uvijek opće prihvaćena i danas:

- Vrijeme odziva od manje od približno 0,1 sekunde je cilj koji aplikacije moraju ispuniti ukoliko želimo korisniku pružiti osjećaj da sustav reagira trenutno.
- Vrijeme odziva lošije od oko 1 sekunde je cilj ukoliko želimo omogućiti da je korisnikov tok misli neprekinut iako će on uočiti kašnjenje.
- Vrijeme odziva od manje od 10 sekundi je ciljano vrijeme ukoliko programi moraju zadržati pažnju korisnika na dijalog. Za veće kašnjenje korisnici će željeti obavljati druge poslove, dok čekaju računalo da završi.
- Ovo vrijeme odziva aplikacija također potvrđujei rad Petera Bickforda iz 1997. godine [Bickford], čije je istraživanje pokazalo da pola korisnika napušta web stranice nakon čekanja od 8,5 sekundi. "Pravilo od 8 sekundi" je naknadno postala univerzalno pravilo web dizajna.

Ti vremenski ciljevi odnose se na vrijeme za dovršavanje korisničke transakcije - to je vrijeme između zahtjeva korisnika i primitka odgovora na njihove zahtjeve. Za klijent/poslužitelj aplikacije koje zahtijevaju mrežne transakcije, kašnjenje mreže je samo jedan aspekt ukupnih transakcijskih kašnjenja na koje ovi ciljevi odnose, a koji se mogu sastojati od sljedećih komponenti:

- **Kašnjenje procesa klijenta.**

  Korisnički sustav može obavljati neke predprocese prije početka mrežne transakcije, a može obavljati dodatne procese na dobivanju odgovora od poslužitelja.

- **Kašnjenje procesa poslužitelja**

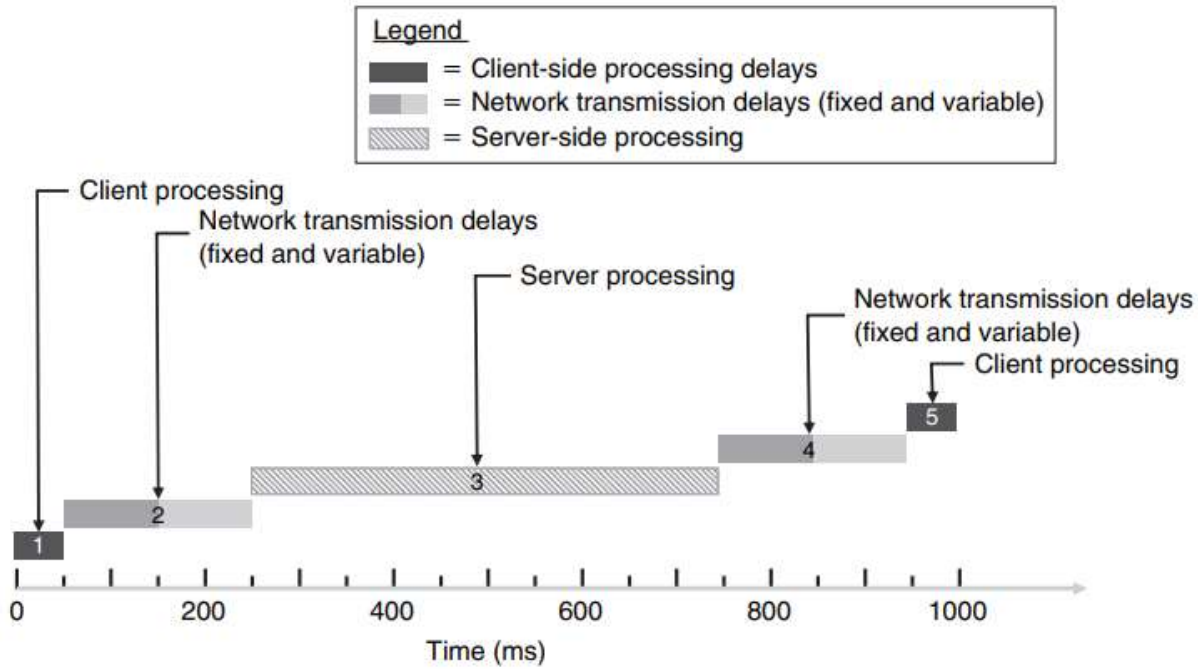
  Poslužitelj će morati obaviti neke procese prije nego što odgovor može biti poslan korisniku. Neke aplikacije mogu uključivati veći broj poslužiteljskih transakcija kao dio procesa pokrenutih od strane korisnika.

- **Kašnjenja mreže**

  Kašnjenje mreža će nastati pri slanju zahtjeva od klijenta do poslužitelja i slanju odgovora od poslužitelja do klijenta. Nadalje neke "pričljive" aplikacije mogu zahtijevati nekoliko mrežnih transakcija između klijenta i poslužitelja za transakciju samo jednog zahtjeva korisnika. Za takve aplikacije, i relativno malo povećanje mrežnog kašnjenja može imati primjetan učinak na vrijeme odziva krajnjem korisniku, odnosno može biti zahtjevana vrlo malo mrežno kašnjenje kako bi se postiglo ciljano vrijeme odgovora aplikacije.

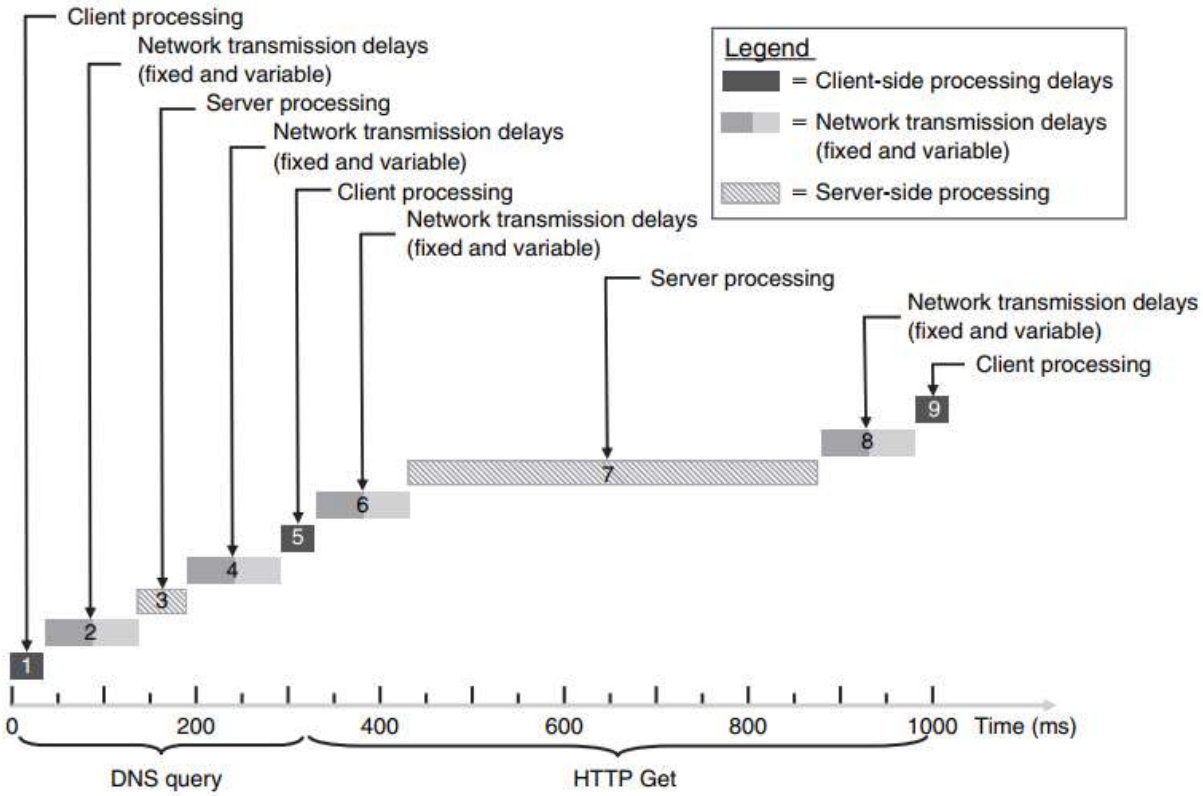
Dakle, za aplikaciju koja cilja vrijeme odziva od 1 sekunde, čak i ukoliko je mrežni RTT daleko ispod sekunde, vrijeme odziva korisnika može i dalje biti veće od jedne sekunde. To znači da je potrebno jako dobro razumijevanje specifičnih ponašanja aplikacija kako bi se shvatilo kakav utjecaj različita mrežna kašnjenja imaju na aplikaciju i da bi mogli preslikaticiljana vrijemena odziva aplikacija u odgovarajuće mrežne RTT zahtjeve.

Pretpostavimo, kao što je prikazano na slici 10, da poslovno-kritična interaktivna aplikacija s ciljanim odzivom u roku 1 sekunde, koristi jednu mrežnu transakciju (npr HTTP GET) po zahtjevu korisnika, koristeći minimalni transportnu jedinicu za zahtjev (veličine jednog paketa) s ukupno 100 ms procesuiranja od strane klijenta (akcija 1 + 5) i 500 ms ukupnog procesuiranja od strane poslužitelja (akcija 3). Kako bi zadovoljili ciljani vremenski odziv zahtijeva se mrežni RTT od oko 400 ms (Akcije 2 + 4) ili manje.



Slika 10: Komponente kašnjenja: primjer interaktivna podatkovnih aplikacija 1

Na primjeru prikazanom na slici 11 imamo aplikaciju s istim ukupnim klijentskim i poslužiteljskim procesnim kašnjenjem, ali koja traži dvije mrežne transakcije (DNS upita i HTTP GET na primjer) po korisničkom zahtjevu. Kako bi zadovoljili ciljano vrijeme odziva aplikacije sada će nam biti potrebna mreža sa RTT od oko 200 ms ili manje.



Slika 11: Komponente kašnjenja: primjer interaktivna podatkovnih aplikacija 2

Loše osmišljena implementacija aplikacija može nametnuti neostvarive RTT uvjete na mreži.U ovom slučaju treba uzeti u obzir ponovno modificiranje aplikacije. Primjena redizajniranja može zahtijevati ponovno pisanje aplikacije kako bi se smanjio broj mrežnih transakcija ili preseljenja poslužitelja bliže klijentu, čime se smanjuje mrežna udaljenost, a samim time i RTT .

Varijacija kašnjenja (*Jitter*) nema eksplicitan utjecaj na interaktivne podatkovne aplikacije; već samo ima utjecaj na TCP po tome što je i *jitter* dio ukupnog mrežnog kašnjenja. Mrežni gubitak paketa i paketi primljeni van slijed mogu imati utjecaj kod interaktivnih podatkovnih aplikacija podataka kod kojih će to povećati vjerojatnost ukupnog mrežnog kašnjenja. Utjecaj gubitka paketa i resekvencioniranja ovisit će o karakteristikama transportnog protokolnog sloja koji se koristi.

Utjecaj gubitka paketa i resekvencioniranja na TCP je već objašnjen, a za UDP bazirane interaktivne podatkovne aplikacije potrebno je detaljno poznavanje svake specifične primjene aplikacije kako bi razumjeli utjecaj gubitka paketa i resekvencioniranja. To bi zahtijevalo analizu svake pojedine aplikacije ponaosob.

On-line igranje

Igranje na vezi s više igrača ili umrežena igra su najpopularniji tip aplikacija poznatih kao **umrežena virtualna okruženja** (*Networked Virtual Environments*-NVEs). Drugi koristi od NVEs su vojne simulacije. Korisnici u NVEs, koji mogu biti na geografski odvojenim mjestima, u interakciji su jedni s drugima u virtualnom svijetu u realnom vremenu.IEEE Podijeljeni Interaktivni Simulacijski (*Distributed Interactive Simulation*-DIS) [IEEE1278]

standard pokriva NVE. Njega obično ne razvijaju proizvođači igara već se koriste nečije tuđe već gotove mrežne implementacije. Zbog varijacija u takvim implementacijama nije moguće dati definitivne smjernice o SLA zahtjevima za podršku on-line igara,već ćemo pregledati trenutna istraživanja na ovu temu.

Iako postoje različite vrste on-line igara u realnom vremenu - najčešće vrste igre su: Pucač u prvom licu (*First Person Shooter*-FPS), Strategija u stvarnom vremenu (*Real-Time Strategy*-RTS) i igranje višestrukih uloga s više igrača na vezi (*Multiplayer On-line Role-Playing Game*-MORPG) . Većina koriste klijent-server arhitekturu, gdje centralni server prati stanje klijenta i stoga je odgovoran za održavanje stanja virtualnog okruženja. Računala igrača su klijenti, koji jednosmerno(*unicast*) odašilju lokacijske i akcijske informacije poslužitelju, koji potom distribuira podatke ostalim klijentima koji sudjeluju u igri. Većina implementacija koristi UDP kao transportni protokol.

Većina implementacija on-line igara su se razvile za rad preko javnog Interneta i imaju zahtjeve propusnosti manje od 64 kb/s i ugrađene mehanizme za rješavanje gubitka paketa. Međutim, primjećeno je da se ti zahtjevi propusnosti mogu povećati tijekom vremena, s učestalošću veće propusnosti dostupne krajnjim korisnicima zbog širokopojasnog pristupa. Osim toga, neke igre nude mogućnost za podešavanje raznih parametara mreže, koji mogu imati značajan utjecaj na njihove zahtjeve za propusnosti.

Obično se navodi da je nisko mrežno kašnjenje neophodan zahtjev za on-line igranje. Igrači koji osjete veće zastoje poslužitelja od drugih igrača, mogu doživjeti relativno "zaostajanje" u igri jer dobivaju informacije od poslužitelja kasnije od korisnika sa manjim kašnjenjem. Slijedom toga, korisnici s nižim RTT imaju prednost pri igranju.

U pogledu postavljanja granica na prihvatljivoj RTT za on-line igranje, istraživanje FPS igara sugerira da s kašnjenjem iznad 100-250 ms, igrači su odvraćeni od igranja i/ili je njihovo igranje blokirano [HENDERSON1, Armitage, Pantel] iako različite vrste igara mogu imati različite zahtjeve. Ovi rezultati su potvrđeni prema istraživanju u različitim područjima s ciljem utvrđivanja kašnjenja iznad kojeg performanse za interaktivne aplikacije gube vrijednost [G.114, Bailey, MacKenzie].

Novije istraživanje [HENDERSON2] je ispitalo utjecaj koje kašnjenje ima na ponašanje korisnika, (ne na utjecaj na samo igranje), zaključivši da visoko kašnjenje mreže može odvratiti korisnika na pridruživanje određenoj igri. Međutim, nakon što se igrač pridružio poslužitelju za igru, čak i kada su igrači mogli primijetiti kašnjenje i njihovo igranje je bilo degradirano, nezadovoljstvo nijedošlo do te mjere da bi oni napustiti poslužitelj.

To može značiti da su igrači spremni tolerirati višu razinu kašnjenja nego što su prethodna istraživanja pokazala. Osim toga, brojne tehnike za kompenzaciju kašnjenja su se pokazale uspješnim. [Bernier].

Istraživanje RTS igara [SHELDEN] sugerira da RTT-ovi do 500 ms imaju minimalan utjecaj na krajnje korisnike; iako su viša kašnjenja vidljiva korisniku, imala su zanemariv utjecaj na ishod igre. To se pripisuje prirodi RTS igranja koja je usmjerena više na strategiju, nego aspektima stvarnog vremena.

PREDAVANJE 5 - Uvod u QoS mehaniku i arhitekture I

Što je kvaliteta usluge?

U umrežavanju, pojam kvaliteta usluge (QoS) može značiti različite stvari različitim ljudima, stoga je ključno započeti ovo poglavlje definiranjem što QoS znači u kontekstu ove knjige.

Prvo, kako definiramo "uslugu" u kontekstu IP umrežavanja? „Uslugu" shvaćamo kao opis cjelokupne obrade prometa kupca kroz određenu domenu. Usluga je praksi korisna samo ako zadovoljava zahtjeve aplikacija krajnjeg korisnika koje treba podržavati. Dakle, cilj usluge je povećati zadovoljstvo krajnjeg korisnika pomoću aplikacija koje usluga podržava, tj. da aplikacije krajnjeg korisnika rade učinkovito.

Kako onda definiramo "kvalitetu" u kontekstu određene IP usluge? Kvalitetu usluge možemo definirati u smislu temeljnih zahtjeva za aplikaciju koji se mogu definirati u smislu SLA metrike za IP performanse prijenosa: kašnjenje,varijacije kašnjenja, gubitak paketa, propusnost, dostupnost usluge i očuvanje sekvence po protoku.

QoS, međutim, podrazumijeva više nego samo garanciju da je mrežna usluga u mogućnosti podržati SLA zahtjeve aplikacije koju cilja podržati. Problem garancije da mreža može zadovoljiti ove zahtjeve je u osnovi problem upravljanja dostupnog kapaciteta mreže u odnosu na usluge opterećenja, na primjer problem upravljanja preopterećenjima (zagušenjima). Ako je moguće osigurati da će uvijek biti znatno više dostupnog kapaciteta nego što je prometno opterećenje, i kašnjenje, podrhtavanje faze signala i gubitak će biti minimalizirani, propusnost maksimalna, a zahtjevi usluge će se lako ispuniti. U praksi, međutim, garancija da je mreža uvijek preopterećena u odnosu na stvarno prometno opterećenje nije uvijek isplativa.

Dakle, u sastavljanju QoS mrežne usluge važno je jedno ograničenje – smanjenje troškova. Ako je prometno opterećenje veće od sposobnosti podrške, npr. ako se dogodi preopterećenje, neki će promet trebati biti ili zadržan (kašnjenje) dok se kapacitet ne oslobodi ili će se morati odbaciti. Minimiziranje troškova može zahtijevati da je više usluga podržano ili multipleksirano na istoj mreži i to klasifikacijom prometa u određene grupe (klase), kako bi problem upravljanja prometnim opterećenjem u odnosu na dostupni kapacitet mogao biti izveden na bazi pojedine klase omogućujući diferencijaciju usluga po klasama.

Ukratko, na visokoj razini, QoS možemo opisati u smislu ciljeva koje pokušava postići, koji učinkovito definiraju optimizacijski problem 1, pokušaj povećanja zadovoljstva krajnjeg korisnika (korisnost ili učinkovitost) i istodobno smanjenje troškova. Maksimiziranje zadovoljstva korisnika zahtjeva da aplikacije krajnjeg korisnika rade učinkovito, na primjer, da je kavliteta razgovora duž IP poziva prihvatljiva, što zahtjeva da su aplikacijski SLA uvjeti zadovoljeni. Minimiziranje troškova zahtijeva da mi previše ne kompliciramo mrežu kako bi postigli tu kvalitetu poziva, što može izazvati potrebu za višestrukom diferencijacijom razine usluge koju nude različite aplikacije.

Kvaliteta usluge nasuprot klase usluga ili vrsta usluge

Pojmovi „klasa usluge“ (*Class of Service – COS*) i „Vrsta usluge“ (*Type of Service" -TOS*) ponekad se koriste naizmjenično sa kvalitetom usluge; za potrebe ove knjige mi ćemo ih izričito definirati da bi izbjegli nejasnoće:

Klasa usluge (CoS)

Kao što se naizmjenično koriste sa pojmom kvaliteta usluge, klasa usluge se također ponekad koristi za opis QoS mogućnosti drugog sloja koje pruža Ethernet ili ATM. Mi radije izbjegavamo te definicije i koristimo „klasu usluge“ ili CoS isključivo u kontekstu klasifikacije prometa kao skup prometnih tokova koji će imati zajedničke tretman prilikom transporta kroz mrežu. Stoga, da bi izbjegli zbrku, koristit ćemo pojam „klasa usluge“ kada se budemo referirali na klasifikaciju skupnih prometnih tokova u broju sastavnih klasa gdje će različite aktivnosti biti primijenjene na svaku pojedinu „klasu usluge“.

Vrsta usluge (ToS)

Mi ćemo koristiti pojam „vrste usluge“ izričito za korištenje Type of Service Octet-a u Ipv4 uvodnom dijelu paketa.

Usluga „najboljeg mogućeg“ *(„best-effort“)*

Mreže projektirane da dostave određenu kvalitetu usluge su često u ograničene sa mrežama „najboljeg mogućeg“. „Najbolji mogući“ opisuje uslugu mreže koja pokušava dostaviti promet na svoje odredište, ali koja za to ne daje nikakvu garanciju isporuke i time nema nikakve obaveze ispunjenja uvjeta za kašnjenje paketa, varijacije kašnjenja, gubitak i propusnost.

Pojam „najboljega mogućeg“ se često i zloupotrebljava. Gdje imamo mreže koje podržavaju višestruke klase usluga istovremeno, izraz „najboljeg mogućeg“ se često koristi za uslugu koja nudi najniže SLA obaveze. Po definiciji, izraz „najbolje moguće“ definira da nema nikakvih SLA obaveza pa stoga usluga koja garantira bilo koju SLA obavezu ne može biti definirana kao usluga „najboljeg mogućeg“, koliko god niske te garancije bile. Čak i ako mreža podržava samo jednu klasu usluge, na primjer, kada je prosljeđivanje paketa ravnopravno i kada svi paketi primaju istu kvalitetu usluge, ako ta usluga pruža definirane SLA obaveze, mi tvrdimo da se to ne može smatrati „najbolje mogućom“ uslugom mreže.Zbrka je također ponekad uzrokovana zato što sam IP može biti opisan kao „najbolji mogući“ protokol mrežne razine, u smislu da ne pruža nikakve mogućnosti za otkrivanje ili ponovno prenošenje izgubljenih paketa.

Isto tako, TCP se ponekad smatra kao protokol zajamčenog prijenosa zbog toga što pruža mogućnost otkrivanja i ponovnog prenošenja izgubljenih paketa. Ta mogućnost, međutim, može biti od nikakve praktične primjene ako temeljna IP usluga ne može isporučiti TCP segmente koje zahtijeva SLA aplikacija; učinkovitost SLA TCP usluge je ograničen SLA obavezama koje pruža osnovna IP usluga.

Kako bi se izbjegla bilo kakva mogućnost za zabunu, namjerno izbjegavamo pojam „najbolji mogući“.

Vremenski okviri koji su važni za QoS

Smatramo da je važno uzeti u obzir tri vremenska okvira koja su bitna za upravljanje kvalitetom usluge mreže; različite QoS tehnike su primjenjene za svaki vremenski okvir:

milisekunde

Prvi vremenski okvir koji ćemo razmatrati je reda milisekunda. Unutar tog vremenskog reda veličine, naleti pojedinih prometnih tokova ili skupni nalet različitih tokova u točkama agregacije mreže, mogu izazvati zagušenja na mjestima gdje prometno opterećenje premašuje raspoloživi kapacitet. Mehanizmi QoS-a važni za ovu vremensku skalu uključuju primjenu tehnika na svakom mrežnom čvoru zasebno poput „čekanja u redovima“ (*queuing*), organiziranja propuštanja prometa i odbacivanja paketa, a sve u svrhu da bi se pružila diferencijacija i izolacija različitih tipova prometa, kako bi se neke vrste prometa u odnosu na druge dobile prednost i kako bismo na taj način upravljali kašnjenjem te osigurali pravednu raspodjelu propusnosti.

100 milisekunda

Sljedeći vremenski okvir koji razmatramo je reda veličine stotine milisekunda. Ovo je vremenski okvir koji definira mrežna vremena obilaska (round trip times (RTT)). Ovaj vremenski okvir je važan za aplikacije koje koriste „vezu zatvorene petlje“ (*closed-loop feedback*) između pošiljatelja i primatelja da bi primijenili mehanizme kontrole toka, kao na primjer aplikacije bazirane na TCP-u. Mehanizmi QOS-a važni za ovaj vremenski okvir tako uključuju AQM tehnike kontrole zagušenja kao na primjer „nasumično rano otkrivanje“ (*random early detection-RED*).

10 sekundi ili više

Vremenski okviri reda veličina sekunda i minuta važni su za upravljanje dugoročnim mrežnim prosječnim prometnim razinama i kapacitetom, što je postignuto kroz planiranja kapaciteta i prometnog inženjerstva o kojem se raspravlja u posebnom poglavlju.

Prometni profil i praskovitost

Prometni profil (*traffic profile*) - određen je prirodom aplikacije, a opisuje se pomoću vršnog i/ili prosječnog protoka i vršne i/ili prosječne „praskovitosti" ulaznog prometa.

Praskovitost prometa (*traffic burst*) predstavlja količinu prometa koju mreža može prihvatiti u definiranom intervalu vremena, a izražava se u bajtovima.

Ovaj parametar je mjera varijabilnosti intenziteta ulaznog prometa.

Vrste prometnih izvora

A) izvor stalne podatkovne brzine (CBR)

   npr. govor kodiran PCM-om

B) izvori promjenjive podatkovne brzine (VBR)

   npr. video kodiran MPEG-om

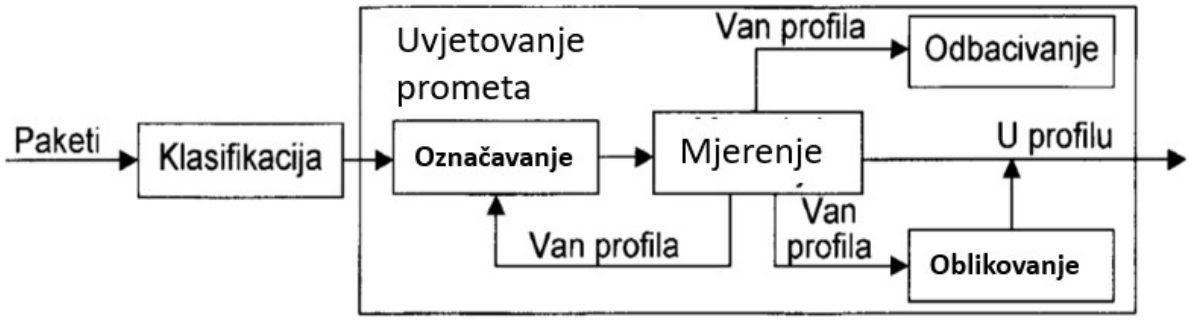
<u>Prometna politika</u> - je jedinstvena regulacija pristupa mrežnim resursima i uslugama na temelju postavljenih administrativnih kriterija.

- Cilj operatera je pružiti garantirani QoS određenim klasama prometa, te tu uslugu naplatiti korisnicima.
- Svaki operater određuje svoju „prometnu politiku" koja određuje parametre klasifikacije i tretman klasa
- Na ulazu u mrežu operatera prvo se vrši klasifikacija paketa (*packet classification*)
- Nekontrolirani ulaz prometa u jezgrenu mrežu mogao bi izazvati zagušenja na mrežnim čvorovima, a time i cijeli niz drugih povezanih problema koji bi narušili QoS garancije koje operater prodaje.
- Kako bi zaštitili svoju jezgrenu mrežu, operateri uvode uvjetovanje tj. regulaciju ulaznog prometa – *Traffic policing*, kako bi osigurali da je ulazni promet u skladu sa njihovim pravilima tj. politikom

Uvjetovanje prometa - može obuhvaćati operacije nadgledanja usuglašenosti prometa sa ugovorenim prometnim profilom (*policing*) , označavanja paketa, oblikovanja i odbacivanja.

U arhitekturi IntServ, mehanizmi kao što su nadgledanje pravila i oblikovanje prometa izvršavaju se u svakom RSVP usmjerivaču.

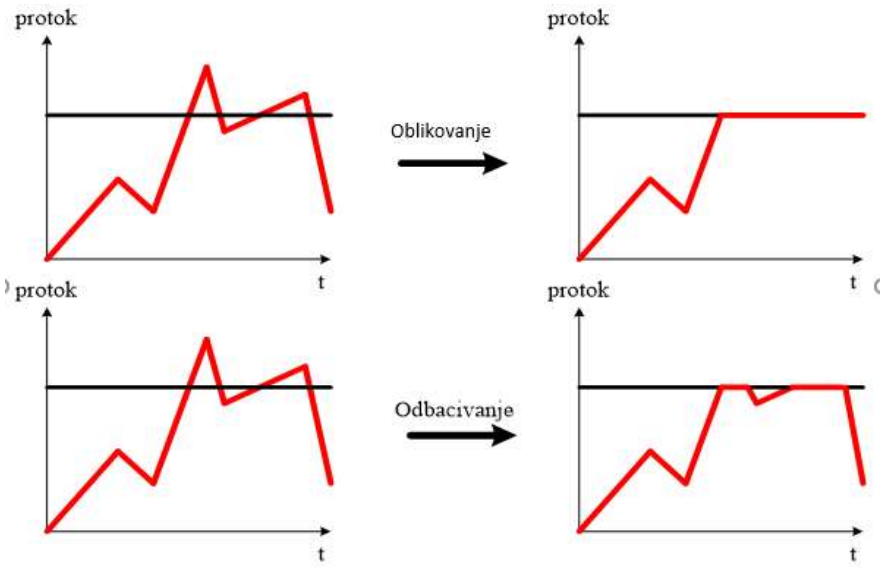
U arhitekturi DiffServ, uvjetovanje prometa obavlja se samo u ulaznom usmjerivaču , kao što je prikazano na slici



Funkcija mjerenja prati prometne parametre korisničkog toka i detektira pakete koji narušavaju dogovorene prometne parametre.

Informacija o paketima koji narušavaju dogovor se prosljeđuje funkcijama obilježavanja, oblikovanja i odbacivanja, a ove potom vrše odgovarajuće akcije na tim paketima u zavisnosti od konkretne implementacije tih funkcija.

Funkcija odbacivanja odbacuje svaki paket koji naruši dogovor, dok funkcija oblikovanja implementira spremnik (*buffer*) kojim se mogu zakasniti paketi koji narušavaju prometne parametre tako da njihovo zakašnjeno slanje bude u skladu sa dogovorenim prometnim parametrima. Očigledno, funkcija uobličavanja unosi dodatno kašnjenje u korisnički tok.



Zašto IP QoS?

Glavni razlozi za korištenje IP QoS-a proizlaze iz činjenice da je IP sloj mrežna tehnologija „s-kraja-na-kraj“ koja se danas koristi u većini aplikacija – **a mi pružamo QoS APLIKACIJAMA!!!!**

Tehnologije drugoga sloja, poput ATM-a i Etherneta imaju svoje određene QoS mogućnosti, stoga se nameće pitanje: „Zašto koristiti IP QOS a ne QOS mehanizme drugog sloja?“. Glavni razlozi za korištenje IP QOS-a proizlaze iz činjenice da je IP sloj mrežna tehnologija „s-kraja-na-kraj“ koja se danas koristi u većini aplikacija.

Da tome dodamo, QoS je disciplina s-kraja-na-kraj u kojoj je usluga koju pojedina grupa prometa prima ograničena elementom koji na putu s-kraja-na-kraj pruža najgoru uslugu.

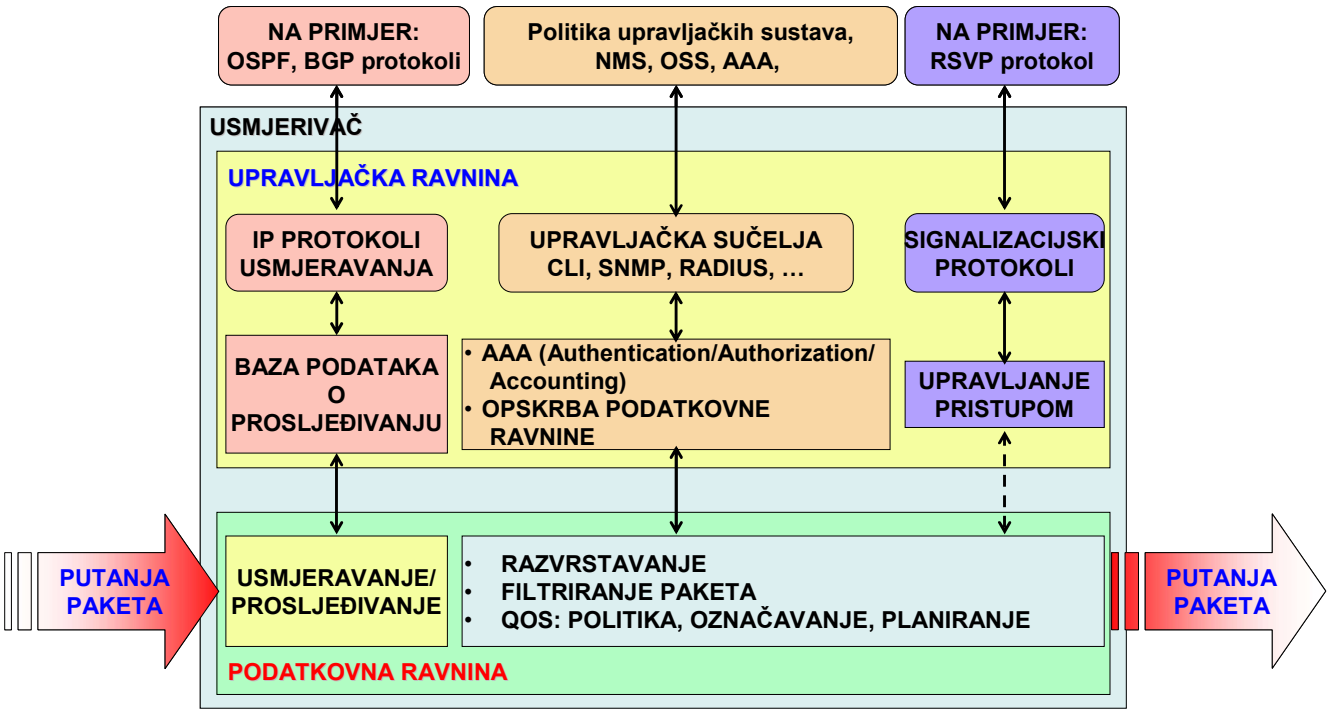
Dakle, kako bi se osiguralo smanjeno kašnjenje i gubitak usluge (i tako povećalo zadovoljstvo korisnika), mreža mora biti projektirana da ukloni sve točke preopterećenosti na putanji s-kraja-na-kraj za tu uslugu. Kako bi osigurali različite SLA-ove za različite grupe prometa (i time smanjili troškove), moramo primijeniti diferencijaciju na svim točkama preopterećenosti.

Različite tehnologije na razini drugog sloja mogu se koristiti za različite dionice putanje s-kraja-na-kraj razine 3. Stoga, kako je IP najniža zajednička razina s-kraja-na-kraj, temeljni smisao je da se IP QOS tehnike koriste gdje god je moguće te ih preslikati u temeljnim QOS mogućnostima u nižim razinama, gdje je to potrebno, radije nego pokušavati preslikati QOS mogućnosti razine 2 jedne dionice na QOS mogućnosti razine 2 sljedeće dionice.

SLA-ovi su osigurani na IP razini, međutim, implicitno su ograničeni SLA-ovima od temeljne tehnologije razine 2.

QOS skup alata

U praktičnom smislu, QoS uključuje korištenje niza funkcija i značajki (npr. razvrstavanje, raspoređivanje, politiku, oblikovanje), u kontekstu opće arhitekture (npr. Integrated Service, Differentiated Services) kako bi se osiguralo da mrežne usluge isporučuju ciljane SLA karakteristike kako bi aplikacije mogle učinkovito raditi. Mehanizmi koji se koriste za inženjering i QoS u mreži mogu se podijeliti na mehanizme u podatkovnoj ravnini i mehanizme upravljačke ravnine, a koji se primijenjuju na mrežne uređaje kao što su usmjerivači, kako je to prikazano na slici.



QoS funkcije podatkovne i upravljačke (kontrolne) ravnine

Podatkovna ravnina.

QoS mehanizmi podatkovne ravnine primjenjuju se u čvorištima mreže gdje se može izravno utjecati na ponašanje prosljeđivanja paketa. To su funkcije intenzivne obrade u visokoučinkovitim usmjerivačima. Obično se te funkcije primjenjuju u hardveru, zajedno s drugim funkcijama podatkovne ravnine kao što je podrška prosljeđivanja paketa i filtriranje paketa.

- Klasifikacija.

  Razvrstavanje tj. klasifikacija je proces razvrstavanja ukupnoga prometnog toka u brojne sastavne razrede - klase, tako da se bilo koja od sljedećih radnji kasnije može primijeniti na svaku pojedini paket koji pripada određenoj klasi usluge (*Class of Service*).

- Označavanje (*Marking*)

  Prometno označavanje (vidi odjeljak 2.2.2) je proces postavljanja izričitih vrijednosti polja u zaglavlju IP paketa koja su namjenjena QoS klasifikacijama u IP ili MPLS zaglavljima paketa, tako da se promet naknadno može lako identificirati.

- Maksimalna brzina izvršenja

  Politika i oblikovanje, mogu se iskoristiti za određivanje maksimalne brzine nekog prometnoga razreda.

- Prioritizacija

  Tehnike poput rasporeda prioriteta koriste se za određivanje prioriteta jedne vrste prometa u odnosu na druge i time upravljaju kašnjenjem i varijacijama kašnjenja.

- Osiguranje minimalne brzine

  Tehnike planiranja kao što su ponderirani ravnopravan red čekanja (*Weighted Fair Queuing - WFQ*) i deficitno kružno ponavljanje (*Deficit Round-Robin-DRR*) mogu se koristiti za različite prometne razrede s različitim minimalnim jamstvom propusnosti.

Upravljačka ravnina

QoS mehanizmi upravljačke i signalizacijske ravnine obično se bave s nadzorom pristupa i rezervacijom prometnih resursa, te se u nekim slučajevima mogu koristiti za uspostavljanje QoS funkcija podatkovne ravnine. QoS funkcije upravljačke ravninesu obično implementirane kao softverski proces, zajedno s drugim funkcijama kontrolne ravninepoput protokola usmjeravanja. U praksi postoji samo jedan protokol koji se naširoko koristi za QoS signalizaciju u kontrolnoj ravnini, a taj signalni protokol je RSVP. RSVP se koristi u raznim kontekstima:

- Arhitektura integriranih usluga (*Integrated services architecture-Intserv*)

  U kontekstu arhitekture integriranih usluga RSVP se koristi za obavljanje rezervacije resursa i kontrole pristupa za svaki pojedini prometni tok.

- MPLS prometno inženjerstvo

  RSVP se koristi u kontekstu MPLS prometnog upravljanja, za nadzor pristupa i za postavljanje MPLS prometnih upravljačkih tunela

Ove QoS funkcije i mehanizmi u pravilu se ne koriste u izolirano već zajedno u suradnji, unutar okvira ukupnog QoS ustroja, gdje ti mehanizmi zajednosluže za postizanje ukupnog QoS rezultata s-kraja-na-kraj mreže.

Postoje dvije definirane IP QOS arhitekture:

- Arhitektura (ustroj) integriranih usluga (*Intergrated Services architecture-Intserv*) i
- Arhitektura diferencijalni usluga (*Differentiated Services architecture-DiffServ*)

QoS mehanizmi podatkovne ravnine

Klasifikacija (razvrstavanje)

Klasifikacija je proces kojim se identifikacije vrste prometa u pojedinačnim tokovima prometa (flow), njihovo razvrstavanje na unaprijed određene klase prometa, te grupiraja pojedinačnih tokova iste klase u jedan zbirni tok (stream) kako bi se na sve pakete tog zbirnog toka mogla primjeniti ista pravila i radnje. To ne moraju biti nužno radnje vezane za QoS postupke, već i radnje druge vrste, npr. filtriranje paketa. Kako bismo kompletirali ovu definiciju, moramo još definirati pojmove *tok*, *zbirni (agregatni) tok* i *prometna klasa (razred*).

- Tokovi

  IPv4 tok obično se definira „petorkom“:

  - izvorna IP adresa,
  - odredišna IP adresa,
  - izvorni TCP/UDP priključak,
  - odredišni TCP/UDP priključak i
  - transportni protokol (npr. TCP ili UDP).

Fragmentacija, kodiranje ili tuneliranje može neke tokove napraviti teškim za klasificikaciju jer je neki od gore navedenih podataka mogu biti nedostupni. Na primjer, pretpostavimo da se tok razvrstava koristeći ovu 5-orku, ali veličine paketa u toku prelaze veličinu paketa koji se mogu podržati (definirao maksimalnom prijenosnom jedinicom ili MTU (*maximum transmission unit*) na nekim od temeljnih linkova koji prenose tokove.Ti paketi, koji prelaze MTU tranzitnih veze, biti će potrebno fragmentirati koristeći IP fragmentaciju. Kad se paket fragmentira, uključuju se informacije TCP/UDP porta samo u prvi paket, dakle, bez prvoga fragmentiranoga paketa, za ostale pakete možda neće biti moguće jedinstveno utvrditi da pripadaju istome toku. IPv6 uvodi polje toka(*Label Flow)*koje se može iskoristiti za rješenje ovoga problema.

Kompliciraniji kriteriji od samog korištenja ove 5-orke također se mogu koristiti za definiranje toka. Jedna od takvih tehnika je tzv.dubinski pregled paketa (*Deep packet inspection*)

- Zbirni ili agregatni tok (*stream*) – je zabirni tok više pojedinačnih tokova koji odgovaraju određenoj vrsti prometa temeljem nekih zajedničkih kriterija razvrstavanja. Na primjer, svi VoIP pojedinačni prometni tokovi koji dolaze iz istog izvora (npr. VoIP centrale ili VoIP *gateway*-a) mogu biti prepoznati podudarnošću odgovarajuće izvorne IP adrese toga *gateway*-a. Zbirni tok može se sastojati od samo jednoga pojedinačnog toka, ili više njih.
- *Prometna klasa*. Prometna klasa je udruživanje (agregacija) pojedinačnih prometnih tokova ili zbirnih prometnih tokova, u svrhu omogućavanja primjene zajedničkih akcije na sve članove te prometne klase. Na primjer, klasa može predstavljati sve VoIP promete od nekog određenoga mjesta u mreži u kojem se objedinjava VoIP promet koji stiže iz brojnih VoIP gateway-a. Prometna klasa može se sastojati od samo jednoga pojedinačnog toka, ili više njih.

U sljedećim poglavljima definirat ćemo pojmove "implicitno", "složeno", "dubinska paketska inspekcija" i "jednostavno" kad ih koristimo u kontekstu klasifikacijskih tehnika.

Implicitna klasifikacija(razvrstavanje)
Iz perspektive IP QoS-a, implicitnu klasifikaciju definiramo vrlo općenito te nije potrebno poznavati zaglavlje ili sadržaj paketa pa može za klasifikaciju prometa koristiti kontekst razine 1/razine 2 kao primljeno sučelje ili primljeni virtualni krug (VC).

Složena (Complex) klasifikacija
Složena klasifikacija omogućava nam znatno veću preciznost nego "implicitna' klasifikacija i uključuje identifikaciju prometa na temelju vrijednosti pojedinog polja ili kombinacije polja u IP zaglavlju paketa, koji nisu izričito namijenjeni QoS klasifikaciji. Ovo uključuje ona polja koje smo prethodno definirali u kontekstu 5-orka za klasifikaciju IP toka. Na primjer, klasificiranje dotoka na temelju 5-orke je početak složene klasifikacije. Složena klasifikacija također može klasificirati promet koristeći kriterij razine 2, kao izvorišnu ili destinacijsku MAC adresu, ili pak identificiranje prometa od strane određenog izvora podataka pomoću MAC adrese tog uređaja.

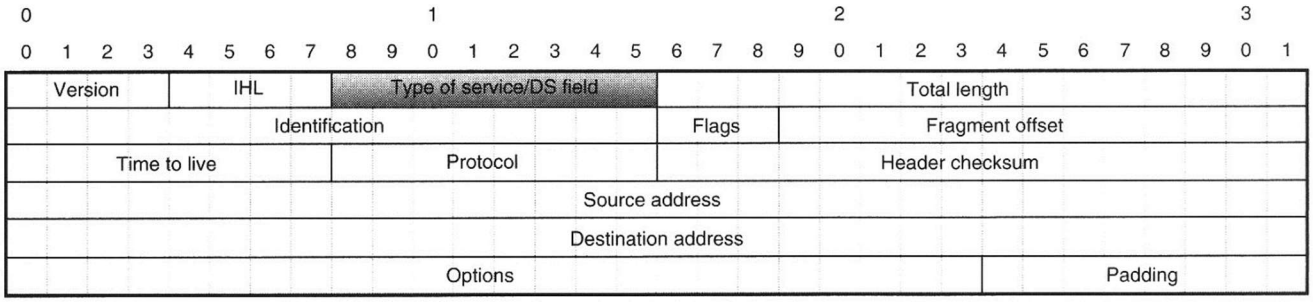
Dubinski paketska inspekcija/inspekcija stanja
Neki sustavi imaju sposobnost klasifikacije prometa koji se ne temelji samo na informaciji sadržanoj u jednom IP zaglavlju paketa. Oni mogu biti u mogućnosti zaviriti dublje i steći uvid u same korisničke podatke koji se prenose u tom paketu. Ovo se naziva dubinski pregled paketa odnosno *dubinska paketska inspekcija (DPI)*. Također, mogu biti u mogućnosti klasificirati pojedinačni tok u skladu s *stanjem informacija* koje se nalaze u višestrukim paketima tog toka, a da se ne gleda svaki paket zasebno. Ovakav pregled nazivamo *inspekcija stanja*(*Statefull Inspection-SI*). Kad se DPI kombinira sa SI, kombinacija može biti korisna za klasificiranje aplikacija koje se ne mogu identificirati pomoću drugih sredstava, kao na primjer neke aplikacije u istoj ravnini (*peer-to-peer applications*). Zbog prometnih zahtjeva koje neke *peer-to-peer*aplikacije mogu zadati mreži, neki programeri takvih aplikacija namjerno pokušavaju otežati klasificiranje svojih aplikacija ili ih prave tako da izgledaju kao druge aplikacije čime otežavaju klasificiranje i kontroliranje. Ova situacija se može usporediti sa utrkom, u kojoj se programeri aplikacija neprestano trude ostati jedan korak ispred klasifikacijskih DPI/SI mogućnosti.

Jednostavna klasifikacija

Ovo je klasifikacija na temelju polja u zaglavljima paketa koji su izričito namijenjeni QOS klasifikaciji. Naziva se 'jednostavna' klasifikacija jer ne zahtijeva razumijevanje drugih polja u IP zaglavlju paketa ili podataka, i ne zahtijeva vidljivost sastavnih tokova unutar zbirnog prometnog toka. Korištenje jednostavnih tehnika klasifikacije čini QoS projekte lakšima te zahtijeva manje složenu provedbu temeljne klasifikacije od strane mrežne opreme. Sljedeće sheme su definirane za izravnu tj. eksplicitnu QoS klasifikaciju u IP i MPLS-u:

- Oktet vrste usluge (*Type of service octet*)

Izvorna Ipv4 specifikacija definira 8-bitno polje koje se koristi za IP QoS klasifikaciju: ovo se naziva *Oktet vrste usluge* i označena je na slici 1

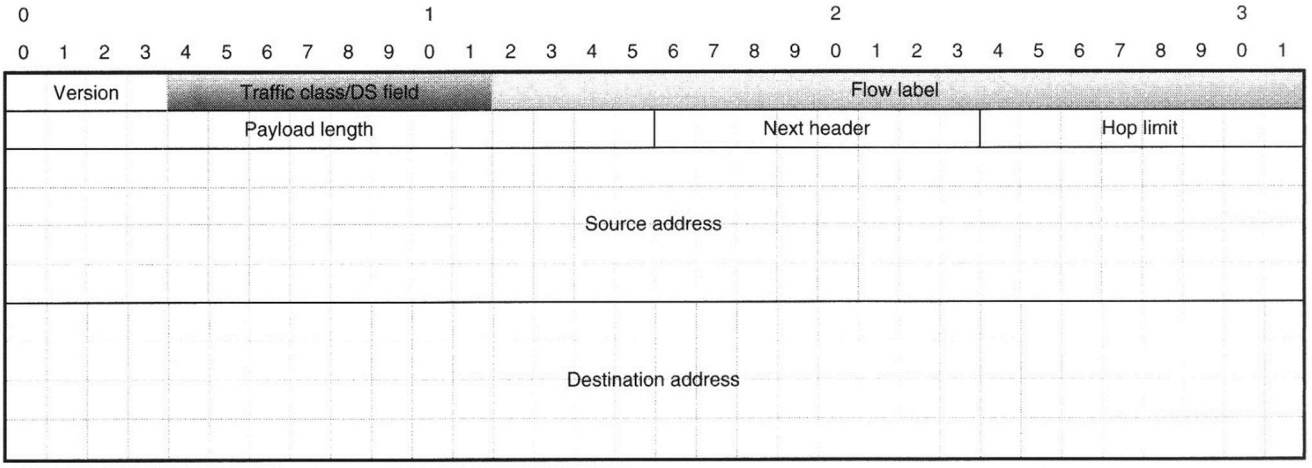


Slika 1: Zaglavlje IPv4 paketa

Informacija iz polja *Oktet vrste usluge* od tada je izgubila na važnosti u odnosu na informaciju iz *polja diferenciranih usluga* (*Differentiated services field*).

- IPv6 oktet klase prometa (*IPv6 traffic class octet*)

[RFC 2460] je prvotno definirao 8-bitno polje klase prometa u okviru IPv6 zaglavlja za QoS oznaku kao što je prikazano na slici 2. IPv6 oktet klase prometa također je zastario u odnosu na polje diferencijalnih usluga.



Slika 2: Traffic Class oktet u IPv6 paketu

Ipv6 zaglavlja paketa također uključuju 20-bitno polje oznake pojedinačnog toka. Oznaka toka pomaže u nedvosmislenom klasificiranju toka u slučaju kada neke informacije koje se inače koriste za identifikaciju toka mogu izostati radi fragmentacije, kodiranja ili tuneliranja, na primjer „trojka“ koja se sastoji od polja oznake toka, izvorišne i destinacijske Ipv6 adrese se koristi za jedinstveno klasificiranje Ipv6 toka.

- Polje diferenciranih usluga (*Differentiated Services field*)

[RFC 2474] je bacio u zastaru i Ipv4 oktet vrste usluge i Ipv6 oktet klase prometa redefinirajući ih kao polje diferenciranih usluga (DS). Od 8 bitova DS polja, 6 ih je definirano kao kodne točake diferencijalnih usluga (*Differentiated Services code point - DSCP*), a 2 bita nižeg reda su u početku zadržana nedefinirana.

[RFC 3168] je kasnije definirao korištenje 2 bita nižeg reda za *Eksplicitno obavještavanje o zagušenju* (ECN).

- MPLS EXP polje

[RFC 3032] definira 3-bitno polje u svakom MPLS zaglavlju za 'eksperimentalno korištenje'. [RFC 3270] je redefinirao uporabu ovog polja za QoS označavanje.

- Označavanje na drugom sloju (Layer 2 marking)

U IP QoS omogućenoj mreži također može postojati potreba da se iskoristi QoS označavanje na razini drugog sloja. Najbolji primjer za ovo je Ethernet, gdje IEEE 802.1D [802.1D] definira uporabu 3-bitnog polja za QoS označavanje.

Posebna klasifikacijska politika može sadržavati logičke kombinacije složenih i jednostavnih klasifikacijskih kriterija. Na primjer, da odgovara cjelokupnom prometu s određenim DS označavanjem polja AND koji dolazi iz određenog izvora IP adrese.

Zašto pravimo razliku između složene i jednostavne klasifikacije? Prvenstveno zato što odabir klasifikacijskih tehnika i način na koji se koriste utječu na složenost i mogućnosti proširenja mreže proizašlih iz QoS dizajna. Na primjer, korištenje izvorišne IP adrese servera može biti razuman način za identifikaciju zbirnog prometnog toka. Ako je ovo jedini klasifikacijski kriterij za taj prometni tok, onda bi svi razvrstavači u cijeloj mreži trebali biti konfigurirani na taj način, tj da se promet tog toka klasificira na način da se izvorišna ili destinacijska IP adresa paketa mora podudarati sa adresom tog servera.

Ovo bi zahtijevalo da je svaki usmjerivač u mreži konfiguriran sa ovim razvrstavačem. Ovo može izgledati izvedivo, ali što ako ima sto servera a ne samo jedan? Nadalje, što ako se IP adresa jednog ili više servera promijeni? Ubrzo postaje jasno da ručna konfiguracija složenih razvrstavača unutar mreže za razvrstavanje tokova nije moguća. Također je primjećeno da složeni razvrstavajući pristupi imaju utjecaj na performanse same usmjerivačke platforme. Na usmjerivačkim platformama koje se temelje na softveru, složena razvrstavanja može biti podizati intenzitet rada procesora i kao posljedicu može imati utjecaj na brzinu prosljeđivanja usmjerivača. Na hardverskim pak usmjerivačkim platformama može postojati ograničenje broja kompleksnih razvrstavača koji mogu biti podržavani hardverom.

Prema tome, i kao što ćemo vidjeti kasnije u knjizi, QoS ustrojstva koja se upotrebljavaju danas ne koriste ručno konfiguriranu kompleksnu klasifikaciju diljem mreže. Umjesto toga koristi se

arhitektura integriranih usluga koja koristi signalizacijski protokol za uspostavljanje razvrstavača po pojedinačnom toku, a arhitektura diferencijalnih usluga općenito koristi jednostavnu klasifikaciju koja se temelji na sparivanju skupina prometa identificiranih pomoću oznaka iz DSCP polja. Tamo gdje je nužna kompleksna klasifikacija, ona se limitira na ulaznom rubu mreže.

Obilježavanje

Označavanje IP paketa, što je također poznato kao „bojanje“, je proces postavljanja vrijednost polja dodijeljenih za QoS klasifikaciju u IP MPLS ili zaglavlju paketa, tako da se prometi kasnije lako mogu prepoznati, tj. prepoznavati pomoću jednostavnih klasifikacijskih tehnika.

Obilježavanje može koristiti bilo koja od shema opisanih u prošlom poglavlju, međutim, sa zastarijevanjem IP i TOS polja, DSCP i polje MPLS EXP postaju glavna polja koja se koriste za označavanje IP/MPLS paketa i njihovu klasifikaciju.

Promet se u pravilu označava na izvoru krajnjega sustava ili što je moguće bliže izvoru prometa kako bi se pojednostavio dizajn mreže:

Označavanje na izvoru

Označavanje paketa može se primijeniti na izvoru krajnjega sustava, a ako se krajnjem sustavu vjeruje, onda se na ovo obilježavanje možemo oslanjti kroz na putu paketa kroz ostatak mreže, a eventualno potom zahtijevati samo jednostavnu klasifikaciju za identifikaciju zbirnih prometnih protoka.

Označavanje na ulasku

Ako krajnji sustav nije sposoban za označavanje paketa koje generira, ili mu se ne može vjerovati da će to učiniti pravilno, tada se taj zadatak može povjeriti pouzdanom uređaju na ulasku u mrežu u blizini izvora koji može koristiti implicitnu, odnosno kompleksnu klasifikaciju za identificiranje prometnog toka iz krajnjega sustava i označiti promet tako da se može naknadno identificirati pomoću jednostavnih klasifikacijskih tehnika. Ako izvor nije pouzdan za označavanje paketa, a onda se sve oznake koje su se prethodno postavljene na pakete mogu promjeniti, a to se ponekad naziva "ponovno označavanje."

Takvo prometno obilježavanje može se primijeniti bezuvjetno, npr. označiti DSCP s 34 za sav promet primljen na određenome sučelju. Prometno označavanje također se može primijeniti kao uvjetno zbog „prometnoga nadglednika („*traffic policer*“) (vidi slijedeći Odjeljak za više informacija o „nadglednicima“), npr. za promet primljen u sučelju koje je u skladu s definiranom oznakom od strane nadglednika DSCP u 34, za promet koji nije u skladu s (tj. veći je od) definicije koju je postavio nadglednik oznakom DSCP u 36. Ovo uvjetno ponašanje obilježavanja omogućuje izvršenje prometnoga ugovora u skladu ili izvan koncepta ugovorenih granica.

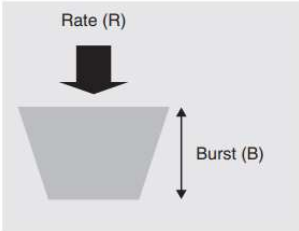
Čak i kada se izvoru krajnjega sustava vjeruje pri označavanju generiranog prometa, nadglednik još uvijek može provjeriti je li prometni tok od izvora u skladu s dogovorenim prometnim ugovorom. Na primjer, izvor može proizvesti sav promet s DSCP 34;što nam onda omogućava da jednostavnom klasifikacijom sa DSCP 34 vršimo ulaznu klasifikaciju zbirnog prometnoga toka, a primjenjeni nadglednik će zatim ostaviti DSCP na 34, ako je promet u

skladu s nadglednikovom definicijom (tj. "u skladu s ugovorom"), ili ga promijenit u DSCP 36 ukoliko on prelazi definiciju nadglednika (tj. "nije u skladu s ugovorom").

Nadzor i mjerenje

Nadgledanje (*Policing)* je mehanizam koji se može koristiti kako bi se osiguralo da prometni tok ne prelazi definiranu maksimalnu brzinu. „Nadglednik“ („*Policer*“) se normalno može vizualizirati kao mehanizam toka žetona. Ovo se ne treba miješati s algoritmom pohrane i propuštanja, koja ima različita svojstva, te se češće koristi za oblikovanje prometa, kao što će biti objašnjeno u slijedećim poglavljima.

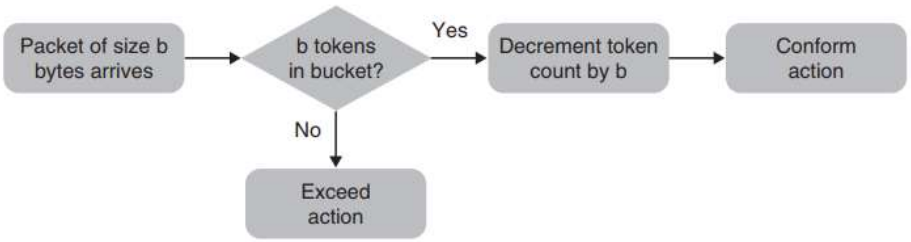
Jednostavan jedno-brzinski nadglednik spremnika žetona (*one-rate token bucket policer*) ima definiranu maksimalnu dubinu spremnika (obično u Bajtovima), poznatu kao prasak B i definiranu brzinu R (obično u bit/s) kojom se spremnik puni žetonima veličine bajta (vidi sliku ispod).



Slika 3: Spremnik žetona

Ovisno o provedbi određenoga nadglednika, žetoni se dodaju u spremnika brzinom R svaki puta kada nadglednik obrađuje paket ili u redovitim intervalima, do maksimalnoga broja žetona koji mogu biti u spremniku, kojega definira B. Minimalan broj žetona u spremnika je nula.

Kada se mehanizam nadglednika spremnika žetona primjenjuje na prometni tok, a paket dolazi iz toga toka, veličina paketa b uspoređuje se s brojem žetona koji su trenutno u spremniku. Ako postoji barem toliko bajt-žetona u spremnika koliko postoji bajtova u paketu, onda ćemo koristiti terminologiju da je paket "usklađen" s definiranim spremnikom žetona, a ako ima manje žetona u spremnika nego bajtova u paketu, onda je paket "premašio" definiciju spremnika žetona. Ako je paket sukladan broju žetona, onda je smanjenje broja žetona u spremniku jednako veličini paketa b. Ponašanje ovoga jednostavnoga nadglednika opisano je dijagramom toka na slici ispod.



Slika 4: Jednostavan jedno-brzinski nadglednik

Ovisno o tome jesu li paket usklađen s brojem žetona ili prelazi definiran broj žetona u spremniku, možemo primjeniti različite aktivnosti. Najjednostavniji akcije su: prenijeti paket, ako postoji usklađenost ili odbaciti paket ukoliko se ona premaši. Primijenjen na takav način,

nadglednik spremnika žetona će prisiljavati prometni tok (na definiranu maksimalnu brzinu R i prasak B) da se drži ugovorenih vrijednosti.

Akcije koje provodi nadglednik kod zadovoljenja ili prekoračenja ugovorenih granica, ne ograničavaju se samo na prijenos ili odbacivanje prometa, već one također mogu uključivati označavanje prometa ili kombinaciju svih tih radnji, stoga se nadglednici ponekad nazivaju i „*markeri*“. Obilježavanje se obično koristi u sprezi s politikom provedbe definirane brzine prometnoga toka "iz ugovora",a da bi se omogućio prijenos prometa brzinom i većom od ugovorene, ali tako da ga se označi drugačije od prometa u okviru ugovorene brzine (ovo bi obilježavanje potencijalno moglo vrijediti za bilo koje polje opisano u prijašnjim poglavljima) kako bi se označilo da je "izvan ugovora", te kako bi mu se potencijalno mogla dati blaža SLA pravila nego ugovorenome prometu.Detaljniji opis primjene označavanja prometa „u neskladu s ugovorom“ i „u skladu s ugovorom“ dan je u sljedećem odjeljku.

Važno je napomenuti da nadglednik spremnika žetona nikada ne usporava promet, a „oblikovatelj“ da. Ne postoje paketi pohranjeni u spremniku, tu su samo žetoni! Dakle, kako nadglednik ne usporava promet, isto tako on ne može se napraviti novi redoslijed ili postaviti novi prioritet prometa već to radi „raspoređivač“ (*scheduler*).

Jednostavan nadglednik spremnika žetona opisan u ovome odjeljku je podskup funkcionalnosti najčešće korištenih nadglednika, što je opisano u nastavku.

RFC 2697: Jednobrzinski trobojni marker (Single Rate Three Color Marker- SR-TCM)
Najčešće korišten nadglednik određen je "jednobrzinskim trobojnim markerom" (SR-TCM) definiranim u IETF RFC 2697 [RFC 2697], iako se ova definicija odnosi na "marker" tj označivač, ona se može iskoristiti za prometnoga nadglednika (*policer*), kao i za označavanje prometa. "Tri boje" odnosi se na tri moguća stanja koja su ishodi SR-TCM-a rada, a koje su opisane pomoću shemu boja "semafora".

SR-TCM koristiti dva spremnika žetona, kao što je prikazano na slici ispod, a ne u jedan spremnik žetona opisan za jednostavnoga nadglednika u prethodnome odjeljku.

Slika 5: Jednobrzinski trobojni marker

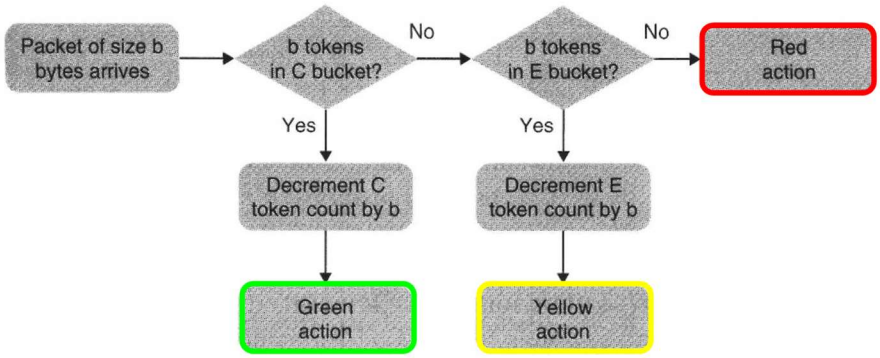
Spremnici su definirani kao C i E (za usklađene ili one koji premašuju) s maksimalnim praskom veličine CBS odnosno EBS.

Oba spremnika sepune žetonima istom brzinom CIR. Kad se SR-TCM primjenjuje na prometni tok i pakete koji dolaze iz toga toka:

- Paket veličine *b* uspoređuje se prema broju žetona koji su trenutno u spremniku C. Ako postoji barem onoliko žetona u spremnika C koliko ima bajtova u paketu, smatra se da je paket usklađen s SR-TCM definicijom, a samo se sadržaj C spremnika smanjujeza

broj žetona koji je jednak broju bajtova u paketu. Kod korištenja sheme boja "semafora" RFC 2697 za označavanje prometne usklađenosti, u ovome slučaju se za paket kaže da je zelen.

- U PROTIVNOME AKO (ELSE IF) u spremniku C nema toliko žetona koliko ima bajtova u paketu, onda je paket premašio C spremnik prema SR-TCM definiciji i sada se uspoređuje s E spremnikom. Ako (IF) postoji barem toliko bajtova žetona u spremnika E kao što ima bajtova u paketu, onda se samo sadržaj E spremnika smanjuje za broj žetona koji je jednak broju bajtova u paketu. Korištenjem sheme boja semafora, u ovome slučaju se za paket kaže da je žut.
- U PROTIVNOME AKO (ELSE IF) ni u spremniku C niti u spremniku E nema toliko žetona koliko bajtova u paketu, onda ćemo koristiti terminologiju da je paket "povrijedio" definiciju oba spremnika jednobrzinskog trobojnog markera. Korištenjem sheme boja semafora, u ovome slučaju, za paket se kaže da je crven pa se ni jedan spremnik neće smanjiti. Dijagram na slici ispod prikazuje rad SR-TCM.



Slika 6: Jednobrzinski trobojni marker (daltonistički način rada)

CIR i CBS moraju se postaviti > 0, inače će svi paketi biti crvene boje. Ako je EBS = 0, tada izlazna vrijednost markera ima samo dva stanja, a paketi će biti obilježeni kao ili zeleni ili crveni, a efektivno ponašanje SR-TCM se svodi na jednostavnog jedno-brzinskoga nadglednika kojeg smo opisali u prethodnom odjeljku, tj. "Jednobrzinski marker u dvije boje".

Sada se mogu primijeniti različite aktivnosti kao što su prijenos, odbacivanje ili obilježavanje paketa - eventualno u kombinacijama - ovisno o tome je li paket određen kao zelen, žut ili crven od strane SR-TCM:

- Zeleni paketi će se prenositi i mogu se također i obilježiti, nema smisla da se vrši akcija odbacivanja zelenih paketa.
- Žuti paketi će se prenijeti, a isto tako mogu se i označiti. Nema smisla da se primijeni odbacivanje žutih paketa ako je EBS ≠ 0, pošto bi učinak bio da će se svi paketi, koji su žute ili crvene boje izostaviti, tj. ne bi bilo razlika između njih.
- Crveni paketi mogu se prenijeti ili obilježiti i prenijeti, ili odbaciti. Možda se pitate zašto ne bi bilo potrebe za prijenos crvenih paketa bez ponovnoga označavanja. To se može učiniti ako se primjenjuje nadglednik koji ima funkciju mjerenja samo da mjeri da li promet premašuje definiranu brzinu.

Primjena SR-TCM može postaviti EBS > 0 i primijeniti zeleno djelovanje (prijenos + oznaka koja navodi da je promet "prema ugovoru"), žuto djelovanje (prijenos + oznaka koja navodi da je promet "izvan ugovora"), i crveno djelovanje za odbacivanje.

Primijenjen na taj način, SR-TCM će ograničiti maksimalnu brzinu CIR i praska (CBS + EBS) prometnih tokova, a prenesen promet će se označiti kao unutar ili izvan ugovora, ovisno je li zadovoljen ili premašen prasak CBS-a. U praksi, međutim, teško je shvatiti koja je smislena korist od usluge koja nudi razlikovanje prometa između „unutar granica“ i „izvan granica ugovora“ ovisno o razini praskovitosti prometa.

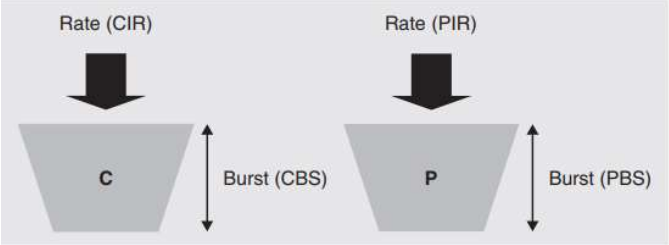
Alternativno isti marker može se primijeniti sa zelenim djelovanjem prijenosa, žutim djelovanjem (prijenos + oznaka da koja navodi da je promet „izvan ugovora“) i crvenim djelovanjem (prijenos + oznaka koja navodi da je promet "jako puno van ugovorenoga"), međutim, u praksi postoji slična poteškoća za razumjeti koja smislena korist može biti od usluge koja nudi razlikovanjem prometa između „izvan ugovora“ i „silno izvan ugovora“ ovisno o njihovoj razini praskovitosti.

Dakle, RFC 2697 "Jednobrzinski trobojni marker" ne koristi se često na taj način, već se uglavnom koristi uz EBS = 0. Najčešće primjene su:

- Provođenje maksimalne brzine za glasovnu klasu prometa, EBS = 0 i primjenom zelene akcije prijenosa i crvene akcije odbacivanja. Primijenjen na taj način SR-TCM će provesti ograničenje na maksimalnu brzinu CIR i maksimalni prasak CBS u prometnome toku, a bilo koji promet koji prelazi ove granice bi se odbacio, što je tipično za uvjetovana ponašanja koja se koriste za *Differentiated Services* ***Expedited*** *Forwarding Per-Hop Behavior* koja će biti opisana u slijedećim poglavljima.
- Obilježavanje određene količinu prometne klase kao „unutar ugovora“, a sve iznad toga kao „izvan ugovora“ uz EBS = 0 i primjenom zelene akcije prijenosa (ukoliko nije bilo prethodnog obilježavanjaonda bi se uz prijenos moglo raditi i obilježavanje„u skladu s ugovorom“) i crvene akcije (prijenos + obilježavanje„izvan govora“). Primijenjen na taj način SR-TCM bi provodio nadzormaksimalne dozvoljene brzine CIRi praska CBS prometnoga toka.Promet bilo kojeg prometnog toka koji bi prelazio te granice ne bi se odbacio, već bi se označio da je „izvan ugovora“, što je tipično za ponašanje uređaja koji se koriste za*Differentiated Services* ***Assured*** *Forwarding Per-Hop Behavior* kao što će biti objašnjeno u slijedećim poglavljima.

RFC 2698: Dvo-brzinski trobojni marker (TR-TCM)

RFC 2698 [RFC 2698] definira drugoga često korištenoga nadglednik/markera: "trobojni marker s dvije brzine" (TR-TCM). Slično kao i SR-TCM, TR-TCM također koristi dva spremnika žetona.Međutim, u slučaju markera s dvije brzine, spremnici su označeni kao C i P, s veličinama praska CBS odnosno PBS ali koji se pune različitim brzinama. C se puni na prema principu CIR-a (*committed information rate*), a P se puni vršnom brzinom informacija – PIR (*peak information rate*), gdje je PIR ≥ CIR, a CBS ≥ PBS kao što je prikazano na slici ispod.

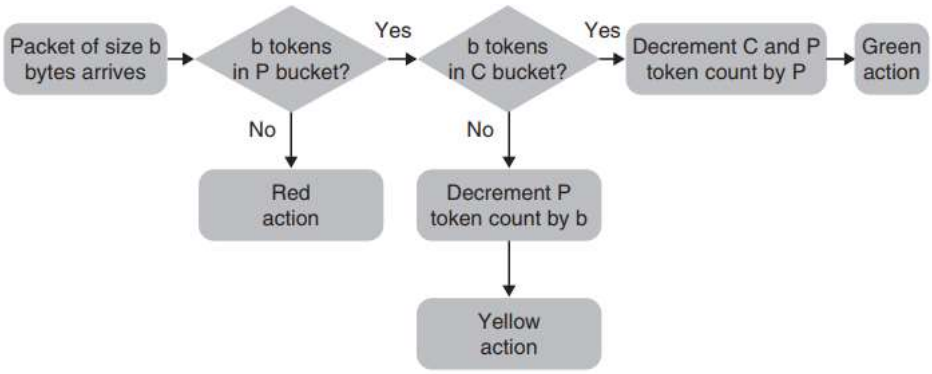


Slika 7: Trobojni marker s dvije brzine

Kada se TR-TCM primjenjuje na prometne tokove, a paketa iz toga toka dolazi:

- Veličina paketa *b* uspoređuje se prema broju žetona koji su trenutno u spremniku P. Ako ima manje žetona u spremniku P od bajtova u paketu, onda paket narušava TR-TCM definiciju, pa se vrijednost nijednog spremnika neće umanjiti. Koristeći shemu semafora, u ovome slučaju za paket se kaže da je crven.
- **U protivnome ako** (ELSE IF) postoji barem onoliko žetona u spremniku P koliko ima bajtova u paketu, onda se paket uspoređuje sa spremnikom C. **Ako**postoji manje žetona u spremniku C nego bajtova u paketu, onda je paket premašio kapacitet spremnika C prema TR-TCM definiciji pa samo spremnik P smanjuje žetone za broj koji je jednak broju bajtova u paketu. Koristeći shemu semafora, u ovome slučaju za paket se kaže da je žut.
- **U protivnome ako** (ELSE IF) ako postoji barem onoliko žetona u spremniku C koliko ima bajtova u paketu, onda je paket usklađen prema definiciji TR-TCM, u spremnicima C i P smanjuje se broj žetona za broj koji je jednak broju bajtova u paketu. Koristeći shemu semafora, u ovom slučaju za paket se kaže da je zelen.

Dijagram toka na slici ispod prikazuje rad TR-TCM.



Slika 8: Dvo-brzinski trobojni marker (mod rada „sljep na boje“)

Kao i kod SR-TCM, sada se mogu primijeniti različite aktivnosti, kao što su prijenos, odbacivanje ili označavanje–eventualno i u kombinaciji - ovisno o tome je li paket od strane TR-TCM određen kao zelen, žut, ili crven.

Primjer korištenje TR-TCM jest označavanje određene količine prometnih klasa kao „u skladu sa ugovorom“, a sve iznad toga kao „van ugovora“ (povreda ugovora), sve do određene maksimalne brzine. U tome slučaju primjenom zelene akcije prijenosa (ako paketi ne bi prethodno bili označeni, onda bi se akcija prijenosa mogla kombinirati s akcijom označavanja

paketa kao „u skladu s ugovorom“), žuteaktivnosti (prijenos + obilježavanje paketa kao„izvan ugovora“) i crvenom akcijom odbacivanja paketa.

Primijenjen na ovaj način, TR-TCM će provesti ograničenje maksimalne brzine CIR i praska CBS na prometnome toku. Bilo koji veći promet onda će se označit kao „izvan ugovora“ sve do najveće brzine PIR i praska PBS . Iako je moguće imaticrveno djelovanje (prijenos + oznaka), iz istih razloga kao što je objašnjeno za SR-TCM, u praksi je teško razumjeti koja bi se smislena uslužna korist dobila razlikovanjem između prometa u smislu „unutar“, „izvan“ odnosno „veoma izvan ugovora“. Dakle, u praksi TR-TCM najčešće se koristi kao "dvo-brzinski dvobojni marker", uz crveno djelovanje odbacivanja paketa.

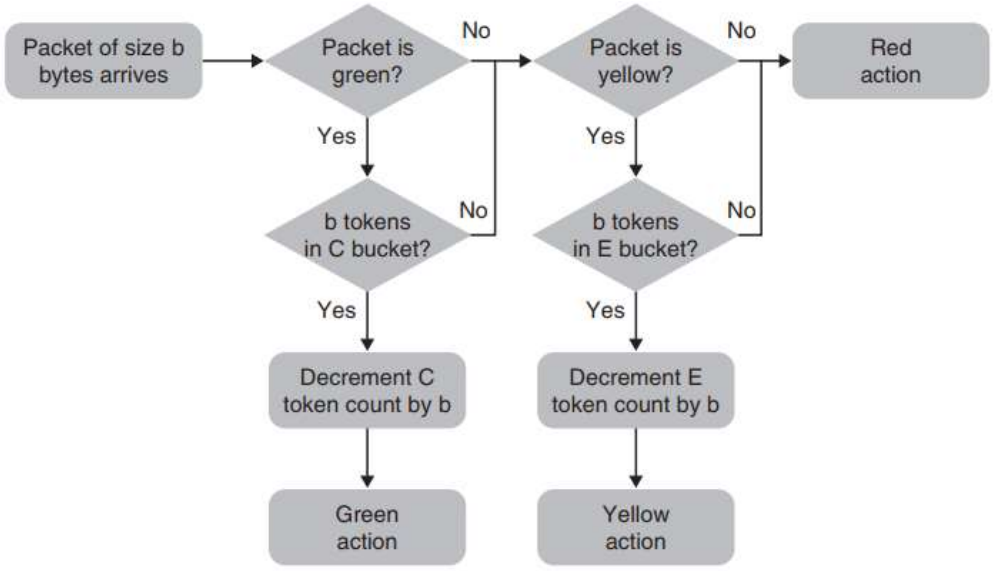
Napomenimo da ako je PIR = CIR, a PBS = CBS, onda izlaz markera ima samo dva stanja, zeleno i crveno. U ovome slučaju, efektivno ponašanje bit će isto kao i kod jednostavnoga jedno-brzinskog nadglednika koji je već opisan. Postavljanje PIR < CIR ili PBS < CBS može uzrokovati nepredvidive rezultate, gdje isti paket može prekoračiti ograničenja P spremnika, tj. biti određen kao crven, a istovremeno biti u skladu s ograničenjem C spremnika, tj. bio određen kao zelen.

Ponašanja nadglednika prometa koje smo do sada opisali bila su zasnovana na „neosjetljivost na boje“, što znači, da nakon što su paketi jednom klasificirani u toku koji se nadzire, nadglednik primjenjuje svoja pravila nevezano za oznake na paketima. Međutim, preporuke RFC 2697 i RFC 2698, također definiraju načine rada "svjesnosti boja" (*color-aware mode*). Pri radu u *color-aware* modu, nakon što su paketi klasificirani u toku koji se nadzire, nadglednik uzima u obzir sve postojeće oznake koje su mogle biti postavljene (npr. od nadglednika u prethodnome čvoru mreže), kod određivanja odgovarajuće akcije koju će primjeniti na paket temeljem „politike svjesnosti boja“, dopuštajući primjenu različitih aktivnosti ovisno o već postojećim oznakama.

RFC 2697 SR-TCM koristi iste takve definicije spremnika žetona kod *color-aware* moda kao i kod *colorblind* moda. Kada se *color-aware* mod primijeni na prometni tok, ponaša se na slijedeći način:

- AKO paket, koji je prethodno obojen zelenom bojom i ima barem onoliko žetona u spremnika C koliko bajtova u paketu, onda paket udovoljava uvjete spremnika C, označava se zeleno te se broj žetona u spremniku C smanjuje za broj jednak broju bajtova u paketu.
- U PROTIVNOME AKO JE paket već obojan zeleno ili žuto i ima barem onoliko žetona u spremniku E koliko i bajtova u paketu, onda se paket koji premašuje kapacitet C spremnika, označava žutom bojom, a samo se u E spremniku smanjuje broj žetona brojem koji je jednak broju bajtova u paketu.
- U PROTIVNOME paket krši SR-TCM definiciju, pa se označava crveno i niti jedan spremnik neće se smanjiti.

Dijagram toka na slici ispod prikazuje rad SR-TCM u *color-aware* modu.



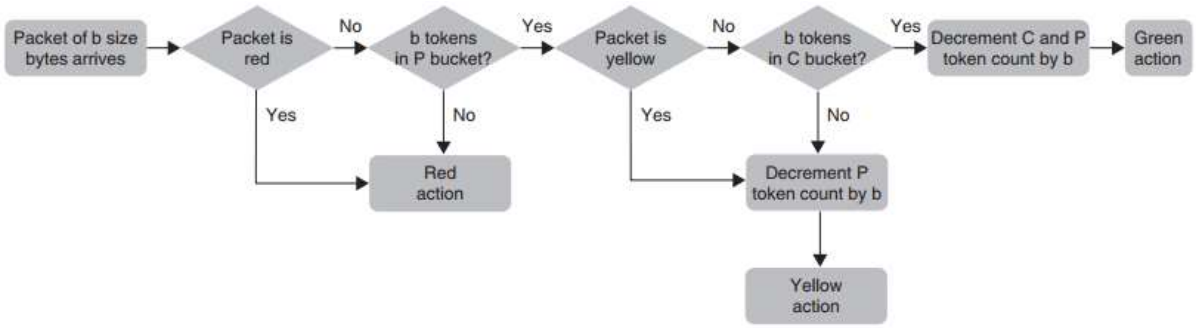
Slika 9: Jedno-brzinski trobojni marker koji prepoznaje boje

Kada SR-TCM djeluje na način da prepoznaje boje (*color-aware* mod), osigurava da se paketi koji su prethodno označeni kao žuti ili crveni ne računaju u odnosu na C spremnik, a oni paketi koji su prethodno označeni crveno, ne računaju se u odnosu na E spremnik.

Preporuka RFC 2698 TR-TCM koristi iste takve definicije spremnika žetona kod *color-aware* moda kao i kod *colorblind* moda. Kada se *color-aware* mod primijeni na prometni tok, ponaša se na slijedeći način:

- AKO je paket prethodno označen kao crven ili ako ima manje žetona u spremniku P od bajtova u paketu, onda paket krši TR-TCM definiciju, označava se crveno, pa se nijedan spremnik neće smanjiti.
- U PROTIVNOME, AKO je paket prethodno označen žutom bojom, ili ako ima manje žetona u spremniku C nego bajtova u paketu, onda paket premašuje definiciju C spremnika, pa se označava žuto, a u P spremniku se smanjuje broj žetona za broj koji je jednak broju bajtova u paketu.
- U PROTIVNOME, paket odgovara TR-TCM definiciji, označava se zeleno, pa se u oba spremnika (C i P) smanjuje broj žetona za broj koji je jednak broju bajtova u paketu.

Dijagram toka na slici ispod prikazuje rad TR-TCM kod *color-aware* moda.



Slika 10: Dvo-brzinski trobojni marker sa prepoznavanjem boja

Nadglednici koji prepoznaju boje (*color-aware policer*) obično se koriste na granicama „povjerenja“, gdje se za čvor prema kojemu teku podaci (čvor A) očekuje da primjenjuje određenu definiciju nadglednika prema prometnome toku poštujući prometni ugovor prije slanja prometa čvoru od kojega dolaze podaci (čvor B). Nadglednik sa prepoznavanjem boja primjenjuje se na čvoru B kako bi se osiguralo da je promet primjereno uvjetovan čvorom A, dok se također nastoji osigurati da se promet ne označava ponovno.

Ako se nadglednik koji nije svjestan boja, primijeni i na čvor B, a obzirom da nadglednici djeluju samostalno, za pakete koji su određeni kao zeleni od čvora A, mogu se odrediti kao žuti ili crveni u čvoru B. Slično tako paketi koji su određeni kao žuti od čvora A mogu promijeniti boje u zelenu ili crvenu u B čvoru, a paketi koji su određeni kao crveni od čvora A mogu postati zelene ili žute boje u čvoru B. Mrežni učinak ovoga mogao bi biti da se pogrešne količine prometa označene kao zelene, žute ili crvene, a samim time PIR, odnosno CIR obveze ne mogu biti ispunjene. Korištenjem nadglednika koji raspoznaje boje u čvoru B u kombinaciji s nadglednikom koji **ne** raspoznaje boje u čvoru A riješava se ovaj problem i osigurava da se u čvoru B žetoni određene boje troše samo na pakete iste boje.

Mjerenja

Mjerenje prometa je postupak mjerenja brzine i karakteristika praska prometnoga toka. Jednostavna funkcija mjerenja može se sastojati od primjene jedno-brzinskoga ili dvo-brzinskoga nadglednika prometnoga toka, ali uz zelene, žute i crvene akcije koje su sve postavljene na prijenos (bez odbacivanja). Ako vodimo statistiku broja paketa te prenesenim i odbačenim bajtovima, onda se ove statistike mogu koristiti kao metrika prometnoga toka. Alternativno, mjerenje se može provesti jednostavno uzimanjem statistike paketa i bajtova prenesenih prometnim tokovima ili klasama, tijekom određenoga vremenskog intervala. Ovkav pristup omogućava nam mjerenje srednje vrijednost brzine tijekom vremenskoga intervala, ne i sposobnost mjerenja prometnoga praska.

PREDAVANJE 6 – Uvod u QoS mehaniku i arhitekture II

U najopćenitijem smislu, ako zahtjevi postavljeni na bilo kojem konačnom resursu premaše sposobnost tog resursa, nastaje sukob. Raspoređivanje (*scheduling*) posreduje između zahtjeva kad se sukob dogodi, određujući vrijeme ili redoslijed servisiranja različitih zahtjeva. Raspoređivač je onaj koji određuje raspored. Raspoređivanje može promijeniti redoslijed obrade zahtjeva u odnosu na njihovo vrijeme dolaska. Mijenjanje redoslijeda je moguće jedino kada zahtjevi kasne ili čekaju u redu (inače bi već svi bili obrađeni pa ih ne bi mogli ni raspoređivati).

U IP QoS smislu kad na primjer dolazni prometni zahtjevi prelaze propusnost veze nastaje zagušenje i dio prometa kasni ili čeka u redu prije nego može biti obrađen. IP raspoređivač djeluje na pakete u redu čekanja tako da određuje vrijeme njihovog odlaska (raspoređivač u realnom vremenu), ili na redoslijed njihova odlaska (raspoređivač u relativnom vremenu), te razmješta odlaske paketa u skladu s pravilima koji proizlaze iz ograničenja brzine ili prioriteta. *Čekanje u redu* i *raspoređivanje* koriste se u sprezi za kontrolu kašnjenja te za osiguranje propusnost prometnih tokova.

Čekanje u redu i raspoređivanje

Čekanje u redu i *raspoređivanje* u IP QoS-u ima mnogo bliskih analogija sa svakodnevnim životom. Razmotrimo jednostavan primjer prijave na aerodromu gdje postoji određeni broj *Check-in*šaltera koji svi opslužuju samo jedan red u kojem čekaju putnici. Kada se neki šalter oslobodi, uslužuje onog koji je trenutno prvi na redu iz tog jednog reda čekanja. To je tzv. *first-come first-served*tj. FCFS princip, a koji se također naziva i prvi-unutra prvi-van (*first-in first-out*tj. **FIFO**). Duljina reda čekanja određena je odnosom brzine kojom putnici pristižu na aerodrom i brzine kojom šalteri obrađuju putnike. Putnici koji dolaze započinju svoje čekanje na kraju, odnosno, "repu“ (*tail*) reda, a uslužuju se početku odnosno "čelu“ (*head*) reda. Ovo je primjer najosnovnije strukture *čekanja u redu*koja je prikazana na slici ispod.

Slika 1: osnovna struktura čekanja u redu

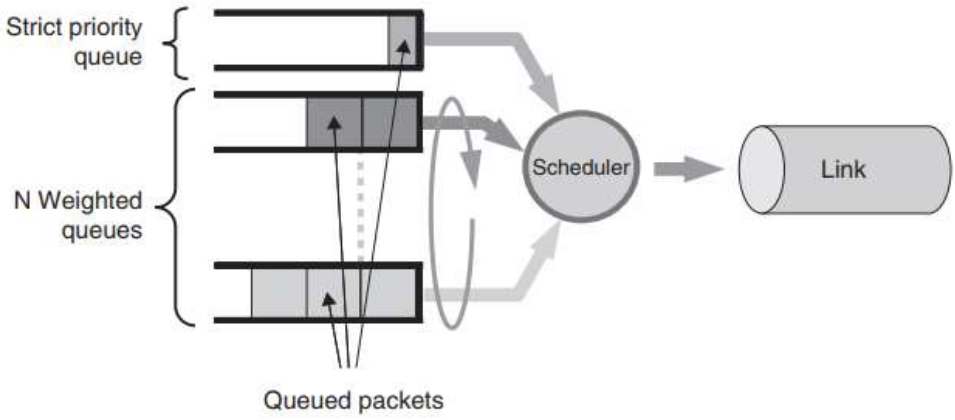
Nekoliko sati prije polaska aviona, brzina dolaska putnika na šalter je relativno niska te će većina putnika koji tad dođu biti uslužena odmah. Sat ili dva prije polaska kad većina putnika dolazi na prijavu, brzina dolaska putnika je veća od brzine posluživanje te se počinje formirati red. Što je veća razlika u brzini dolaska putnika i brzini usluživanja na šalteru, to će red biti duži, a mogućnost kašnjenja putnika u redu će se povećati. Ovaj slučaj je analogan IP mreži sa jednom klasom usluge (suzdržavamo se od naziva *"best-effort*" iz razloga opisanih u prethodnom odjeljku) gdje je prosljeđivanje paketa ravnopravno: svi paketi dobivaju istu kvalitetu usluge te se paketi prosljeđuju koristeći stroga FIFO pravila čekanja u redu.

Ukoliko postoji šalter (ili šalteri) namijenjen poslovnoj klasi putnika koji imaju poseban red, i ako je razlika između brzine dolaska i brzine posluživanja za putnike poslovnog razreda manja

nego za putnike ekonomskog razreda, onda bi duljina reda poslovnog razreda trebala biti manja nego red čekanja u ekonomskom razredu kao i kašnjenje uzrokovano čekanjem na šalteru. Razmislimo sada o dodatnom šalteru i redu čekanja za putnike prvog razreda; ako je razlika između brzine dolaska i brzine posluživanja za putnike prvog razreda manja nego za putnike poslovnog razreda, onda je putnicima prvog razreda vrijeme čekanja na šalteru još kraće.

Dakle, vremenom kašnjenja usljed redova čekanja različitih razreda može se upravljati kontroliranjem brzine posluživanja (ovisi o broju šaltera) u odnosu na brzinu dolaska putnika pojedinog razreda. Kašnjenje usljed čekanja u redu za putnike prvog razreda se može dodatno smanjiti primjenom prioriteta tako da putnik prvog razreda bude uslužen odmah nakon što se oslobodi bilo koji šalter, bez obzira o kojem se šalteru radi (ekonomski, poslovni ili prvi razred). Osim toga, da bi učinkovito iskoristili resurse i osigurali da ni jedan šalter ne stoji prazan, čim se bilo koji šalter oslobodi (ekonomski, poslovni ili prvi razred), putnik iz bilo kojeg reda čekanja treba prijeći na taj prazan šalter.

Ova aerodromska shema *čekanja u redu* na *check-in* šalterima jako je blizu osnovne IP izvedbe raspoređivanja. Na isti način na koji je *check-in* šalter točka gomilanja putnika, tako usmjerivač može biti točka gomilanja IP prometa; promet koji pristiže sa više veza može biti nagomilan na jednu odlaznu vezu. Ovako gomilanje može dovesti do preopterećenja tj. zagušenja, pa stoga i do potrebe za *čekanjem u redu* i *raspoređivanjem* paketa pri postavljanju na fizičko sučelje.



Slika 2: Shema osnovnog IP raspoređivača

Prioritetno raspoređivanje (*Priority Scheduling*)
Većina danas dostupnih osnovnih IP paketskih raspoređivača, podržava obradu reda čekanja s raspoređivačem koji pruža prioritet obrade prometu koji ne tolerira kašnjenje kao što su glasovni i video podaci.

Općenito smatrajući, prioritetno raspoređivanje može biti prethodno tj. preventivno (*pre-emptive*) ili ne-preventivno. Algoritam preventivnoga prioriteta posluživat će prioritetan red čekanja čim dođe do nastanka reda, dok će algoritam ne-preventivnoga prioriteta odmah staviti prioritetan red čekanja na vrh popisa posluživanih redova čekanja. U tome kontekstu, preventivno raspoređivanje može biti bilo na razini paketa ili na kvantnoj razini (na razini neke određene količine paketa).

Ukoliko imamo preventivno raspoređivanje na razini paketa, paketu bez prioriteta koji se treba rasporediti, prvo će mu se postaviti prioritet, a tek tada će ga raspoređivač u potpunosti poslužiti. Ovakav pristup nam pružanajmanje kašnjenje za prvenstveni red čekanja, ali i rezultira sa lošom učinkovitosti propusnosti jer se javlja pojava samo djelomičnog slanje paketa s nižim prioritetom, koje onda treba ponovno poslati u cijelosti.

Ukoliko imamo preventivno raspoređivanje na kvantnoj razini, tada će se paketima u redu čekanja bez prioriteta, prvo dodijeliti prioritet,a prije nego se potpuno popuni red čekanja (što predstavlja neku količinu paketa) u potpunosti će ga poslužiti raspoređivač, ali bilo kojemu paketu, kojega trenutno poslužuje taj red, dopustit će se posluživanje do kraja. Ovaj pristup je učinkovit za širinu pojasa, ali može dovesti do većega kašnjenja za prioritetan red.

Praktične implementacije preventivnog raspoređivanja prioriteta rade na kvantnoj osnovi, tj. ako neki prioritetni red čekanja postane aktivan, onda će se taj prioritetni red čekanja poslužiti odmah nakon što se bilo koji ne-prioritetan paket koji se trenutno poslužuje, posluži do kraja. To osigurava da promet u prioritetnome redu ima ograničeno kašnjenje i varijacije kašnjenja. Ako paket stiže u prioritetan red čekanja, a red je prazan, on bi trebao čekati barem jedan paket iz drugoga reda čekanja, prije nego što ga raspoređivač posluži. U praksi, kašnjenje na prioritetnog reda može biti više od jednoga paketa zbog prisutnosti reda čekanja FIFO sučelja (kao što je opisano u predhodnom odjeljku).

Obzirom da se prioritetan red poslužuje prioritetom koji je viši od prioriteta drugih redova čekanja, ukoliko je prioritetan red stalno aktivan - to jest da uvijek ima pakete za slanje, tada ostali redovi čekanja mogu ostati bez ikakve širine pojasa. Kako bi to spriječili, uobičajena je praksa da se postavljaju pravila (policy) i za najveću dozvoljenu brzinu prometa prioritetnog reda čekanja. Ako je maksimalna dozvoljena brzina manja od raspoložive brzine same veze, onda će uvijek biti dostupne propusnosti za uporabu od strane drugih redova čekanja, bez obzira na opterećenje u prioritetnome redu. Nadalje, kontrolirajući ponuđeno opterećenje prioritetnoga reda čekanja, mogu mu se ograničiti kašnjenje, varijacije kašnjenja (*jitter*) i gubici.

Raspoređivanje temeljem ponderirane širine pojasa (Weighted Bandwidth Scheduling)
Ako prioritetan red čekanja nije aktivan - to jest, ne postoje paketi u redu čekanja - onda postoji niz drugih redova od koji su spremni za FIFO posluživanje. Ovi redovi će uglavnom biti posluživani na ponderiran način, gdje težinski faktor određuje ponuđenu uslugu jednoga reda

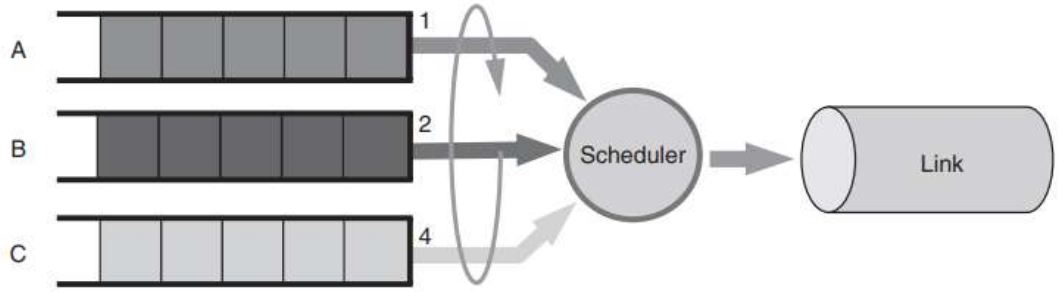
relativno u odnosu na druge redove, pa ponderiranje određuje međusobnu diobu širine pojasa linka među različitim redovima čekanja. Algoritam raspoređivanja se koristi za osiguranje tog relativnog posluživanje između redova čekanja. Kontrolom relativne razlike između brzina dolaska prometa i brzine posluživanja (a koju određuju ponderi) različitih redova čekanja, može se kontrolirati utjecaj stajanja u redu na kašnjenje, te se uvodi diferencijacija usluga u odnosu na ove redove čekanja.

Za napomenuti je da se redovi čekanja mogu dodijeliti diskretnim tj. pojedinačnim prometnim tokovima (kao u slučaju arhitekture integriranih usluga- IntServ) ili prometnim razredima (kao u slučaju arhitekture diferencijalnih usluga DiffServ). Zbog problema skaliranja (širenja) kod pridruživanja pojedinačnih tokova podataka redovima čekanja, češće se redovi čekanja određuju po prometnim „razredima tj. klasama“, gdje „razred tj. klasu“ stvara niz tokova koji imaju zajedničke SLA zahtjeve.

Ponderirani vrtuljak (Weighted Round Robin - WRR)
Ponderirani vrtuljak (WRR) je najjednostavniji primjer takvog ponderiranog algoritma za raspoređivanje. Rad WRR-a najlakše je objasniti na primjeru.

Primjer 1. Ponderirani vrtuljak

Uzet ćemo u obzir raspoređivač koji ima tri ponderirana reda čekanja (uz prioritetne redove čekanja) te ćemo ih označiti sa A, B i C te s težinskim faktorima od 1, 2 i 4 kako što je prikazano na slici ispod.



Slika 3: Primjer WRR raspoređivanja

U jednom krugu, raspoređivač obilazi svaki red čekanja i obrađuje količinu prometa iz tog reda određenu težinskim faktorom pojedinog reda. Dakle, u ovom primjeru, u svakom krugu, WRR raspoređivač obrađuje 1 paket, 2 paketa i 4 paketa iz redova A, B i C ponaosob. Ako se svi redovi neprestano puni (tj. ako brzina dolaska paketa neprestano premašuje brzinu obrađivanja), raspored reda će biti A, B, B, C, C, C, C, A, B, B, C, C, C,C, A...

U gore navedenom primjeru, ponderiranje usluge između redova je definiran u smislu paketa. Ako su svi paketi u različitim redovima iste veličine, onda je i raspodjela raspoložive ukupne propusnosti veze između redova također u istom omjeru. U ovom slučaju, ako je veza propusnosti 512 kb/s, redu A će biti dodjeljena $1/(1 + 2 + 4) \cdot 512 \approx 73$ kb/s, redu B će biti dodijeljena $2/(1 + 2 + 4) \cdot \approx 512$ 146 kb/s, a redu C $4/(1 + 2 + 4) \cdot 512 \approx 293$ kb/s. U postocima, propusnost veze će otprilike bit raspodijeljena ovako: red A – 14%, red B – 29 % i red C – 57%.

Dakle, raspoređivač pruža minimalno jamstvo propusnosti za redove čekanja.Ovo je minimalno jamstvo propusnosti bez obzira na prometno opterećenje (ali u ovom konkretno slučaju ne bez obzira na veličinu paketa kao što ćemo ubrzo vidjeti) u drugim redovima čekanja.

Ovisno i izvedbi određene opreme, neki proizvođači zahtijevaju da redovi budu konfigurirani prema svojim relativnim težinama, dok drugi dopuštaju konfiguraciju u smislu apsolutnog (na primjer kb/s) ili relativnog postotka osiguranja minimalnešširine pojasa koji se zatim pretvara u težinske faktore kako bi se programirao raspoređivač.

U WRR raspoređivaču, ako neki red nije aktivan, onda raspoređivač prelazi na sljedeći red i tako neiskorištenu propusnost neaktivnih redova raspoređuje na aktivne redove proporcionalno njihovim težinskim faktorima, tj. proporcionalno minimalnoj propusnosti reda. Da je red B u prošlom primjeru bio neaktivan, onda bi 146 kb/s osiguranja minimalne propusnosti za red B bilo raspoređeno između reda A i red C proporcionalno njihovim težinskim faktorima, tj., u omjeru 1:4. Tada bi redu A bilo dodijeljeno $73 + (146 \cdot 1/5) \approx 102$ kb/s a redu B $292 + (146 \cdot 4/5) \approx 410$ kb/s.

Raspoređivače koji imaju ove karakteristike – dopuštaju da se neiskorištena propusnost iskoristi u aktivnim redovima- nazivamo raspoređivači koji "održavaju rad". Oni miruju jedino onda kada nema paketa koji bi se poslao u redove: većina raspoređivača danas radi na ovakav način. U prethodnom primjeru, neiskorištena propusnost se prebacuje proporcionalno osiguranju minimalne propusnosti aktivnih redova: neke naprednije provedbe raspoređivanja podržavaju dodatne parametre koji dopuštaju redistribuciju neiskorištene propusnosti da bi se ona mogla konfigurirati neovisno o minimumu propusnosti nekog reda (CISCO).

Učinkovitost IP raspoređivača se mjeri bliskošću postignute i ciljane raspodjele propusnosti, a naziva se "pravičnost“(*fairness*) raspoređivača. U prethodnom primjeru, WRR je točan dok su god veličine paketa u različitim redovima jednake, te kada se gleda potpuni krug rada raspoređivača. Ako su prosječne veličine paketa u različitim redovima iste, onda će WRR biti u prosjeku točan. Ako prosječne veličine paketa u različitim redovima nisu iste, onda bi raspoređivač potencijalno mogao normalizirati težinski faktor reda u odnosu na prosječnu veličinu paketa svakog reda.

Primjer 2: Ponderirani vrtuljak

Kao nastavak prethodnog primjera, pretpostavit ćemo da su prosječne veličine paketa redova A, B i C 64 bajta, 1500 bajtova i 300 bajtova, a da veza ima 512 kb/s. Sa težinskim faktorima iz prethodnog primjera raspored propusnosti reda bi bio:

Red A: $512 \cdot (1 \cdot 64)/((1 \cdot 64) + (2 \cdot 1500) + (4 \cdot 300)) \approx 8$ kb/s

Red B: $512 \cdot (2 \cdot 1500)/((1 \cdot 64) + (2 \cdot 1500) + (4 \cdot 300)) \approx 360$ kb/s

Red C: $512 \cdot (4 \cdot 300)/((1 \cdot 64) + (2 \cdot 1500) + (4 \cdot 300)) \approx 144$ kb/s

Ako je ciljana relativna podjela propusnosti veze između redova 1:2:4, onda je očito daleko od poštene raspodjele!

Ako se normalizira težina svakog reda u odnosu na prosječnu veličinu paketa za taj red, i ako se uzima cjelobrojna vrijednost, onda su težinski faktori redova sljedeći:

Red A: težinski faktor = 1/64 = 15 x 10^{-3} = 150

Red B: težinski faktor = 2/1500 = 1,3 × 10^{-3} = 13

Red C: težinski faktor = 4/300 = 13 x 10^{-3} = 130

U praksi, međutim, može biti teško procijeniti kolika je prosječna veličina paketa u redu te može varirati tijekom vremena. U tim slučajevima, ograničenja jednostavnog WRR raspoređivača mogu doći do izražaja i očitovati se time da neki redovi mogu biti zakinuti za njihov dio propusnosti.

Napredniji raspoređivači su u mogućnosti savladati ovaj problem, a neki mogu i dostići "točnost" u vremenskim razdobljima manjim od cijelog kruga. Pravednost se mjeri usporedbom ponašanja raspoređivača prema idealiziranoj shemi Generaliziranog djeljenja procesa(Generalized Process Sharing - GPS). GPS raspoređivač obrađuje infinitezimalno malu količinu iz svakog reda u svakom krugu raspoređivanja; dakle, on obilazi sve aktivne redove u bilo kojem konačnom vremenskom intervalu i tako je pravedan u svakom vremenskom intervalu. Redovi imaju definiranu težinu te primaju usluge proporcionalne svojoj težini kad god su podaci u redu čekanja.

GPS raspoređivač je idealiziran u načinu da pretpostavlja da redovi mogu biti obrađeni u infinitezimalno malim količinama. Ovo očito nije moguće izvesti u praksi i za IP raspoređivače: najmanja jedinica koja može biti obrađena u redu je jedan paket; u vremenskom okviru u kojem se obrađuje jedan paket, raspoređivač mora biti nepravedan prema ostalim redovima. Dakle, realni raspoređivač paketa ne može biti pravedan kao GPS. U sljedeća dva odjeljka ćemo uzeti u obzir dvije praktične provedbe raspoređivanja koje se danas često koriste i kojima je cilj imitirati GPS shemu.

2.2.4.1.2.2 Ponderirani “pravedan” red čekanja (Weighted fair queuing-WFQ)

Ponderirani „pravedan ili pošteni“ red čekanja (WFQ) izračunava vrijeme u kojem će paket biti obrađen ako se obrađuje pomoću GPS sheme; nakon toga obrađuje pakete na temelju njihovog vremena završetka koje u stvari postaje redni broj. WFQ je GPS verzija koja se temelji na paketu. Razmotrimo sljedeći primjer.

Primjer 3: Ponderirani „pravedan“ red čekanja

Ako uzmemo u obzir raspoređivač koji ima 3 ponderirana reda (uz redove s prioritetom): A, B i C sa željenom relativnom raspodjelom propusnosti 1:2:4 (ili 14%, 29% i 57%). Pretpostavimo da su redovi A, B i C neprestano puni i da su veličine njihovih paketa 64 bajtova, 1500 bajtova i 300 bajtova i da veza ima propusnost 512 kb/s. Razmislimo kako bi bilo kad bi paketi dolazili odmah jedan iza drugoga u redoslijedu A1, A2, B1, C1, C2, C3, ... i to brže nego raspoređivač stigne obraditi prvi paket.

Kako bi se utvrdilo vrijeme obrade paketa, WFQ raspoređivač vodi računa o varijabli koja se zove okrugli broj. Ako sagledamo GPS raspoređivač koji obrađuje svaki red bajt po bajt a ne u infinitezimalno malim količinama, okrugli broj predstavlja broj ukupnih krugova obrade bajt po bajt koju je WFQ raspoređivač izvršio.

Kada paket stigne na prethodno neaktivni red, vrijeme njegove obrade (tj., redni broj) se izračunava tako što se uzima trenutno vrijeme obilaska i dodaje veličinu paketa pomnoženu sa težinskim faktorom reda; pa je stoga WFQ udio propusnosti reda obrnuto proporcionalan težinskom faktoru reda. U ovom slučaju, kako bi se postigao željeni udio propusnosti od 1:2:4, težinski faktori (ponderi) 4, 2 i 1 su dodijeljeni redovima A, B i C pojedinačno. Sa WFQ, aktivnost reda može se odrediti time postoje li kakvi paketi u redu kojem je redni broj veći nego trenutni broj obilazaka. Kad paket stigne na aktivni red, njegov redni broj se izračunava tako da se veličina dolaznog paketa pomnožena sa težinom reda doda najvišem rednom broju paketa koji je već uredu.

Razmotrimo da je trenutni broj krugova 0:

- Paket A1 stiže, redni broj paketa se izračunava kao $0 + 64 \cdot 4 = 256$
- Paket A2 stiže i, kako je red aktivan, redni broj paketa se izračunava kao $256 + 64 \cdot 4 = 512$
- Paket B1 stiže i , kako je red neaktivan, redni broj paketa se izračunava kao $0 +1500 \cdot 2 = 3000$
- Paket C1 stiže i , kako je red neaktivan, redni broj paketa se izračunava kao $0 + 300 \cdot 1 = 300$
- Paket C2 stiže i , kako je red aktivan, redni broj paketa se izračunava kao $300 + 300 \cdot 1 = 600$
- Paket C3 stiže i , kako je red aktivan, redni broj paketa se izračunava kao $600 + 300 \cdot 1 = 900$.

Raspoređivač prvo obrađuje paket s najmanjim rednim brojem i ažurira krug da bi bio jednak rednom broju tog paketa. Ako usporedimo redne brojeve primljenih paketa u ovom slučaju, vidjeti ćemo da su paketi primljeni u redoslijedu A1, A2, B1, C1, C2, C3, poslani u redoslijedu A1, C1, A2, C2, C3, B1.

Deficitni vrtuljak (Deficit Round Robin -DRR)
Deficitni vrtuljak (DRR) modificira WRR tako da može raspoređivati pošteno bez da zna prosječnu veličinu paketa u pojedinim redovima. To se postiže praćenjem brojila deficita svakog reda. DRR raspoređivač kružno obilazi svaki red i ima za cilj obraditi težinski faktor ili kvantnu vrijednost iz svakog reda. Za razliku od WRR, kvant se definira u bajtovima a ne u paketima. Kada neki red čekanja stigne na obradu, raspoređivač pokuša obraditi cijeli kvantum iz reda.

U praksi, malo je vjerojatno da će „kvantum“biti točno jednak veličini sljedećeg paketa, ili sljedećih nekoliko paketa na čelu reda. U ovom slučaju količina paketa koja će biti obrađena na prednjem dijelu reda ovisi o tome koliko će se cijelih paketa smjestiti kvantum; ako je prvi paket veći od raspoloživog kvantuma, onda ni jedan paket iz tog reda u tom krugu neće biti obrađen. Ako u redu ima više paketa nego što ih se može smjestiti u kvantum, neprenesena količina paketa iz reda čekanja u tom krugu raspoređivača će biti prenesena u sljedećikrug, inače će se brojač deficita resetirati. Na ovaj način će redovi koji nisu primili „pravedan“ udio u jednom krugu, rekompenzirati to u drugom krugu. Razmotrimo sljedeći primjer.

Primjer 4: Deficitni vrtuljak - DRR

Razmotrimo raspoređivač koji ima tri ponderirana reda (uz prioritetne redove) A, B i C čija je željena propusnost 1:2:4 (ili 14%, 29% i 57%) pojedinačno i imaju kvante od 100, 200 i 400 u skladu s tim. Pretpostavimo da su redovi A, B i C neprestano puni i da su veličine njihovih paketa 64 bajta, 1500 bajtova i 300 bajtova a da je veza 512 kb/s.

Svi brojači deficita redova čekanja su u početku postavljeni na nulu. U prvom krugu raspoređivača, kvantna količina podataka za red A je 100, a paketi imaju 64 bajta, tako da je količina kvantuma dovoljna da obradi jedan cijeli paket. Kako u redu A ima više paketa, ostatak količine će se prenijeti kao deficit u sljedeću rundu: u ovom slušaju, brojač deficita za red A će biti: 100 – 64=36 bajtova. Ovo će biti nadodano kvantumu reda u sljedećem krugu raspoređivača.

U prvom krugu, nakon reda A, DRR raspoređivač prelazi na red B; količina podataka kvantuma za red čekanja je 200 a paketi imaju 1500 bajtova, što bi značilo da nema dovoljno kvantuma da se obradi bilo koji paket pa se ostatak kvantuma prenosi dalje u novi krug kao deficit; u ovom slučaju brojač deficita za red B će iznositi 200 bajtova. Brojač deficita za red B se nastavlja povećavati do 8. kruga kada će brojač deficita + kvantum iznositi 1600 bajtova što bi značilo da će se samo jedan paket od 1500 bajtova obraditi. Kako u redu postoji još paketa od 1500 bajtova, brojač deficita će iznositi 1600 – 1500 = 100 bajtova i to će se prenijeti u krug 9.

U prvom krugu, nakon reda B kada DRR raspoređivač prelazi na red C; količina podataka kvantuma za red čekanja je 400 a veličina paketa 300 bajtova, tako da je kvantum dovoljan za obradu jednog cijelog paketa. Kako u redu C postoji još paketa, ostatak kvantuma se prenosi dalje u sljedeći krug kao deficit; u ovom slučaju, brojač deficita za red C će biti 400 – 300 = 100 bajtova. Ovo će se pridodati kvantumu reda u sljedećem krugu raspoređivača.

Tablica na slici ispod pokazuje status redova u smislu kvantnih paketa koji su poslani i deficita, i to u svakom krugu raspoređivača.

Red		Krug 1	Krug 2	Krug 3	Krug 4	Krug 5	Krug 6	Krug 7	Krug 8
A	Quantum	100	136	108	144	116	152	124	100
	Pkts sent	1*64B {A1}	2*64B {A2, A3}	1*64B {A4}	2*64B {A5, A6}	1*64B {A7}	2*64B {A8, A9}	2*64B {A10, A11}	1*64B {A12}
	Deficit	36	8	44	16	52	24		36
B	Quantum	200	400	600	800	1000	1200	1400	1600
	Pkts sent	0	0	0	0	0	0	0	1*1500B {B1}
	Deficit	200	400	600	800	1000	1200	1400	100
C	Quantum	400	500	600	400	500	600	400	500
	Pkts sent	1*300B {C1}	1*300B {C2}	2*300B {C3, C4}	1*300B {C5}	1*300B {C6}	2*300B {C7,C8}	1*300B {C9}	1*300B {C10}
	Deficit	100	200	0	100	200	0	100	200

Tijekom 8 krugova raspoređivanja, ukupan broj bajtova pridodanih svakom krugu biti će:

Red čekanja A: $12 \cdot 64 = 768$

Red čekanja B: $1 \cdot 1500 = 1500$

Red čekanja C: $10 \cdot 300 = 3000$

Ako dodajmo vrijednosti brojača deficita, možemo utvrditi efektivnu relativnu raspodjelu propusnosti za svaki red u svih 8 krugova:

Red čekanja A: $= (768 + 36)/((768 + 36) + (1500 + 100) + (3000 + 200)) \approx 14\%$

Red čekanja B: $= (1500 + 100)/((768 + 36) + (1500 + 100) + (3000 + 200)) \approx 29\%$

Red čekanja C: $= (3000 + 200)/((768 + 36) + (1500 + 100) + (3000 + 200)) \approx 57\%$

Dakle, možemo vidjeti da DRR prikazuje 'pravednost' bez obzira na veličinu paketa, ali tijekom više krugova raspoređivanja; što je više krugova uzeto u obzir, to je pravednije, a brojač deficita (koji predstavlja bajtove koji nisu još poslani u taj red) ima proporcionalno manji utjecaj.

Koji algoritam za raspoređivanje izabrati?
Algoritme za raspoređivanje razlikujemo po više značajki kao i mjesta gdje se koriste:

- Pravednost

Kao što je prethodno opisano, pravednost raspoređivača je mjera koliko točno raspoređivač postigne željenu raspodjelu propusnosti. Jasno, pravednost je poželjna karakteristika svakog raspoređivača. Stoga su DRR i WFQ IP algoritmi za raspoređivanje paketa koji se preferiraju više od WRR-a. WRR pruža pravednu raspodjelu propusnosti između redova samo ako su veličine paketa u različitim krugovima iste, što obično nije slučaj.

- Granice najgorih slučajeva kašnjenja

Neke izvedbe raspoređivača mogu pokušati podržati promet koji ima zahtjeve niskog kašnjenja iz reda pondrirane propusnosti, koja se obrađuje pomoću algoritma za raspoređivanje kao štoje WRR ili WFQ. Različiti algoritmi raspoređivanja koji djeluju na istom skupu redova će rezultirati različitim redom prijenosa paketa, čak i kada su konfigurirani da proizvedu istu željenu raspodjelu propusnosti.

Prema tome, granica najgorih slučajeva kašnjenja za pojedini red ovisi o tome koji se algoritam za raspoređivanje koristi. Također može biti ovisiti o broju redova koji se koriste u pojedinoj izvedbi. Nadalje, za neke algoritme raspoređivanja, težinski faktor koji ponderira red mora se umjetno podići da bi se smanjila granica najgoreg kašnjenja povećanjem brzine efektivnog raspoređivanja reda. Podizanjem propusnosti jedne klase, relativna propusnost dostupna drugim skupinama se može smanjiti, što bi rezultiralo u grubljoj relativnoj „zrnatosti“ raspodjele propusnosti za druge skupine. Stoga bi poželjno da se granica najgoreg slučaja kašnjenja pojedinog reda postavi što preciznije pravoj granici (da nemamo pretjerano osigueranje za kašnjenje).

U praktičnim izvedbama, međutim, promet koji ima niske zahtjeve kašnjenja se u većini slučajeva obrađuje pomoću prioritetnog reda, a ne redom sa ponderiranom propusnosti. Stoga, granica najgoreg slučaja kašnjenja za redove sa ponderiranom propusnosti ne mora biti kritična kad se bira algoritam za raspoređivanje.

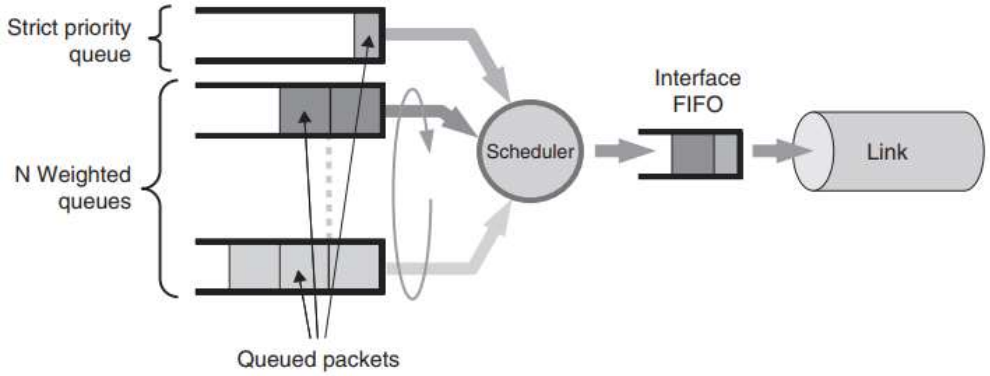
- Jednostavnost

Iz perspektive provedbe platforme, postoje prednosti algoritama koji su jednostavani za implementaciju; što su manji ciklusi i stanja kojisu potrebni za provedbu određenog algoritma, to je potrebno manje energije i memorije, te je stoga lakše širenje sustava, a smanjuje se i cijena. DRR je manje računalno intenzivan i jednostavniji za provedbu nego WFQ, stoga se općenito preferira u slučajevima u kojima je potreban visoka razina mogućnosti nadogradnje (proširenja) platforme, bilo da je riječ o brzim vezama ili o velikom broju veza s niskom brzinom.

Iako postoje i drugi algoritmi za raspoređivanje koji se koriste u IP mrežama, mi smo opisali one koji se daleko najčešće koriste zajedno sa ključnim značajkama koje određuju gdje će se različiti algoritmi koristiti.

FIFO sučelje
Za većinu praktičnih usmjerivačkih primjena, raspoređivač zapravo neće obrađivati redove direktno na fizičkoj vezi, već će obrađivati redove koji mu pripadaju u redu linijskog

hardverskog pokretača na sučelju izlaznoj linije. Ovaj red služi za pružanje međupohrane (*buffering*) prije nego linijski hardver pokretač dopusti linijskom pokretaču da maksimalno poveća propusnost sučelja. Ovo je FIFO red koji je još poznat i kao FIFO sučelje ili spremnik prijenosnog prstena (kraće tx-ring) i koji je prikazan na slici ispod.



Slika 4: FIFO sučelje

Ako raspoređivač može ukloniti pakete iz reda čekanja u FIFO sučelju brže nego što će biti obrađeni (tj., brže od propusnosti veze), onda će se prijenosna prsten međumemorija početi puniti. Uobičajeno je da se mehanizmi kontrole protoka implementiraju da bi se osiguralo da se FIFO sučelje ne nastavi puniti nekontrolirano, nego kad broj paketa u redu u FIFO sučelju počne prelaziti definirani prag, kontrola protoka će zaustaviti daljnje raspoređivanje paketa (ovo je poznato kao "gašenje protoka"). Kad broj paketa u redu FIFO međumemorije padne ispod praga (koji mora biti jednak ili niži od praga "gašenja protoka"), mehanizmi kontrole protoka dopuštaju raspoređivaču da ponovno šalje pakete u FIFO sučelje (ovo je poznato kao "paljenje protoka").

Ova vrsta kontrole protoka se ponekad naziva "stražnji pritisak" izvršen iz FIFO sučelja na raspoređivač. Stoga paketi koji više nisu u redu čekanja raspoređivača mogu biti stavljeni u red čekanja iza paketa koji su već u FIFO sučelju. Čak se i prioritetni paket može vratiti u red čekanja na repu FIFO sučelja i stoga veličina FIFO sučelja može utjecati na kašnjenja reda čekanja raspoređivača. Stoga je važno da veličina FIFO sučelja nije nepotrebno velika.

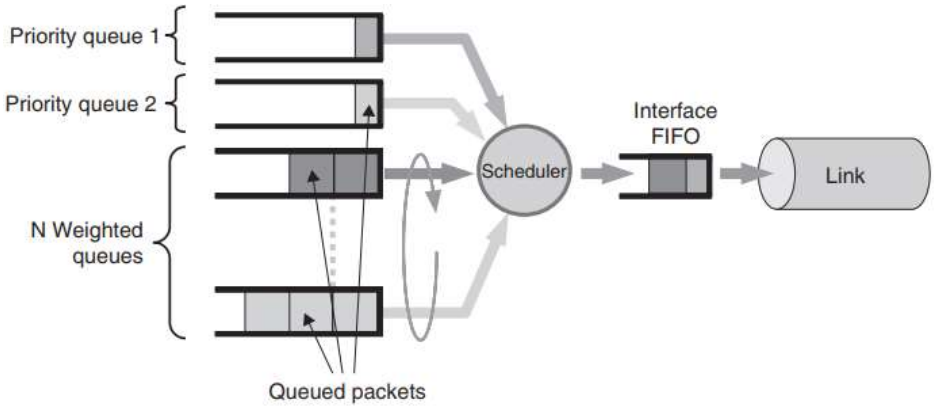
Utjecaj čak i razumne veličine FIFO sučelja na kašnjenje prioritetnih redova može ukazivati na nedovoljnu brzinu pristupnih veza; optimalno bi trebao biti podešen na 1–na-2 MTU-a, gdje se jedan paket odašilje na vezu, dok se drugi paket postavlja paralelno na FIFO sučelje. Ako kašnjenje uvedeno FIFO sučeljem prelazi ciljano kašnjenje prometa u prioritetnom redu, onda je možda potrebno uvesti fragmentaciju i *interleaving*na razini veze, kao što će biti opisano u slijedećem odjeljku. Pri vezama većih brzina, tj., u jezgrenoj mreži, utjecaj kašnjenja FIFO sučelja će uglavnom biti zanemariv.

Napredni koncepti u raspoređivanju: Višeslojni strogi prioritet

Neke unaprijeđene implementacije raspoređivača dodatno podržavaju više od jedanog prioritetnog reda. Potražnja koja uvodi ove zahtjeve je istodobna podrška za glasovne i video usluge. Kako je opisano u početnim poglavljima, glasovne usluge općenito imaju strože zahtjeve kašnjenja od prijenosa video usluga, iako video usluge također imaju granice kašnjenja usluge. Osim toga, video aplikacije često koriste velike pakete kako bi efikasnije koristile propusnost veze.

U alternativnom razvojnom pristupu, kod korištenja istog raspoređivača, jedan od redova sa ponderiranom propusnosti može biti iskorišten za potporu video prometa. U ovom slučaju, kao što je opisano, granica kašnjenja koju će video promet doživjeti može varirati ovisno o tome koji se raspoređivač koristi te može također ovisiti o broju drugih redova sa ponderiranom propusnosti koji se koriste u određenoj implementaciji. Promet u tim redovima, na niskim brzinama veze može zakazati u postizanju željenih ciljeva kašnjenja. Nadalje, za neke algoritme raspoređivanja, težinski faktor koji se primjenjuje za redove može biti umjetno povećan da bi se smanjilo najgori slučaj kašnjenja veze. Podizanjem propusnosti jedne grupe, relativni udio propusnosti dostupan drugim grupama se smanjuje, što može rezultirati u grubljoj relativnoj zrnatosti raspodjele propusnosti drugim grupama.

Da bi se ovi problemi izbjegli, neke naprednije implementacije raspoređivanja koje pružaju podršku za više od jedan prioritetni red su prikazane na slici ispod.



Slika 5: Više prioritetnih redova

Prioritetni red s najvećim prioritetom obrađuje se linijskom brzinom čim postane aktivan: jednom kada je ovaj red obrađen, počinje se uslužiti slijedeći prioriteni red. Konačno, nakon što se obradi i drugi po redu prioritetni red, redovi ponderirane propusnosti bivaju sljedeći. Kada se podržava glas i video, na primjer, korištenje najvišeg prioritetnog reda za glasovni promet i sljedećeg prioritetnog reda za video promet će omogućiti da glasovni promet primi najniže kašnjenje i *jitter*, dok će video promet imati veće kašnjenje i *jitter* ali oni neće ovisiti o konfiguraciju i opterećenju redova sa ponderiranom propusnosti. S multi prioritetnim implementacijama raspoređivača kao što su ove, kašnjenje i *jitter* prometa obje razine prioriteta može biti ograničeno i stoga su obje razine prioritetnog reda u skladu sa konceptom Diferencijalnih usluga (Diffserv).

Odbacivanje

U ovom trenutku, prije nego počnemo razmatrati odbacivanje, važno je istaknuti razliku između međumemorije (*buffer*) i reda čekanja (*queue*). Međumemorija je fizička lokacija memorije gdje se paketi privremeno pohranjuju dok čekaju da budu preneseni. Redovi, na drugu stranu, ne sadrže pakete iako je uobičajeno reći "paketi u redu". Red se sastoji od uređene skupine pokazivača lokacije u međumemoriji gdje su paketi u tom pojedinom redu pohranjeni. Brza međumemorija je često skupi dio usmjerivača i stoga se međumemorija može dijeliti

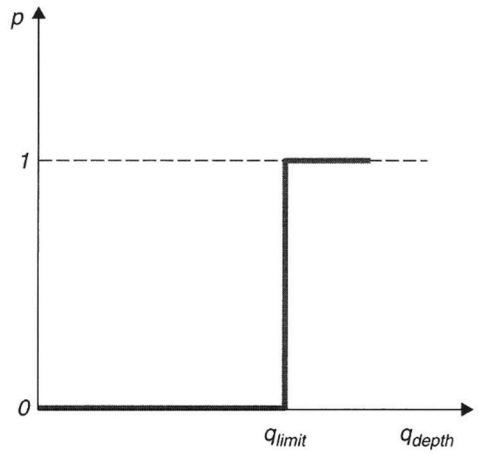
među svim redovima, a nije strogo fizički podijeljenamеđu redovima. Međumemorija može biti organizirana u blokove fiksne veličine (koji mogu biti poznati kao čestice), obično 256-512 bajtova, kako bi se olakšalo brzo pretraživanje memorije što povećava učinkovitost korištenja memorije. Na primjer, ako sistem koristi čestice od 256 bajtova, paket od 576 bajtova troši tri čestice u međumemoriji.

Ako dolazna brzina prometa neprestano premašuje dostupnu propusnost veze, onda broj paketa u najmanje jednom od redova mora neprestano rasti. Kako veličina međumemorije mora biti konačna, u nekom trenutku, dubina reda mora preći dostupnu međumemoriju, te je neizbježno da paketi budu odbačeni. Važno je da usmjerivači imaju dovoljno memorije kako bi mogli pohraniti pakete koji su u redu čekanja u skladu s konfiguriranom Diffserv politikom. Nedostatak memorije u usmjerivaču može dovesti do odbacivanja paketa sa uzrokom „no buffer“ koji se javljaju bez obzira na klasu prometa što rezultira povredom SLA obaveza. Primjena ograničenja „dubine“ pojedinih redova ima utjecaj na pad efikasnosti korištenja memorije.

U praksi današnje usmjerivačke platforme imaju dovoljno memorije pa njena veličina nije ograničavajući faktor za dubine pojedinog reda. Glavni razlozi za ograničavanje ili upravljanje dubinama redova su ili ograničenja kašnjenja paketa u redu, ili pokušaj optimiziranja postignutog protoka za promet u redu. Različite tehnike odbacivanja se primjenjuju ovisno o cilju.

Odbacivanje repa (Tail drop)

Mehanizam odbacivanja repa se koristi kod postavljanjaoštre granice broja paketa koji mogu biti u redu. Prije nego paket dođe na rep reda, provjerava se trenutna dubina paketa u redu i ako dubina reda prelazi maksimalni limit za taj red, što se obično navodi u bajtovima, onda će paket biti odbačen a ne stavljen u red na čekanje. Možemo pretpostaviti da je vjerojatnost odbacivanja paketa mala, dok je dubina reda manja od limita, ali kad se dosegne limit vjerojatnost odbacivanja je 100%, kako je prikazano u grafikonu vjerojatnosti odbacivanja u slici ispod.



Slika 6: Vjerojatnost odbacivanja paketa

Postavljanje maksimalnog limita reda se može koristiti za postavljanje maksimalne granice za kašnjenje prometa u redu. Zašto bi željeli postaviti takvu granicu kašnjenja u redu? Nije li bolje,

ako smo u mogućnosti, poslati paket a ne ga odbaciti? Odgovor na ova pitanja ovisi o aplikaciji. Ako se vratimo usporedbi s prijavom u zrakoplovnoj luci, ako red na prijavi postane predug, onda kašnjenje može premašiti vrijeme polaska aviona, pa u ovom slučaju nema smisla da putnici čekaju jer će ionako zakasniti na avion. Isto tako, u slučaju nekih aplikacija kao što je VoIP, ako paket kasni previše, neće biti od koristi i bolje ga je odbaciti nego njime gušiti propusnost mreže te ga odbaciti na odredištu.

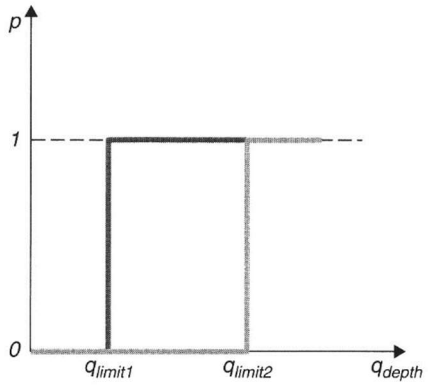
Ako je brzina obrade reda poznata, kao i maksimalna većina reda, onda se može odrediti i najgora granica kašnjenja paketa u redu. Ako je, na primjer, brzina obrade za red 2 Mb/s, a maksimalni limit reda 4 kilobajta, onda je najgora granica kašnjenja paketa postavljenog u red čekanja oko $4096 \cdot 8/2048000 \approx 16$ ms. Ako je utvrđeno da je maksimalno kašnjenje po skoku koje aplikacija može podnijeti 16 ms, onda ovo može biti parametar maksimalne dubine reda. Ovo je bio pojednostavljeni primjer, a u praksi mogu postojati i druga kašnjenja osim samo kašnjenja zbog čekanja u redu, pa je potrebno provesti znatno dublje analize kašnjenja.

Odbacivanje čela (poznat i kao "prednji pad" ili DFF) je moguća alternativa odbacivanju repa. Kod odbacivanja čela paketi se odbacuju sa početku reda a ne sa kraja (repa), kada dubina reda prelazi konfigurirani maksimalni limit reda. Lakshman je pokazao da odbacivanje čela poboljšava izvedbu TCP-a dopuštajući signalu indikacije zagušenja da stigne do pošiljatelja bez čekanja da se prvo prenese cijeli red. Head drop, međutim uglavnom je bio predmetom akademskih istraživanja i nije podržan od strane proizvođača usmjerivača, tako da ga nećemo dalje uzimati u obzir.

Ponderirano odbacivanje repa (*Weighted Tail Drop*)

Neke implementacije stavljanja paketa u red podržavaju više od jednog limita unutar istog reda.Ovo se nekad naziva „ponderirano odbacivanje repa“(*weighted tail drop*). Koncept iza ovoga jest taj da ako u redu postoji zagušenje- tj., brzina dolaska prometa Ra premašuje Rs brzinu usluživanja, onda se počinje stvarati dubina reda, te će neki od podskupova prometa u redu biti preferencijalno odbačeni.Brzina dolaska prometa koji će biti odbačen jest Ra1, a ostatak je Ra2, tako da Ra= Ra1+Ra2. Promet koji će preferencijalno biti odbačen može biti klasificiran različito u odnosu na ostatak prometa. Promet može biti diferencijalno označen kao „unutar“ ili „van ugovora“, koristeći nadglednik opisan u predhodnim odjeljcima.

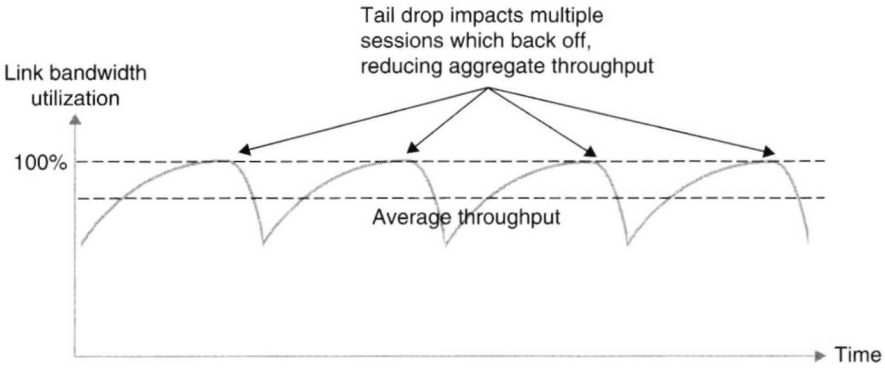
Preferencijalno odbacivanje se postiže primjenom nižeg limita reda **qlimit1** na podskup prometa koji će se odbaciti prvi, dok se za ostali promet koristi limit reda **qlimit2**. Ako je brzina dolaska za ostatak prometa Ra2 manja nego brzina usluge reda Rs, a prasaktog prometa manji nego razlika između dvaju limita reda (qlimit2 − qlimit1), onda će kod pojave zagušenja samo promet iz podskupa sa preferencijalnim odbacivanjem, biti ispušten. Ova shema je prikazana grafikonom vjerojatnosti odbacivanja na slici ispod.



Slika 7: Ponderirano odbacivanje repa

Slučajno rano otkrivanje (Random Early Detection)

Slučajno rano otkrivanje (Random early detection (RED)) je mehanizam aktivnog upravljanja reda čekanja (AQM). AQM mehanizmi otkrivaju zagušenje prije prekoračenja rednih limita (tj. prije nego što se dogodi odbacivanje repa), te osiguravaju povratnu informaciju pošiljatelju o ovom zagušenju u krajnjim sistemima, sa ciljem izbjegavanja suvišnog gubitka paketa zbog zagušenja te održavanja visokog mrežnog protoka uz minimiziranje kašnjenja u redovima. Dakle, AQM mehanizmi su također poznati kao tehnike „izbjegavanja zagušenja“. RED je originalno bio dizajniran kao algoritam usmjeren na poboljšavanje protoka za TCP-bazirane sjednice, sprječavanjem pojave „globalne sinkronizacije“ između TCP sesija. Globalna sinkronizacija je ponašanje koje se može pojaviti tamo gdje su paketi TCP sjednice nakupljene na jednoj vezi (ili redu), a kada se desi zagušenje, limit reda je premašen, što uzrokuje odbacivanje paketa višestrukih TCP sesija. TCP zbog svoje adaptivne prirode, reagira na način da kada shvati da su paketi odbačeni, smanjuje svoju brzinu slanja, te zagušenje tako jenjava, aukupni efektivni protok podataka pada ispod brzine linije. Budući da sada nema zagušenja, nema gubitaka paketa, pa sve sjednice opet povećavaju svoju brzinu slanja dok se ponovno ne dogodi zagušenje i ciklus se ponavlja. Ovakvo ponašanje kreira karakteristiku gregatnog protoka u obliku zubaca pile, kao što je prikazano na slici ispod.



Slika 8: TCP „globalna sinkronizacija“

RED cilja na pokušavanje prevencije globalne sinkronizacije na način da pamti prosječnu dubinu reda i koristi je kao indikator približavanja. Ovdje se radije prati prosječna dubina reda nego stvarna dubina (koja se koristi kod odbacivanja repa), da bi se prilagodilipraskovitom

ponašanju TCP prometa. Kako se povećava prosječna dubina reda, ova indikacija zagušenja šalje se natrag krajnjim sustavima putem nasumičnoodbačenih paketa iz pojedinačnih sjednica, radije nego da se kasnije odbacuju paketisvih sjednica. Cilj ovoga pristupa je potaknuti individualne sjednice na smanjenje brzine slanja kako bi se reduciraoukupni protok paketa na kontrolirani način, tako da se u prosjeku postigne viši agregatni protok i izbjegne karakteristika zuba pile.

RED donosi odluku o ispuštanju prije stavljanja paketa u red, baziranu na trenutnoj prosječnoj dubini reda tog reda i na skupu od četiri parametra, koji se mogu konfigurirati u većini implementacija:

Prosječna dubina reda (qavg) se izračunava pomoću sljedeće formule:

$$q_{avg} = q_{avg\_old} \times \left(1 - \frac{1}{2^w}\right) + \left(q_{current} \times \frac{1}{2^w}\right)$$

gdje je:

qavg_old = prethodno izračunata prosječna dubina reda

qcurrent = trenutna (ne prosječna) dubina reda

w = eksponencijalna težinska konstanta

RED koristi eksponencijalni ponderirani pomični prosjek; eksponencijalna težinska konstanta (w, što je normalnopodesiva) određuje koliko će točno prosječna dubina reda pratiti stvarnu dubinu reda; što je w niži, prosječna dubina reda će pratiti stvarnu dubinu reda točnije, tj. RED će biti osjetljiviji na praskove prometa.

- Ako je trenutna prosječna dubina reda (q_{avg}) ispod konfiguriranog minimalnog praga (q_{minth}), paket se stavlja u red

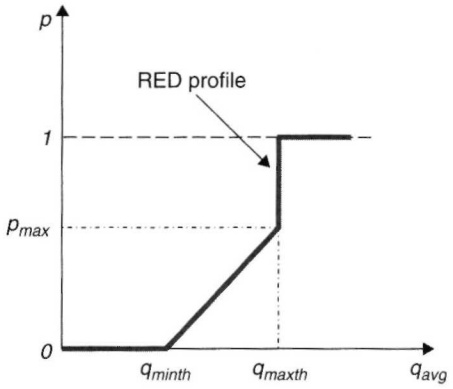
- Ako je trenutna prosječna dubina reda (qavg) iznad definiranog maksimalnog praga (q_{maxth}) onda se paket uvijek ispušta; ovo se naziva „prisiljeno ispuštanje“

- Ako je trenutna prosječna dubina reda (qavg) iznad qminth i ispod qmaxth paket može biti odbačen sa povećavajućom, ali nasumičnom, vjerojatnošću.Ovo se naziva „slučajno odbacivanje“ a vjerojatnost nasumičnog odbacivanja (p) se određuje sljedećom formulom:

$$p = \left(\frac{q_{avg} - q_{minth}}{q_{maxth} - q_{minth}}\right) \times P_{max} \times RAND(1)$$

Gdje je p_{max} vjerojatnost gubitka paketa pri q_{maxth}, što utječe na to koliko brzo se vjerojatnost odbacivanja paketa povećava između q_{minth} i q_{maxth}.

RED odbacivanje prikazano je grafikonom vjerojatnosti na slici ispod, gdje izabrani specifični parametri definiraju određeni profil RED odbacivanja.



Slika 9: RED odbacivanje

Poboljšanje RED-a je bilo predloženo u „Red-Light“ [JACOBSON] te se koristi u nekim implementacijama. RED-LIGHT nema koncept konfiguriranja konstante eksponencijalnog ponderiranja. Daljnja poboljšanja RED-a predložena su u [FLOYD2].

Široka upotreba RED-a savjetovana je u [RFC 2309], međutim, u praksi je teško odrediti prednosti RED-a. AQM je bio popularna tema znanstvenih studija a neka istraživanja nisu savjetovala upotrebu RED-a [MAY]. Također je predloženo više novih algoritama za AQM; [BITORIKA] bilježi da je više od 50 novih algoritama predloženo samo između 1999. i 2003. godine. U praksi, ni jedna od ovih shema nije danas u širokoj upotrebi te RED i dalje ostaje najkorišteniji AQM algoritam implementiran od proizvođača usmjerivača, te najčešće implementiran u mrežama.

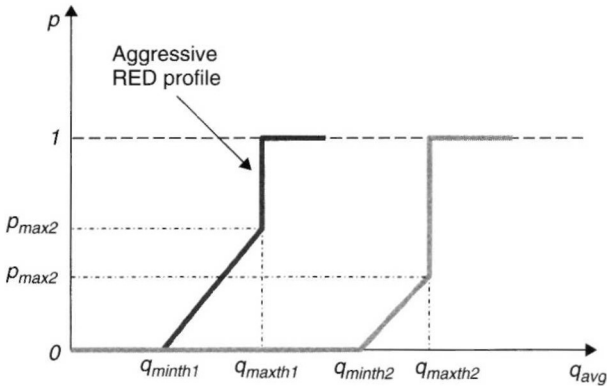
RED je dizajniran za TCP te se kao takav koristi za redove koji nose TCP aplikacije. RED nije namijenjen upotrebi sa neelastičnim aplikacijama kao što su VoIP ili video, koji obično koriste UDP, budući da se ove aplikacije ne mogu prilagoditi RED odbacivanjima paketa. Nadalje, kod aplikacija kao što su glasovne i video usluge, općenito je bolje imati ograničenje najgoreg slučaja kašnjenja uspostavljeno sa čvrstim limitom dubine reda. Sa RED-om, međutim, maksimalna dubina reda ovisna je o maksimalnom pragu i trenutnoj prosječnoj dubini reda, stoga trenutna maksimalna dubina reda može biti značajno veća nego maksimalni prag pagranica najgoreg slučaja kašnjenja reda može biti teško odrediva.

Postoje neke elastične aplikacije koje koriste UDP radije nego TCP, kao što je npr. Protokol Prijenosa Nevažnih Dokumenata (Trivial File Tranfer Protocol (TFTP)). UDP nema nikakvu implicitnu pouzdanost ili ugrađene mehanizme kontrole toka, dakle ako su potrebne trebaju biti ugrađene u aplikacije. Za ovakve aplikacije potrebna su detaljna poznavanja specifičnih implementacija aplikacija, da bi se razumjelo kakav bi utjecaj RED imao na njih; međutim, općenito izvedba sa RED-om ne bi trebala biti značajno lošija nego sa odbacivanjem repa.

Ponderirana slučajna rana detekcija (*Weighted RED-WRED*)

Ponderirani RED (WRED) proširuje osnovni koncept RED-a, dopuštajući da se više različitih RED profila koristi za isti red, gdje se svaki profil može primijeniti na različiti podskup prometa koji je određen za red. Koncept je vrlo sličan ponderiranom odbacivanju repa po tome što ako se u redu događa zagušenje, neki će podskupovi prometa u redu biti odbačeni. Ovo se postiže

pomoću agresivnijeg WRED profila (niže vrijednosti qminth i qmaxth) za promet koji će biti odbačen prvi. Promet koji će biti preferencijalno odbačen može npr. biti označen pomoću različitih oznaka nego ostatak promet.Promet može biti diferencijalno označen kao „unutar“ ili „van-ugovorni“ pomoću nadglednika opisanog u predhodnim odjeljcima. Ponašanje WRED odbacivanja prikazana su pomoću grafikona vjerojatnosti odbacivanja na slici ispod.



Slika10: Profil odbacivanjaWRED-a

Oblikovanje (Shaping)

Oblikovanje je, slično kao i nadgledavanje (policing), mehanizam koji se može koristiti kako bi se osiguralo da je prometni tok ne prelazi definiranu maksimalnu brzinu. Isto kao i kod nadglednika, oblikovatelj (*shaper*) se može predočiti kao mehanizam spremnika žetona kao što je to prikazano na slici ispod, s definiranom najvećom dubinom (obično u bajtovima), poznat kao prasak B i definiranom brzinom R (obično u bit/s) u kojem se spremnik puni žetonima veličine bajta. Ovisno o provedbi određenoga oblikovatelja, žetoni se dodaju u spremnik ili svaki put kad oblikovatelj obrađuje paket, ili u redovitim intervalima, do maksimalnoga broja žetona koji mogu biti u spremniku, što definira B. Minimalan broj žetona u spremniku je nula.

Razlika između oblikovatelja i nadzornika postaje očita kada razmotrimo što se događa kada se oblikovatelj primjenjuje na prometni tok. Kad paket stigne iz toga toka, veličina paketa b uspoređuje se s brojem žetona koji su trenutno u spremniku. Ako postoji barem toliko bajt žetona u spremniku koliko postoji bajtova u paketu, onda se paket prenosi bez odgode.

Ako ima manje žetona u spremniku nego bajtova u paketu, onda se paket usporava (tj. stavlja u red čekanja, stoga se oblikovatelji implicitno koriste zajedno s redovima čekanja) sve dok ne bude dovoljno žetona u spremniku. Kada ima dovoljno žetona u spremniku, paket se šalje i spremnik se smanjuje za broj žetona koji je jednak broju bajtova u paketu.

U tome smislu oblikovatelj se značajno razlikuje od nadglednika, koja djeluje na odbacivanje ili označavanje neprilagođenoga prometa, a ne na usporavanje. Nadglednik se može smatrati posebnim slučajem oblikovatelja reda čekanja sa maksimalnom duljinom reda čekanja od nula paketa. Dakle, dok nadgledanje odrezuje vrhove praskovitoga prometa, oblikovanje ujednačava prometni profil usporavanjem (unošenjem kašnjenja) vršnoga prometa.

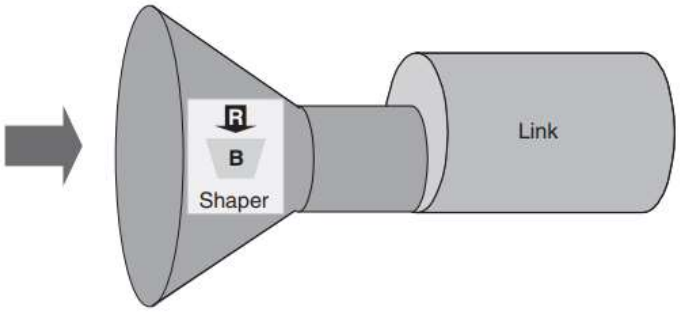
Spomenuto je da se svi oblikovatelji ne trebaju primijeniti s mehanizmom spremnika žetona. Drugi mehanizam koji se koristi za oblikovanje je spremnik s otjecanjem (*leaky bucket*). Često

se miješaju spremnici s otjecanjem i spremnici žetona, ali među njima postoje značajne i temeljne razlike.

Algoritmom spremnika s otjecanjem, može se vizualizirati da se paketi, a ne žetoni pohranjuju su u spremnik. Dolazni paketi se smještaju u spremnik koji ima „rupu na dnu“. Dubina spremnika s otjecanjem B, određuje maksimalan broj paketa koji se mogu spremiti u red čekanja u spremniku (isti je učinak kao ograničenje reda čekanja, primijenjeno na red čekanja predstavljen spremnikom). Ako paket stigne kada je spremnik već pun, paket se odbacuje. Paketi „istječu“ iz rupe u spremniku (tj. prenose se) konstantnom brzinom R, čime se „peglaju“ prometni praskovi. Najpoznatiji primjer algoritma spremnika s otjecanjem (*leaky bucket*) je generički algoritam brzine ćelija GCRA (Generic Cell Rate Algorithm) koji se koristi u prometnome oblikovanju ATM mreža [GCRA].

Raspoređivači u stvarnome vremenu koji određuju vremena izlaska paketa iz redova čekanja umjesto samog određivanja relativnog rasporeda odašiljanja, također se mogu koristiti za oblikovanje prometnih tokova. Takvi raspoređivači ne rade u modu konstantnog odžavanja rada(*non-work-conserving*), tj. mogu biti u stanju mirovanja (ne šalju promet) čak i kada postoji promet za slanje, kako bi oblikovali prometni tok. Većina praktičnih primjena oblikovanja IP prometa danas, temelji se na mehanizmima spremnika žetona. Napomenimo da, iako postoje standardizirane definicije oblikovatelja za ATM (Asynchronous Transver Mode) i FR (Frame Relay), ne postoje takve standardizirane definicije za IP.

Oblikovatelj se može primijeniti za provođenje limita maksimalne brzine za sve vrste prometa na fizičkome ili logičkome sučelju kao što je prikazano na slici ispod.

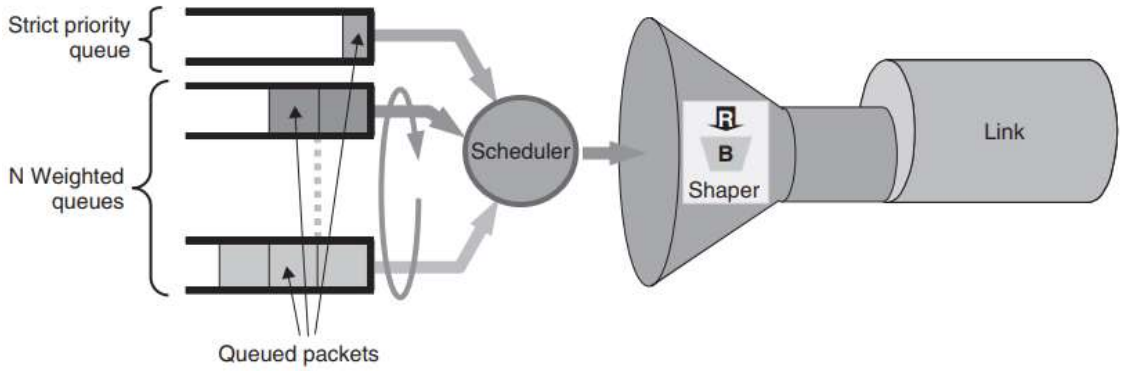


Slika 11: Skupni oblikovatelj (Aggregate shaper)

Na primjer, ovo bi se moglo iskoristiti za ponudu usluge pod-brzine (sub-rate), tamo gdje kupac od davatelja usluga kupuje uslugu povezivanja neke lokacije koja nije jako opterećena prometom. Davatelji usluga u svojim paketima vrlo često definirju združenu ostvarenu brzinu (tj. u svim razredima) za pristupnu vezu koja je u ovom slučaju prevelika u odnosu na zahtjeve kupca. Davatelj usluga može osigurati traženu uslugu, bilo fizičkimodabirom neke sporije veze prema ugovorenoj brzini, ili alternativno osiguravanjem veze veće brzine pristupa uz oblikovanjem prometa na tome linku prema ugovorenoj ukupnoj brzini po korisniku, koja bi bila ispod maksimalne brzine linka. Na taj način oblikovatelj može djelovati kao umjetno usko grlo, ograničavajući korisnički promet.

Alternativno, oblikovatelj se može primijeniti za provođenje limita maksimalne brzine za pojedine prometne razrede (klase). U tome slučaju, usporen promet nekog razreda će se staviti

u red čekanja za taj razred. Oblikovatelj se također može primijeniti na ukupnom (agregatnom tj. skupnom) prometnome toku koji se sastoji od brojnih razreda. U ovome slučaju, važno je da se oblikovatelj kombinira s raspoređivačem, kao što je prikazano na slici ispod.



Slika 12: Skupni oblikovatelj s raspoređivačem razreda

Tako da ako brzina skupnog prometa dosegne oblikovanu brzinu, promet se uspori s redom čekanja za svaki razred, a raspoređivač određuje redoslijed kojim će se ti redovi servisirati oblikovanom brzinom, osiguravajući razlikovanje između različitih prometnih razreda.

Primjer prikazan na prethodnoj slicije najjednostavniji oblik hijerarhije raspoređivanje/oblikovanje. Prema tome, oblikovatelj i raspoređivač su u relacijskome odnosu roditelj/dijete, gdje su pravila raspoređivanja „dijete“, a pravila oblikovanja „roditelj“. Neke implementacije mogu zahtijevati dodatne razine oblikovanja i raspoređivanja.

Fragmentacija veze i preplet (interleaving)

Čak i sa striktno prioritetnim raspoređivačem za promet osjetljiv na kašnjenje, kao što je VoIP, novopridošli prioritetni paket može u najboljem slučaju biti stavljen u red nakon raspoređivanja zadnjeg paketa. Kod relativno malih brzinaveze, jedan 1500 bajtni (maksimalna jedinica prijenosa za Ethernet) neprioritetni paket raspoređen neposredno prije nego što stigne prioriteni paket može imati značajan utjecaj na kašnjenje prioritetog paketa. Za 512 kb/s vezu ovo bi bilo ~23 ms, što prelazi ciljanu vrijednost od 15ms maksimalno prihvatljivogkašnjenja pristupne veze za VoIP klasu, izvedenu iz primjera koji je dan u prethodnom poglavlju. U praktičnim primjenama problem može biti i gori, sa nekoliko neprioritetnih paketa koji su potencijalno postavljeni u red prije prioritenog paketa, zbog prisutnosti FIFO sučelja.

Promotrimo, npr., da je određena implementacija reda dizajnirana tako da ako paket iz prioritetnog reda stigne kada je prioritetni red prazan, najviše 2 neprioritena paketa mogu biti uslužena prije tog paketa prioritenog reda; tj. maksimalna veličina FIFO sučelja je 2 paketa, što je reprezentativan primjer praktične implementacije. Ako se ova implementacija koristi na vezi od 512 kb/s, te uz pretpostavku neprioritenih paketa od 1500 bajtova, tada i ako prioriteni paket stigne u prioritetni red kada je prazan, prioritetni paket može čekati do ($2 \cdot 1500 \cdot 8/512000$) ≈ 47 ms prije nego što se ga se uopće počne slati ka sučelju. Ovo bi značajno premašilo tipični predviđeni segment kašnjenja pristupnih veza i zauzelo značajan dio ukupno predviđenog kašnjenja od-kraja-do kraja.

U takvim slučajevima nužna je primjena mehanizama fragmentacijena sloju veze i prepletanja (*interleaving*) (LFI) , a koji trebaju smanjiti učinak neprioritenih paketa na kašnjenje prioritetnog prometa. Fragmentacija slojeva veze razbija velike neprioritetne pakete u manje fragmente sa kojima se prioriteni paketi mogu preplesti (*interleaving*), a ne da moraju čekati prijenos cijelih neprioritenih paketa.

Dakle, fragmentacija slojeva veze smanjuje utjecaj na kašnjenje uzrokovan neprioritetnim paketima. Svaki fragment se transportira kao jedinstveni okvir sloja 2, koji sadržava identifikator koji im omogućuje da ih razlikujemo od prioritetnih paketa, i slijedni broj koji omogućuje ponovno slaganje fragmenata u cijele pakete na kraju veze. Tipične LFI implementacije imaju konfigurabilnu veličinu fragmenta tako da će neprioritetni paketi koji su veći od te veličine biti razbijeni u fragmente veličine do te određene veličine.

Promotrite prethodni primjer ali uz korišrtenje LFI tehnike sa veličinom fragmenta od 300 bajtova.Ako paket prioritetnog reda stigne u prazni prioritetni red bio bi sada odgođen samo sa $2 \cdot 300$ bajtova fragmenata u FIFO sučelju, tj. $2 \cdot 300 \cdot 8/512000 \approx 9$ ms prije nego što bi se počeo slati van sučelja, što bi bilo u skladu sa predvidviđenim maksimalnim kašnjenje. Iako se fragmentacija IP sloja može koristiti na sličan način, ima mnogo mana [SHANNON], te se stoga ne preporučuje, već se koristi samo na drugom sloju.

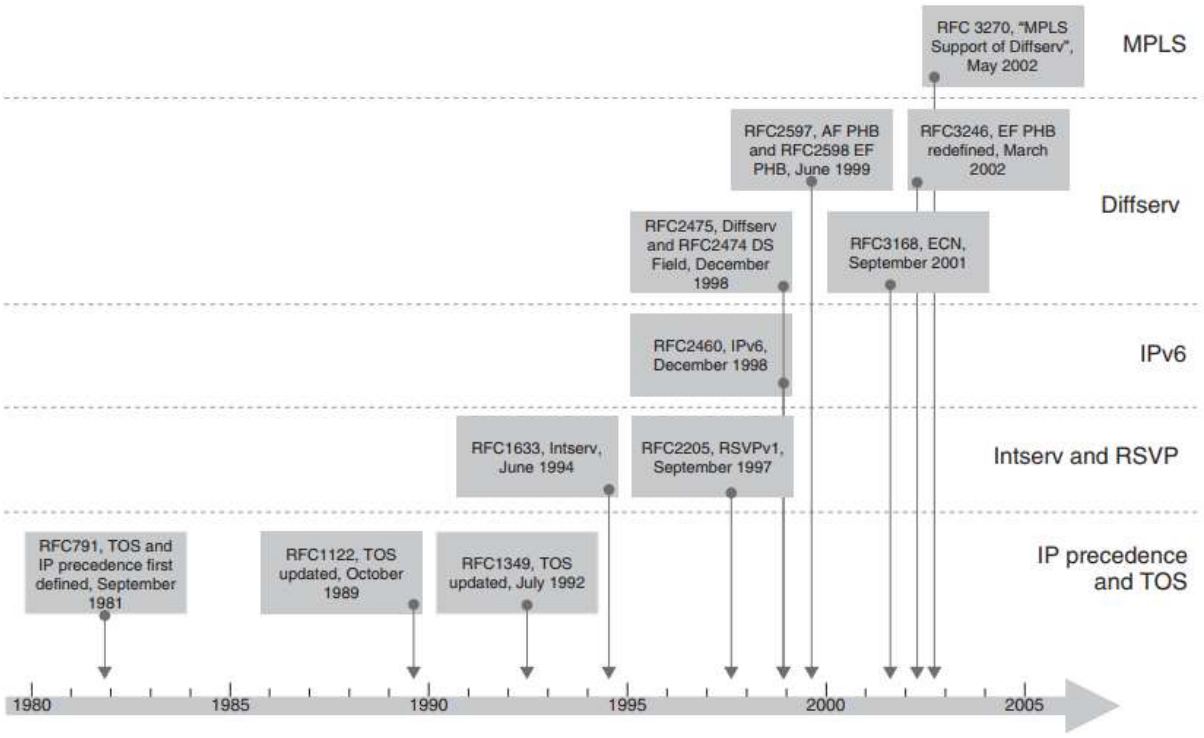
Fragmentacija slojeva veza i preplitani mehanizmi su procesorski zahtjevne funkcije i stoga mogu imati izvedbeni učinak na software-bazirane implementacije usmjerivača.

PREDAVANJE 7 - IP QoS Arhitekture

Kratka povijest IP kvalitete usluge

Da bi se razumjela povijest IP QoS arhitektura, prvo trebamo definirati što arhitektura znači u ovom kontekstu. QoS arhitekture definiraju strukture unutar koji pokrećemo QoS mehanizme kako bi osigurali SLA QoS zahtjeve sa kraja-na-kraj mreže. Da bi se ti zahtjevi potpuno definirali, trebaju osigurati kontekst u kojem se mehanizmi kao što su klasifikacija, označavanje, usmjeravanje, stavljanje u red, raspoređivanje, odbacivanje, i oblikovanje koriste zajedno da bi osigurali određenu SLA uslugu.

Standardi koji definiraju različite arhitekture za IP QoS definirane su od strane internetke inžinjerske radne skupine (Internet Engineering Task Force IETF). Slika ispod prikazuje vremensku liniju objavljivanja glavnih IETF pravila za definiranje QoS arhitektura za IP i MPLS.

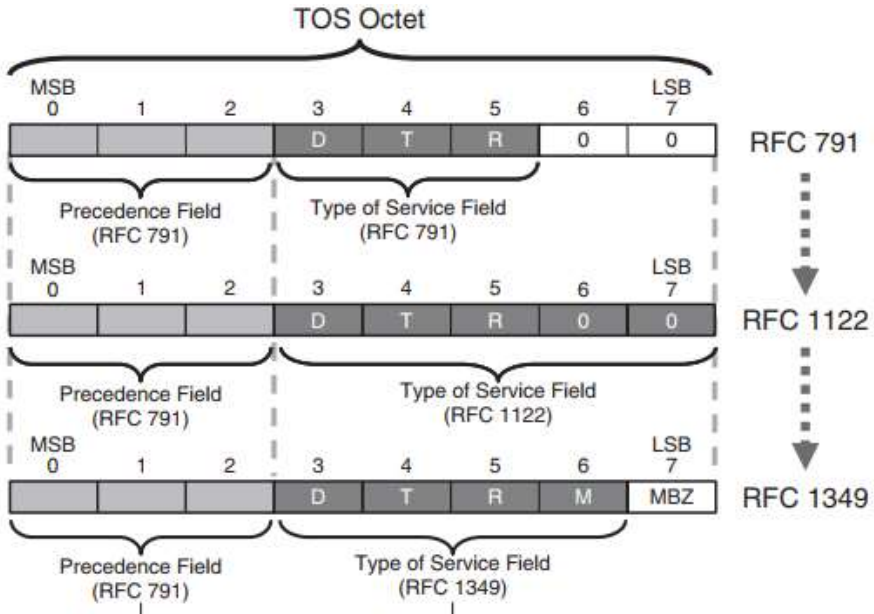


Slika 1: Vremenska linija IP QOS standarda

Sljedeći odjeljci opisuju evoluciju IP QoS arhitektura iz IP prednosti i Tipa usluge, kroz Integrirane Usluge i Diferencirane Usluge, te također opisuje kako se IP QoS arhitekture primjenjuju na MPLS.

Vrsta usluge/IP prioritet (*type of service/IP precedence*)

Godine 1981., originalna IPv4 specifikacija [RFC 791] je opisala 8 bitno polje koje se koristi za IP QoS klasifikaciju; ovo se naziva Oktet Tipa Usluge (*Type of Service octet*). Ova vrsta okteta usluge posljedično je prošla kroz nekoliko faza redefinicije u [RFC 1122] and [RFC 1349], kako je prikazano na slici ispod.



Binary	Decimal	Name
111	7	Network Control
110	6	Internet work Control
101	5	Critical and Emergency Call Processing (ECP)
100	4	Flash Override
011	3	Flash
010	2	Immediate
001	1	Priority
000	0	Routine

Bit	Meaning
3	Minimize Delay (D)
4	Maximize Throughput (T)
5	Maximize Reliability (R)
6	Minimize Monetary Cost (M)

Slika 2: Evolucija okteta tipa usluge

Oktet tipa usluge originalno (u RFC 791) je bio podijeljen na tri bita korištena za polje IP prioriteta (bitovi 0-2), tri bita (bitovi 3-5) korištena za polje vrste usluge (*type of service* (TOS)), a bitovi 6 i 7 bili su zabilježeni kao „Rezervirani za buduću upotrebu“, te su prikazani namješteni na nula. Bilježimo da je donekle zbunjujuće da je TOS polje podskup okteta tipa usluge; a to su potpuno odvojene stvari koje moramo razlikovati.

[RFC 1122] nadalje proširuje TOS polje te ono uključuje bitove 3-7, iako u to vrijeme značenje 2 bita nižeg reda (bitovi 6 I 7) nije bilo definirano.

[RFC 1349] eksplicitno definira da značenje bita 6 od okteta tipa usluge pripada TOS polju te se koristi za indikaciju težnje za „minimizacijom novčanog troška“ za pakete označene na ovaj način. Upotreba bita nižeg reda (bit 7) bila je redefinirana kao „trenutno nekorištena“ i označena „MBZ“ za „mora biti nula“ (*must be zero*). RFC 1349 je također odredio da “Izvor datagrama podešava [MBZ] polje na nula (osim ako ne sudjeluje u eksperimentu Internet protokola koji koristi taj bit)“.

Specifična značenja prioriteta i TOS polja opisana su u slijedećim poglavljima. Definicije okteta tipa usluga zastarjele su zbog „Definicije polja Diferenciranih Usluga (DS Polje) u IPv4 i IPv6 Zaglavljima“ [RFC 2474], što je također opisano u slijedećim odjeljcima.

IP Prioritet

Upotreba oznaka IP prioriteta definirana je internet protokolom RFC 791, koji definira pojam prioriteta kao "neovisno mjerilo važnosti određenog datagrama." Retrospektivno, očito je da je IP prioritet više definira shemu označavanja relativnog prioriteta, nego nadsvođene QoS arhitekture.

- Protokol RFC 791 definirao je mnoštvo denominacija prometa – označavajući kontrolu mrežnog prometa, promet usmjerivača, te različite razine ovlasti – te povezanu shemu označavanja uz upotrebu polja prednosti kako bi omogućio određivanje kojoj denominaciji pripada određeni paket. Bitovi polja prednosti nemaju pojedinačno značenje, nego se vrijednost polja uzima kao cjelina kako bi se odredilo "IP prioritet" određenog paketa; stoga, pošto postoje tri bita prednosti, postoji osam različitih vrijednosti IP prioriteta. Vrijednosti IP prioriteta i njihovih odgovarajućih denominacija prikazane su u tablici ispod; način označavanja koji se redovito koristi kada se govori o određenim vrijednostima IP prednosti je ili upotreba decimalnih vrijednosti ili upotreba prikazanih denominacija. Dodatak 2.A pruža vodič za pretvorbu vrijednosti prednosti, TOS-a i DSCP-a.
- IP prioritet omogućio je označavanje paketa, tako da se jednostavna klasifikacija može upotrijebiti u narednom čvorištu kako bi odredila postupak raspoređivanja, tj. kojim bi redom usmjerivača paket trebao biti poslužen. Kao takva, omogućila je paketima s različitim oznakama da budu tretirani različito, no nije postojala ni relativna ni apsolutna definicija kako bi se trebao tretirati promet različitih vrijednosti IP prioriteta s obzirom na kašnjenje, jitter, gubitak, protok ili dostupnost. Primjerice, nije bilo definicije kako bi paket s oznakom Prioriteta 3 ("hitno") trebao biti tretiran u odnosu na paket s oznakom Prioritet 2 ("odmah"). Protokol RFC 791 uviđa sljedeće; "Neke mreže nude prednost usluge, koja na neki način tretira promet visokog prioriteta kao bitniji od ostalog prometa."
- Stoga, IP prioritet nije definirala arhitektonski okvir mogućnosti nužnih za održavanje usluga s definiranim SLA uvjetima te, kao posljedicu toga, nije dosegla široku primjenu. Unatoč tome, upotreba nekih oznaka IP prednosti postala je stvarna – npr. većina prodavača usmjerivača danas obilježava promet protokola isporučitelja oznakom IP prednosti 6 – *po default-u*. Iako je upotrebu IP prioriteta naslijedilo polje DS, ovo stvarno obilježavanje ne uzrokuje nikakve probleme s obzirom na povratnu kompatibilnost, pošto Diffserv omogućuje povratnu kompatibilnost upotrebom grupe izabranih kodnih točaka.

Vrsta usluge (TOS)

Definicija polja vrste usluge razvila se protokolima RFC 791, RFC 1122 I RFC 1349. Od njih, protokol RFC 1349 predstavlja najnoviju i najrazumljiviju definiciju, tako da se ovaj odlomak poziva upravo na nju.

- RFC 1349 definirao je shemu upotrebe 4-bitnog TOS polja (bitovi 3-6 Okteta Tipa Usluge) kako bi odredio uslugu koja se traži od mreže za svaki paket. Suprotno polju prioriteta, gdje pojedinačni bitovi nemaju određeno značenje, svaki bit TOS polja zasebno je postavljen u paket ako bi taj paket zahtijevao uslugu koju taj bit predstavlja na način kako je prikazano na Slici 2.26; svi bitovi namješteni na nulu ukazuju na to da paket zahtjeva normalnu uslugu.

- Kako je definirano protokolom RFC 1349, označavanje polja TOS-a nije trebalo odrediti točan red čekanja koji bi trebao opslužiti određeni paket u mrežnom čvoru - to je bio zadatak polja IP prioriteta – već je označavanje TOS-a nekog paketa trebalo upotrebljavati da bi se odredilo kojim će putem taj paket ići kroz mrežu. Specifikacije nekih protokola usmjeravanja omogućili su potporu usmjeravanju TOS-a, pomoću kojeg bi se mogao odreditiset različitih staza za svaku vrijednost IP TOS-a, tako da bi neki IP paket mogao biti usmjeravan na temelju i odredišne IP adrese tog paketa i vrijednosti njegova TOS polja.
- Već smo napravili razliku između Okteta tipa usluge i TOS polja. Nazivi ‘’vrsta (tip) usluge’’ ili ‘’TOS’’, ‘’kada se samostalno koriste, odnose se općenito na upotrebu TOS polja za TOS usmjeravanje. Kada se generalno govori o TOS-u,smatra se da uzimamo cjelokupnu vrijednost Okteta tipa usluge (uključujući polje IP prioriteta te bit 7 od Oktetatipa usluge) izraženu dekadski, gdje se bit 0 uzima kako najznačajniji bit.To se naziva "vrijednost TOS-a". Na primjer, ako uzmemo da je binarna vrijednost polja prednosti 101, a vrijednost TOS polja 1000, TOS vrijednost bi se općenito spominjala kao dekadska "176" (tj. binarno 10110000).Ovaj sistem bilježenja ponekad može dovesti do konfuzije jer upotrebljava vrijednost IP prioriteta; stoga, iako paket može imati binarnu vrijednost TOS polja 0000 (t.j. normalna usluga), ako ima binarnu vrijednost polja prednosti 101, vrijednost TOS-a bi se općenito označavala dekadskom "160" (10100000).

Kada su ustanovljena ograničenja IP prioriteta i vrste usluge došlo je do definiranja QoS arhitekture Integriranih usluga i Diferenciranih usluga, koji su doveli do zastarijevanja TOS polja na račun polja Diferenciranih usluga.

IPv6 Oktet tipa usluge (IPv6 Traffic Class Octet)

IPv6 oktet vrste (tipa) usluge nakratko je postojao samo u teoriji, pa stoga nije vrijedan duže rasprave. Definiran je protokolom [RFC 2460] u prosincu 1998. godine, a potom je u istom mjesecu redefiniran definiranjem polja Diferenciranih Usluga (DS), određenog protokolom [RFC 2474].

Arhitektura integriranih usluga

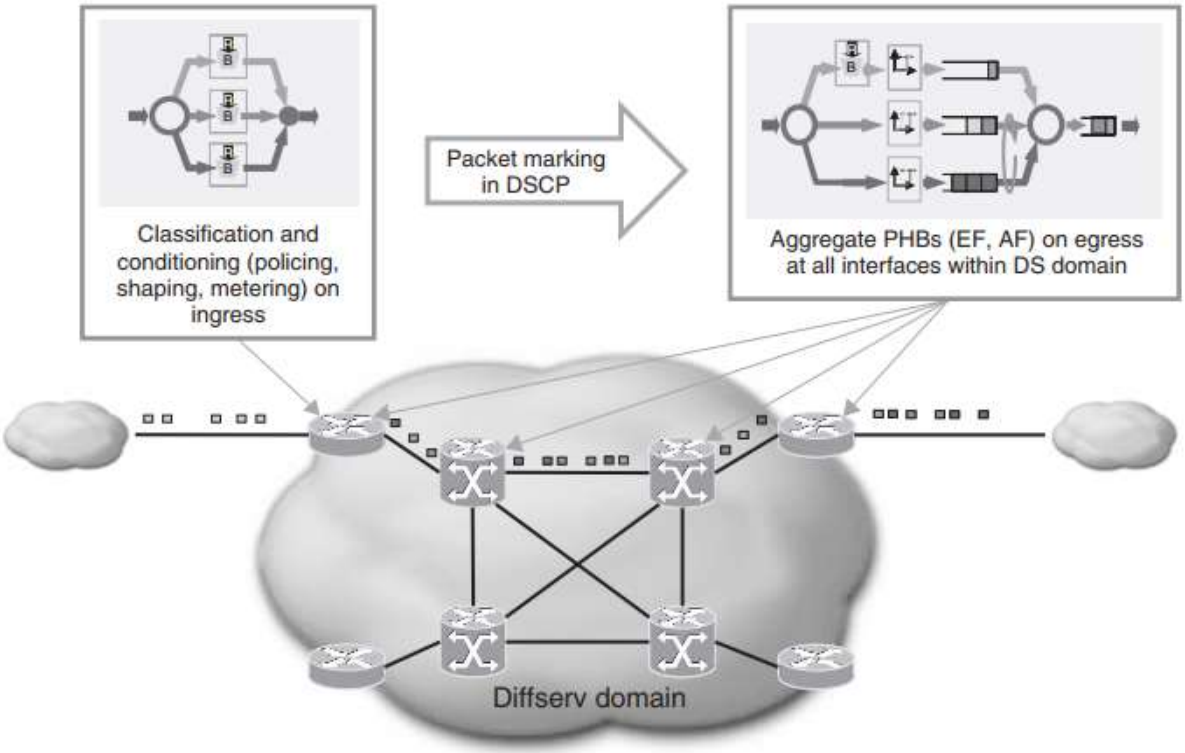
Preporuka [RFC 1633] opisuje filozofiju integriranih usluga tj „Intserv IP QoS arhitekturu“. Arhitektura je dizajnirana za rješavanje problema identificiranih IP prioritetom i vrstom usluge, pružajući sposobnosti podrške striktnim SLA zahtjevima aplikacija kao što su VoIP i video.

Intserv se hvata u koštac s problemom pružanja sigurne razine usluga aplikacijama izričitim upravljanjem resursima širine pojasa i raspoređivačima protoka na osnovi svakog pojedinačnog toka. Resursi se rezerviraju i postupak nadzora se obavlja za svaki tok. Protokol za rezervaciju resursa (RSVP) je signalizacijski protokol s kraja na kraj mreže koji se koristi za postavljanje Intserv rezervacije.

Arhitektura diferenciranih usluga (*Differentiated Services Architecture*)

Problemi sa skalabilnošću koji su se pojavili kod Intserv-a vode do definicije arhitekture diferenciranih usluga DS (Differentiated Services) ili "Diffserv" IP QoS Arhitekture [RFC 2475].

Diffserv obuhvaća ključne komponente pod nazivom Diffserv domena (*Diffserv domain*) za različite vrste ili razrede usluga.koje se koriste zajedno kako bi Diffserv IP mreža podržavala: diferencirano kašnjenje s kraja na kraj mreže, jitter i gubitak podataka. Ove komponente prikazane su na slici ispod



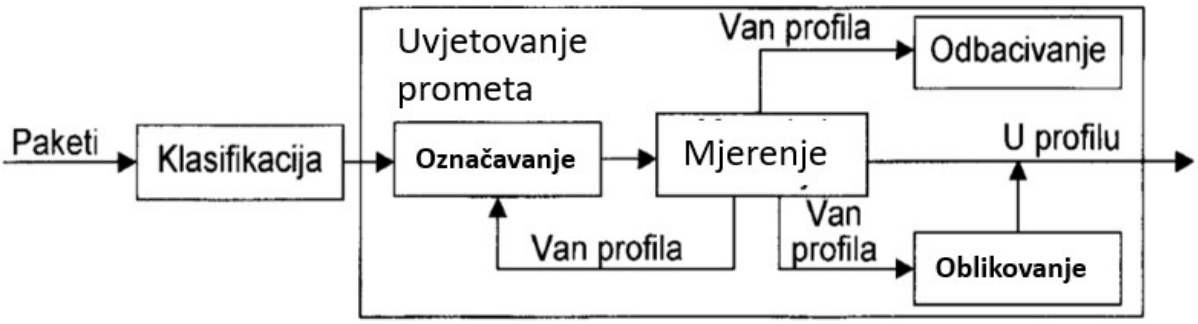
Slika 3: Diffserv arhitektura - RFC 2475

Prometna klasifikacija i uvjetovanje

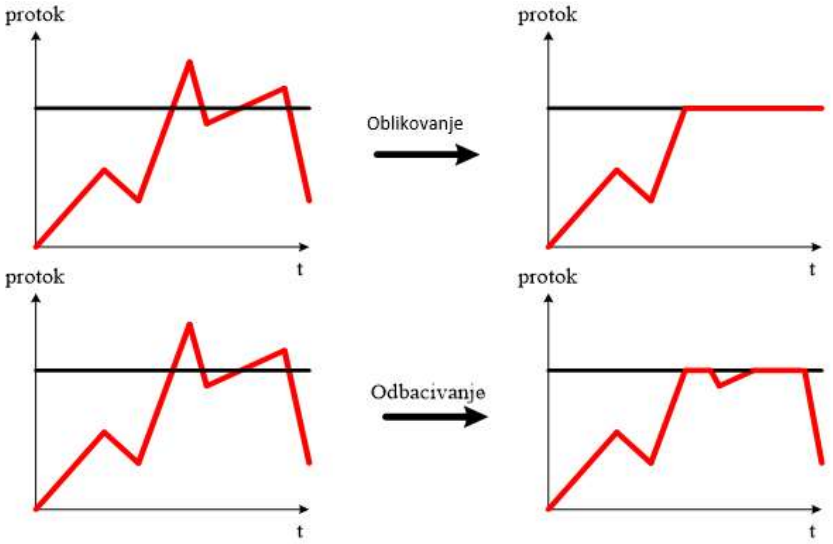
Rub Diffserv domene je naznačen granicom između davatelja i korisnika usluga unutar koje se provode Diffserv garantirane usluge . To ne znači zaključak da je Diffserv arhitektura primjenjiva samo na pružatelja mrežnih usluga. Odjel za umrežavanje unutar neke korporacije predstavlja ponuđača usluga za svoje poduzeće.

Na ulazu u Diffserv domenu, korisnički promet se klasificira korištenjem jednostavne, implicitne ili složene klasifikacije u ograničen broj prometnih razreda, koji su također poznati kao "skupno tj. agregatno ponašanje" u Diffserv načinu izražavanja. Ove agregatne prometne razrede provjerava se u skladu s dogovorenim profilima – što se u Diffserv izričaju naziva sporazum o regulaciji prometa (*Traffic Conditioning Agreements-TCA*). QoS mehanizmi, kao

što su oblikovanja ili nadgledanja, koriste se za "regulaciju (*conditioning*)" prometa kako bi se osiguralo da je ulaz prometa u Diffserv domenu usklađen s TCA. Neusklađen promet može se kasniti, odbaciti se, ili ponovno označiti.TCA je izveden iz SLA (Ugovor o razini usluge) između davatelja i primatelja usluge, a definira karakteristike ponuđenoga prometa za koje je osigurana SLA razina.



Na primjer, ako je nekoj lokaciji osigurano 128 kb/s zajamčeneVoIP usluge, TCA bi mogao imati ulogu nadgledanja i ograničenja pristiglog VoIP prometa iz te lokacije na 128 kb/s (uz odgovarajući prasak), sa odbacivanjem viška prometa.



Ulaskom u domenu DiffServ, mrežni promet podvrgnut je klasifikaciji i usklađivanju. Promet se može klasificirati prema mnogim parametrima, kao što su izvorišna adresa, odredišna adresa ili vrsta prometa i dodjela određenom prometnom razredu. Prometni razvrstači poštuju DiffServ oznake primljenih paketa ili ih mogu ignorirati te nametnuti svoje oznake. Budući da operatori žele čvrstu kontrolu nad količinom i vrstom prometa u određenome razredu, vrlo rijetko mreža poštuje oznake paketa koji dolaze do DiffServ domene. Promet u svakome razredu može se dodatno regulirati podvrgavanjem ograničenju brzine, prometnom nadgledanju ili oblikovanju.

DSCP označavanje

Kako bi se utvrdilo kojemu određenom razredu ili združenome ponašanju pripadaju paketi, oni se ili unaprijed označavaju pomoću *Diffserv Code Point*(DSCP) unutar DS polja u zaglavlju IP paketa, ili se označavajuna ulazu u Diffserv domenu. Označavanje može napraviti nadglednik

koji provodi TCA pa u tom slučaju Diffserv čvorovi koji slijede, trebaju samo napraviti jednostavnu klasifikaciju pomoću DSCP kako bi se odredio razred paketa. Diferencirane usluge ili DiffServ je arhitektura umrežavanja računala koja određuje jednostavan i proširiv mehanizam sa grubom podjelom na klase za upravljanje mrežnim prometom i pružanjem kvalitetne usluge (QoS) u modernim IP mrežama.DiffServ se može na primjer koristiti tako mrežnom prometu osjetljivom na kašnjenje, kao što su glasovni promet ili video usluge, osigura malo kašnjenje, a da istovremeno omogućiti jednostavnu „*best effort*“ uslugu ne kritičnim uslugama kao što su web promet ili prijenos datoteke. DiffServ koristi 6-bitni polje u zaglavlju IP paketa DSCP za potrebe razvrstavanja. DSCP zamjenjuje zastarjelu „vrstu usluge“ (TOS) polja. Budući da moderne podatkovne mreže prenose različite vrste usluga, uključujući i glasovne, video projekciju, glazbu, web stranice i e-mail, mnogi od predloženih QoS mehanizama koji omogućavaju ovim uslugama zajedničko postojanje na mreži, bili su i složeni i nisu omogućavali daljne brzo širenje kako bi se zadovoljili zahtjevi javnoga Interneta. U prosincu 1998, IETF RFC objavljuje preporuku 2474 koja definira polje diferenciranih usluga DS (*Definition of the Differentiated Services Field*) u IPv4 i IPv6 zaglavljima, čime je zamijenjeno TOS polje s DSCP poljem. U DSCP polju, područje od osam vrijednosti (izbornik razreda) koristi se za povratnu kompatibilnost s prethodnom IP specifikacijom u bivšemu TOS polju. Danas je DiffServ u velikoj mjeri istisnuo TOS polje i druge QoS mehanizme trećega sloja, kao što su integrirane usluge (IntServ).

Ponašanja na skoku (*Per-hop behaviors*)

Ponašanjena skoku (*Per-Hop Behavior*) određuje se prema DS polju diferenciranih usluga IPv4 ili IPv6 zaglavlja. DS polje se sastoji od 6-bitnog koda diferenciranih usluga (DSCP), a izravno obavješćivanje o zagušenju ECN (*Explicit Congestion Notification*) zauzima 2 najmanje značajna bita.

U teoriji mreža može imati do 64 (odnosno 2^6) različitih prometnih razreda koji koriste različite oznake u DSCP. DiffServ RFC preporuča, ali ne zahtijeva, određena kodiranja. To mrežnim operatorima daje veliku fleksibilnost u definiranju prometnih razreda. U praksi, međutim, većina mreža koristiti sljedeća uobičajeno definirana ponašanjana skoku:

- Standardno prosljeđivanje (*Default PHB*) - što se koristi kod „best effort“ prometa
- Ubrzano prosljeđivanje (*Expedited Forwarding- EF*) PHB odnosi se na promet sa zahtjevanim malim gubitkom i promet maloga kašnjenja
- Zajamčeno prosljeđivanje (*Assured Forwarding- AF*) PHB osigurava isporuku u skladu s propisanim uvjetima
- Odabir kategorije PHB (*Class Selector PHB*) - održava kompatibilnost s poljem IP prioriteta (*IP Precedence field*).

Default PHB je jedino zahtijevano ponašanje. U osnovi, bilo koji promet koji ne ispunjava uvjete bilo kojega od drugih definiranih klasa nalazi se u standardnome PHB-u. Standardni PHB ima „best effort“ svojstva prosljeđivanja. Za standardni (*default*) PHB, preporučeni DSCP je '000000' (u binarnome prikazu).

Uvjetovanje koje se primjenjuje na rubovima mreže, osigurava da se sav promet koji ulazi u Diffserv domenu podčinjava TCA-ovima i odgovarajuće se označava. Unutar Diffserv domene, cilj nam je osiguranjeispunjenja SLA prema zadanim klasama prometa, za ograničen

broj podržanih klasa. Kontrolni mehanizmi raspoređivanje prema klasama i čekanja u redovima primjenjuju na prometne klasepomoću DSCP obilježavanja.

Diffserv nije obvezujući za definiranje algoritama raspoređivanja i upravljanja čekanjem u redu, koji bi se trebali primijeniti u svakome sljedećem skoku kroz mrežu, već koristi razinu apstrakcije u definiranju uočljivih ponašanja prosljeđivanja koja se zovu ponašanja prema skoku PHBs (*Per-Hop Behaviors*), a koja se mogu primijeniti na promet u svakome sljedećem skoku.

Za razliku od Intserv, Diffserv konfiguracije se podešavaju bilo ručnim ugađanjem ili u NMS (*Network Management System*) sustavu, umjesto postavljanjem od strane mrežnoga signalizacijskoga protokola.

SLA s kraja na kraj mreže zajamčen je korištenjem Diffserv-a osiguranjem odgovarajućih resursa pri svakome skoku u odnosu na prometno opterećenje unutar klase. Prometna opterećenja prema vrsti klase unutar Diffserv domene vremenom će se mijenjati, a time i planiranje kapaciteta prema vrsti klase što postaje ključan segment Diffserv-a kako bi se osiguralo da su resursi za svaku klasu prometa na odgovarajući način osigurani. Planiranje kapaciteta je objašnjeno u poglavlju 5.

Skalabilnost Diffserv postiže se izvođenjem složenih QoS funkcija po svakom korisniku i održavanjem tog stanja (npr. složeni klasifikacijski kriteriji), samo na rubovima mreže. Distribucija ove funkcije samo na rubu mreže omogućuje nesmetano proširenje (skaliranje) mreže, širenjem ruba mreže sa porastom mreže. Za razliku od Intserv, u Diffserv domeni, nema obrade prema pojedinačnom toku ili prema klijentu, nego se skalabilnost postiže korištenjem samo ograničenoga broja prometnih klasa, koja se jednostavno klasificiraju pomoću DSCP obilježavanja unutar svakoga paketa, dakle obavezna je samo obrada prometa prema klasi (razredu).

Diffserv može se primijeniti jednako na IPv6 na IPv4. Diffserv se također može primijeniti na MPLS, iako ograničena veličina polja dostupna QoS oznakama u MPLS uvodi neke složenosti, koje ćemo naknadno opisati.

Diffserv je daleko najraširenija IP QoS arhitektura. Ona je široko korištena u poslovnim mrežama i kao i u mrežama javnih pružatelja usluga(*Service Provider-SP*) koji poduzećima pružaju uslugu virtualne privatne mreže (*Virtual Private Network*-VPN). Diffserv također je angažiran za podržavanjeprijelaza prema tzv. mrežama nove generacije (Next Generation Network-NGN), koje podržavaju migraciju PSTN telefonskih usluga prema IP/MPLS mrežama.

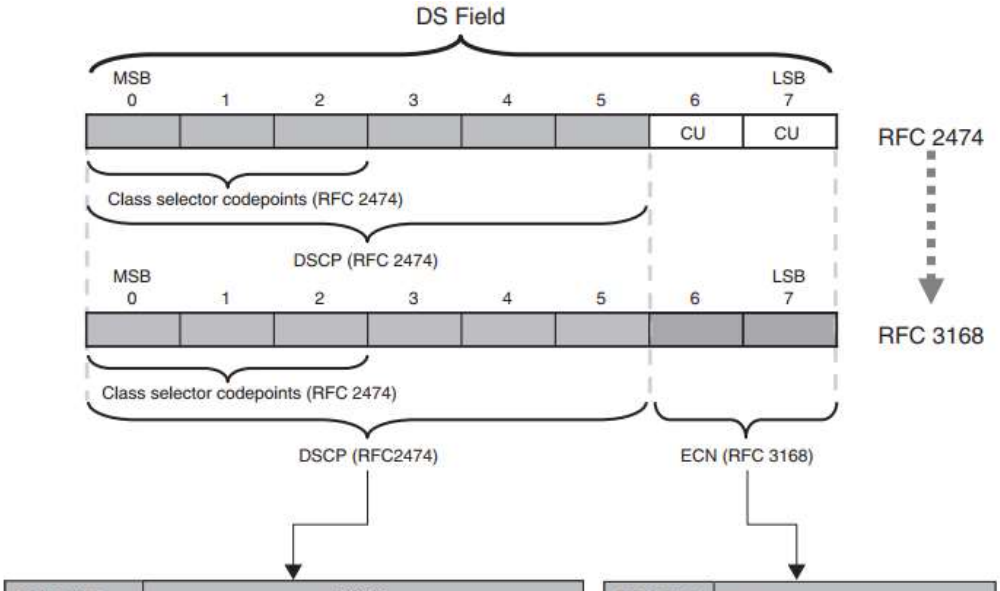
U mrežama sljedeće generacije NGN, PSTN zamjenske usluge koje se temelje na IP koegzistiraju na istoj mreži s uslugama "*best effort*" pristupa Internetu i s poslovno orijentiranim VPN uslugama. Diffserv se koristi kako bi se osiguralo da se za svaku uslugu ispune SLA zahtjevi i osigura izoliranost između mrežnog ponašanja prema različitim uslugama.

SLA ugovori temeljeni na Diffserv-u općenito nisu napravljeni za pristup Internet uslugama, odnosno uslugama na širem Internetu, jer se usluge pristupa Internetu prenose preko više različitih mreža pružatelja usluga te ako svi oni ne omogućuju jednake Diffserv mogućnosti,

nema koristi da od toga što pojedini pružatelj podržava Diffserv za takve usluge. Nadalje, pošto su usluge pristupa Internetu roba koja je na začelju IP ponude usluga, nema poticaja pružateljima usluga za troškove i bavljenje složenošću pružanja Diffserv-e kvalitete za usluge pristup Internetu svojim klijentima.

DS polje

Polje diferenciranih usluga (DS), određeno protokolom [RFC 2474], redefiniralo je upotrebu 8-bitnog polja koje se prije koristilo za „Oktet tipa usluge“ protokola IPv4 [RFC 1349] i „Oktet klase prometa“ protokola IPv6 [RFC 2460]. Definicija DS polja odredila je da se prvih 6 bitova polja (bitovi 0-5) nazovu „Kodnom točkom diferenciranih usluga“ (Differentiated Services code point-DSCP). DSCP polje je nestrukturirano i vrijednost polja se uzima u cjelini, t.j. ne postoji pojedinačno značenje svakog posebnog bita. Određena kombinacija DSCP bitova naziva se "kodna točka", a podešena je tako da se može upotrijebiti pri odabiru PHB-a koji će određeni paket doživjeti u svakom čvoru. DS polje prikazano je na slici ispod.



Codepoint	DSCP		
Default/CS0	000000		
EF PHB	101110		
CS1	001000		
CS2	010000		
CS3	011000		
CS4	100000		
CS5	101000		
CS6	110000		
CS7	111000		
AF PHB Group	Drop Precedence		
AF Class	Low (AFx1)	Medium (AFx2)	High (AFx3)
AF1x	AF11 = 001001	AF12 = 001010	AF13 = 001011
AF2x	AF21 = 010001	AF22 = 010010	AF23 = 010011
AF3x	AF31 = 011001	AF32 = 011010	AF33 = 011011
AF4x	AF41 = 100001	AF42 = 100010	AF43 = 100011

ECN Field		Meaning
0	0	Not ECT
0	1	ECT(0): not defined in [RFC 2481]
1	0	ECT(1)
1	1	CE

Slika 4: format DS polja

Kodne točke mogu biti izražene binarno ili decimalno. U binarnom obliku, koriste se oznake "xxxxxx", gdje "x" može biti "1" ili "0", a znamenka najviše lijevo označava bit 0 DSCP-a. U

decimalnom obliku, svih 6 bitova izraženi su dekadski, a bit 0 se uzima kao najznačajniji bit; na primjer, DSCP binarne vrijednosti 010000 prikazan je kao DSCP 16.

DSCP je 6-bitno polje i stoga se može upotrijebiti da označi 64 različite kodne točke. Protokol RFC 2474 razdijelio je ovaj prostor kodnih točaka na tri kvalifikacijske skupine u cilju označavanja i upotrebe kodnih točaka:

Skupina 1 – standardna upotreba. Prva skupina sastoji se od 32 kodne točke u granicama xxxxx0, po definiciji doznačene standardiziranim PHB-ovima u IEFT-u.

Skupina 2 – pokusna ili lokalna upotreba. 16 kodnih točaka u granicama xxxx11 rezervirane za pokusnu ili lokalnu upotrebu (EXP/LU).

Skupina 3 – pokusna ili lokalna upotreba. 16 kodnih točaka u granicama xxxx01 također rezerviranih za pokusnu ili lokalnu upotrebu (EXP/LU). Razlika između Skupina 2 i 3, pak, je u tome što upotreba ovog polja može biti naknadno redefinirana za standardizirane zadatke ako se Skupina 1 ikada istroši.

Prostor dodjele DSCP kodnih točaka sažet je u tablici na Slici ispod.

Pool	Codepoint Space	Assignment Policy
1	xxxxx0	Standards Action
2	xxxx11	EXP/LU
3	xxxx01	EXP/LU

Slika 5: prostor zadataka DSCP kodnih točaka

Neke od vrijednosti DSCP-a u prostoru kodnih točaka Skupine 1, mada ne sve, dodijeljene su određenim PHB-ovima standardiziranim u IFTF-u:

DSCP 0 (binarno 000000) dodijeljen je standardnom PHB-u

Žurnom prosljeđivanju (EF) dodijeljen je DSCP 46 (binarno 101110).

Grupa 12 kodnih točaka prikazanih ns Slici 2.28 dodijeljena je grupi AF PHB

Grupa kodnih točaka definiranih kao kodne točke "izbornika klase" (*Class Selector-CS*) su bilo koje od 8 kodnih točaka oblika "xxx000" gdje "x" može biti "1" ili "0". Oznaka koja se koristi za CS kodne točke je "CS", nakon kojeg slijedi vrijednost prva tri bita DSCP-a izražena decimalno, gdje se bit 0 uzima kao najznačajniji, npr. Kodna točka 101000 izražava se kao CS5.

CS kodne točke koriste tek prva tri bita DSCP-a, odnosno, bitove koji su prije definirani za polje IP prioriteta, stoga upotreba CS kodnih točaka pruža povratnu kompatibilnost s IP prioritetom, t.j. označavanje ili klasifikacija nekog paketa kao CS5 zapravo je u svakom smislu isto kao označavanje ili klasifikacija nekog paketa s IP prioritetom 5 (pod pretpostavkom da je TOS polje namješteno na 0). CS kodne točke imaju povezanu PHB definiciju opisanu prošlom odlomku

Jednako kao što je specificirano u dokumentima koji definiraju određeni PHB, postoji središnji „Registar polja DS kodnih točaka“ (*DS Field Codepoints Registry*-DSCR) koji održava međunarodna organizacija *Internet Assigned Numbers Authority*-IANA.

Imajte na umu da je gore navedena raspodjela kodnih točaka u Skupini 1, za standardizirane PHB-ove definirane od strane IEFT-e, više preporučljiva nego obvezna. To znači da, iako možda ima smisla koristiti ove vrijednosti, u slučaju da postoje valjani razlozi da se koriste druge vrijednosti DSCP-a umjesto onih preporučenih, sve ovisi o nahođenju mrežnog dizajnera mreže hoće li to učiniti. Stoga, suprotno raširenom mišljenju, upotreba vrijednosti koje nisu preporučene ne znači da određeni IP QoS dizajn nije sukladan Diffserv-u.

Nadalje, iako protokol RFC 2474 kaže da "preporučene kodne točke TREBAJU preslikavati specifične, standardizirane PHB-ove", isto tako kaže da "preslikavanje kodnih točaka u PHB MORA biti podesivo" kako bi dopustile alternativne konfiguracije, gdje se umjesto preporučenih koriste neke druge kodne točke.

Nadalje, svi paketi s istim DSCP-om trebali bi biti tretirani istim PHB-om. Kada bi se paketi s istim DSCP-om tretirali različitim PHB-ovima, mogli bi, primjerice, biti usmjereni u različite redove čekanja, s posljedicom da paketi istog protoka budu preraspoređeni. Stoga je ključnoda se svi paketi istog DSCP-a tretiraju istim PHB-om kako bi se spriječila preraspodjela unutar određenog protoka, zbog različitog utjecaja koji preraspodjela paketa može imati na učinkovitost nekih aplikacija (ovo je detaljnije razrađeno u Poglavlju 1).

Mnogostruke kodne točke, međutim, mogu biti preslikane istim PHB-om. Kao posljedica, iako su CS kodne točke definirane kako one kodne točke oblika xxx000, može se, a kako bi se postigla povratna kompatibilnost s IP prioritetom, koristiti alternativni pristup zanemarivanja oznaka u bitovima 3-5 DSCP-a, te klasificirati paket jedino na temelju bitova 0-2. Ako se primjeni ovaj pristup, vrijednosti DSCP-a 101000 i 101001 obje bi bile preslikane u isti PHB.

Protokol RFC 2474 izvorno je definirao bitove 6 i 7 DS polja kao rezervirane i dodijelio im oznaku "trenutno neupotrjebljene" (*Currently Unused*-CU), kao što je prikazano na Slici 2.28. Upotreba ovog polja kasnije je redefinirana protokolom [RFC 3168] za upotrebu s „Izričitom obavijesti o zagušenju“ (Explicit Congestion Notification-ECN), koji je opisan u prethodnim odlomcima.

Ponašanja na skoku (*Per hop behaviours*)
Diffserv nije nadležan za definiranje algoritama za raspoređivanje i postavljanje u redove čekanja koji bi trebali biti primijenjeni pri svakom skoku, nego koristi određenu razinu apstrakcije u definiranju iz vana vidljive "crne kutije" sa određenim ponašanjima pri prosljeđivanju (PHB-ovi), koja se primjenjuju prometu pri svakom skoku.

Postoje 4 tipa PHB-a koja su opisana u sljedećim odlomcima. Formalno su definirani na način da će primjena koja je u skladu s određenim PHB-om zasigurno podržati karakteristike ponašanja namijenjene tim PHB-om. Svaka definicija PHB-a sastoji se od dvije komponente: formalne definicije potrebnog ponašanja pri prosljeđivanju i preporučene sheme označavanja koja se koristi za klasifikaciju paketa koji će biti podvrgnuti tom PHB-u.

PHB žurnog prosljeđivanja (*Expedited Forwarding* - EF)
EF PHB [RFC 3246]2 koristi se za podržavanje aplikacija s zahtjevima za niskim kašnjenjem, jitterom i gubicima paketa kao što je VoIP. Karakteristike upotrebe koja podržava zahtjeve EF PHB-a su da je u sposoban održavati EF promet na određenoj ili čak višoj brzini, mjerljivoj unutar definiranog vremenskog intervala i neovisnoj o ponuđenom opterećenju bilo kojeg prometa drukčijeg od EF na mjestu se primjenjuje EP PHB. Ako su ove karakteristike podržane i ako se kontroliraju prometne brzine i praskovitost prometa pomoću spremnika žetona, koristeći, , onda će kašnjenje i jitter u EF prometu biti ograničeno. Nadalje, ako je dostupni prostor međumemorije za klasificirani EF promet veći od karakteristika praska signala, onda se gubitak također može kontrolirati (t.j. bit će jednak nuli).

Neke primjene raspoređivača mogu pokušati podržati EF promet koristeći algoritam raspoređivanja poput WRR-a ili WFQ-a, no kod takvih će granice najgoreg mogućeg kašnjenja EF prometa ovisiti o algoritmima upotrebljenog raspoređivača, a također mogu ovisiti i o broju redova čekanja korištenih u određenoj primjeni raspoređivača, kao što je opisano u Odlomku 2.2.4.1.2.4. kao posljedica toga, EF PHB se najčešće primjenjuje uz korištenje mehanizma za određivanje strogog prioriteta na listama čekanja, kako je opisano u odlomku o raspoređivačima. S primjenama koje podržavaju višestruke prioritetne redove čekanja, tipično svi oni podržavaju EF PHB.

Protokol RFC 3246 također određuje da ako koristimo EF PHB koji primjenjuje raspoređivač koji omogućuje EF prometu prvenstvo pred drugim prometom (npr. stroge prioritetne liste čekanja), onda mora postojati neki mehanizam koji bi ograničavao utjecaj koji on može imati na drugi promet, tj. koji bi spriječio da on iscrpi drugi promet.

Stoga, aplikacija "nadglednika" kod EF toka prometa služi dvjema svrhama: prvo, da ograniči opterećenje EF prometa na način da se, kada je u toku obrada prometa EF PHB-om, može zajamčiti kašnjenje, jitter i gubitak, a drugo, da ograniči utjecaj koji EF promet može imati na drugi promet.

EF PHB-u dodijeljena je preporučena DSCP vrijednost od 101110 (binarno) ili 46 (decimalno).

Osigurano prosljeđivanje (*Assured Forwarding* -AF) PHB
Grupa Osigurano prosljeđivanje (AF) PHB [RFC 2597] definira skup AF klasa, koje su dizajnirane kao potpora podatkovnim aplikacijama sa zahtjevima osiguranim širine pojasa, kao što su minimalna apsolutna ili relativna garancija širine pojasa, sa svojstvom „očuvanja rada“.

Ključni koncept AF PHB grupe je korištenje određene klase kao DS domene koja nudi uslugu, npr. određenoj lokaciji, sa osiguranjem da će IP paketi u toj klasi biti proslijeđeni sa visokom vjerojatnošću, sve dok brzina prometa te klase sa te lokacije ne prelazi onu definiranu ugovorom. Ako se ta brzina prometa premaši, tada se prekomjerni promet može proslijediti, ali sa vjerojatnošću koja može biti niža od one za promet koji je bio ispod ugovorene brzine.

Postoje četiri definirane AF klase koje se označavaju sa AF1x, AF2x, AF3x, i AF4x. Unutar svake klase može se dodijeliti paket jednoj od tri razine odbacivanja, npr. AF11, AF12 i AF13 unutar klase AF1x. Unutar određene klase, vjerojatnost prosljeđivanja AFx1 ne smije biti

[2] EF PHB je prvo definiran protokolom [RFC 2598], no, kasnije je određeno da je formalna definicija netočna, pa ju je kasnije naslijedila nova, u protokolu [RFC 3246].

manja od one za AFx2, a koja pak ne smije biti manja od one za AFx3, tj. AFx1 ima nisku razinu odbacivanja, AFx2 ima srednju razinu odbacivanja, a AFx3 ima visoku razinu odbacivanja. Dakle razina odbacivanja unutar klase označava relativnu važnost paketa. Skup od dvanaest preporučenih DSCP vrijednosti dodijeljen je da bi se označile četiri klase i tri razine odbacivanja unutar svake klase, kao što je prikazano na Ilustraciji 2.28. Iako su definirane samo četri AF klase u teoriji ne postoji ništa, osim veličine DSCP polja, da bi se ograničio broj klasa koje se opslužuju sa AF prosljeđujućim ponašanjem. Ako su potrebne više od četiri AF klase, onda se nepreporučene DSCP vrijednosti trebaju biti korištene za dodatne AF klase.

Određena AF klasa se ostvaruje kombinacijom uvjetovanih ponašanja na ulasku u Diffserv domenu- gdje se određena AF klasa nudi kupcu- koja kontrolira količinu prometa prihvaćenog na svakoj razini odbacivanja unutar te klase te prikladno označava promet. U tom i slijedećim čvorištima, pojasna širina AF klase je dodijeljena da bi se osiguralo da se promet unutar ugovorene brzine prijenosa dostavlja sa visokom vjerojatnošću. Ako se dogodi zagušenje unutar klase, zagušena čvorišta imaju za cilj odbacivanje paketa sa višom razinom odbacivanja prije onih sa manjom razinom odbacivanja. Dakle, na DS čvorištu, osiguranje prosljeđivanja određenog paketa ovisi o prosljeđujućim resursima dodjeljenima toj klasi, o trenutno ponuđenom opterećenju za tu klasu, te ako se zagušenje dogodi unutar klase, o razini odbacivanja paketa unutar te klase.

Rubna uvjetovana ponašanja za AF klasu će se obično implementirati koristeći jednobrzinski ili dvobrzinski nadglednik. Iako su oba nadglednika sposobna označiti „3 boje“ koje mogu odgovarati trima razinama odbacivanja, u praksi je teško shvatiti koja smislena usluga je postignuta diferencijacijom prometa sa shemom od tri boje, tj. „unutar ugovora“, „van ugovora“ i „ekstremno van ugovora“. Dakle, uobičajenije je da usmjerivači koriste samo dvije boje (unutar ugovora i van ugovora), te se stoga najčešće koriste dvije razine odbacivanja, npr. AFx1 i AFx2.

AF PHB klasa je tipično smještena u red čekanja koji je servisiran iz ponderiranih mehanizama raspoređivanja, kao što su WFQ ili DRR, gdje se ponderiranje reda čekanja i dubine redova konfigurira tako da se osigura da se paketi sa niskom razinom odbacivanja unutar klase prosljeđuju sa visokom vjerojatnošću. Ako se zagušenje dogodi unutar klase onda se za odbacivanje obično koristi WRED, npr. AFx2 promet sa većom vjerojatnošću nego AFx1 promet; ovo se obavlja pomoću agresivnijeg RED profila odbacivanja za AFx2 promet.

Standardni (*Default*) PHB

Standardni PHB [RFC 2474] se definira kao PHB koji se koristi za pakete koji nisu ekspicitno mapirani tj. pridruženi na druge PHBove. Standardni PHB se pomalo dvosmisleno označava kao PHB koji nema dodjeljenih resursa ali također ne može biti iscrpljen od drugih PHBova, ali potencijalno može iskoristiti neiskorištenu pojasnu širinu drugih klasa kad je dostupna, npr. ako ima implicirano svojstvo „očuvanja rada“. RFC 2474također tvrdi da se defaultni PHB može podržavati „mehanizmom u svakom čvorištu koji rezervira nekakav minimalan izvor (npr. međuspremnici, pojasne širine) za agregate defaultnog prometa.“. Dakle, u praksi, razlika između usluge AF PHBa, koji ima minimalnu ali neznamenarivu sigurnost pojasne širne i defaultnog PHBa je semantička. Da bi se izbjegla zabuna biramo nekorištenje defaultnog

PHBa; ako klasa zahtjeva samo minimalnu sigurnost pojasne širine, smatramo da je obavljena sa AF PHBom, koji ima minimalnu ali nezanemarivu sigurnost pojasne širine.

Može doći do zabune između defaultnog PHBa i koncepta default klase kod klasifikacije. Većina ugrađenih usmjerivača ima koncept default klase kojoj su dodijeljeni svi paketi koji nisu eksplicitno klasificirani u ostale klase; ova zadana klasa služi pojednostavljivanju QoS konfiguracije. Default klasa će biti dodijeljena redu a osiguranja pojasne širine ovoga reda će biti uglavnom podložna konfiguraciji; RED će također biti podložan konfiguraciji u ovome redu, sa ciljem optimatizacije propusnosti za TCP. Npr., promotrimo slučaj u kojem se promet koji se sastoji od pet različitih DSCP oznaka klasificira u tri odvojene klase, koje se servisiraju sa AF PHBovima. Ako se diskretne DSCP oznake preslikaju na svaku od dvije klase, onda se preostali DSCP može eksplicitno preslikati na treću klasu, ili ako je podržan koncept zadane klase, mogu se implicitno preslikati na zadanu klasu bez zahtjevanja eksplicitne konfiguracije.

PHB selektor klase
[RFC 2474] definira skup PHB zahtjeva koji se povezuju sa Selektorima klase kodnih točki. Namjera CS PHB zahtjeva je definiranje PHB grupe koja bi mogla zamijeniti (i stoga osigurati povratnu kompatibilnost) ponašanja primjenjena na pakete bazirane na njihove oznake IP prioriteta. Tim postupkom CS PHB zahtjevi pretpostavljaju da su paketi sa numerički višom vrijednosti IP prioriteta bili tretirani sa višom vjerojatnošću prosljeđivanja (npr. niža vjerojatnost odbacivanja), nego paketi sa numerički nižim vrijednostima prioriteta. Dakle, RFC 2474 specificira da paketi sa višim numeričkim vrijednostima CS kodnih toči ne smiju imati nižu vjerojatnost pravodobnog prosljeđivanja nego paketi sa nižim vrijednostim CS kodnih točaka. Definicija CS PHBa zahtjeva minimalno dvije klase koje servisiraju osam vrijednosti CS kodnih točaka; dakle, u minimalnom slučaju višestruke vrijednosti CS kodnih točaka možda trebaju biti preslikane na jednu CS PHB. Tamo gdje se na ovaj način koriste višestruke PHB, nazivaju se CS usuglašene PHB grupa. Uobičajeniji praktični razlog za korištenje CS kodnih točki nije olakšavanje povratne kompatibilnosti sa IP prioritetom, nego umjesto toga olakšavati procese preslikavanja oznaka IP paketa na MPLS eksperimentalno polje. U ovakvim slučajevima, EF ili AF PHBovi se mogu primjenjivati na klase gdje je promet klasificiran u te klase, baziran na CS klasifikaciji kodnih točki.

Ponašanja po domenama (*Per-Domain Behaviors*)
[RFC 3086] definira Diffserv „Ponašanja po domenama“(PDB-s); PDB je namijenjen definiciji određenih od-kraja-do-kraja ponašanja koja su isporučena od strane Diffserv domene. PHB se može smatrati izvana vidljivom „crnom kutijom“ koja prosljeđuje ponašanja koja se odvijaju na određenom skoku u Diffserv domeni, a slično se PDB može smatrati definicijom „crne kutije“ koja prosljeđuje ponašanja koja se odvijaju u klasi paketa unutar Diffserv domene kao cjeline. Kao takva, PDB se može smatrati Diffserv definicijom od-kraja-do-kraja inženjerskih SLAova . Samo je jedna PDB definirana i to PDB sa nižim naporom.

PDB sa nižim opterećenjem (*Lower effort* PDB)
[RFC 3662] je informacijski RFC koji definira „niži napor“ (LE) po domeni ponašanja (PDB). Usluga koju osigurava LE PDB može se okarakterizirati kao ona kod koje sav drugi promet ima prednost pred LE prometom u korištenju pojasne širine mrežnih veza, ali promet podupiran LE PHB-om može koristiti neiskorištenu pojasnu širinu drugih klasa kada su dostupne, tj. ima sposobnost čuvanja rada. Stoga, ako dođe do bilo kakvog zagušenja u Diffserv domeni, usluge

koje pruža LE PDB mogu biti potpuno iscrpljene; to jest, druge klase mogu zauzeti svu dostupnu pojasnu širinu tako da LE PDB neće dobiti ništa. Ovo je različito od od-kraja-do-kraja usluge koju pruža zadani PHB, budući da definicija zadanog PHB-a (Poglavlje 2.3.4.2.3) eksplicitno navodi da ne može biti iscrpljena. LE PDB i izrazi „klasa strvinara“ i „niže od najboljeg pokušaja“ su sinonimi.

RFC 3662 o LE PDB tvrdi: „Ovo ponašanje se može postići, npr., korištenjem rasporeda (stavljanje u red čekanja) sa malim udjelom i dopuštenim posuđivanjem.“. Dakle, u praksi razlika između LE PDB i usluge koju pruža zadani PHB je mala. Ali, kao što je raspravljano u Poglavlju 2.3.4.2.3, ne postoji značajna razlika između usluge koja je pružena AF PHB-u, koji ima minimalnu ali nezanemarivu sigurnost pojasne širine, i zadanog PHB-a. Dakle, odlučujemo se ne koristiti LE PDB za zadani PHB; radije, ako je zahtijevana sigurnost pojasne širine klase zanemariva, smatramo da je uslužena sa AF PHB-om, koji ima minimalnu sigurnost pojasne širine.

Eksplicitna obavijest o zagušenju (*Explicit Congestion Notification*)
TCP tretira mrežu kao „crnu kutiju“ po tome što se pri kontroli ponašanja ne oslanja niti na jedno određeno mrežno ponašanje pri određivanju dostupne mrežne pojasne širine. Umjesto toga, TCP se oslanja na TCP *timeout*-e ili prijema dvostrukih ACK-ova, da bi implicitno odredio gubitak paketa. AQM mehanizmi, kao što je RED, koriste se za detekciju zagušenja prije nego što redovi prekorače kapacitete (tj. prije nego što se dođe do odbacivanja s kraja reda), te selektivno odbacuju pakete da bi poslali povratnu informaciju o zagušenju krajnjim sustavima, tako da ovi smanje količinu slanja sa ciljem izbjegavanja prekomjernog gubitka paketa zbog zagušenja i održavanja visoke mrežne propusnosti uz istovremeno minimiziranje kašnjenja u redovima.

Eksplicitna obavijest o zagušenju (ECN) ima za cilj daljnje poboljšavanje propusnosti za TCP (a potencijalno i za druge transportne protokole) te reduciranje kašnjenja u redovima čekanja dodavanjem mrežne sposobnosti eksplicitnog javljanjem krajnjim sustavima kada dođe do zagušenja. Podrška za eksplicitnu obavijest o zagušenju (ECN) dodana je Diffservu u [RFC 3168]. Glavni koncept iza ECN-a je taj da umjesto da se koriste AQM mehanizmi kao što je RED koji odbacuju pakete kad dođe do zagušenja, oni se koriste da bi eksplicitno označavali pakete. Krajnji TCP stustavi bi koristili oznake paketa za određivanje kada su se zagušenja dogodila, te u tom slučaju usporili brzinu slanja. ECN se oslanja na proaktivnu indikaciju zagušenja prije nego što su paketi zapravo odbačeni, umjesto da reagiraju na gubitak paketa kao sa ne-ECN TCP stogovima, dakle ECN reducira gubitak paketa i poboljšava ukupni protok.

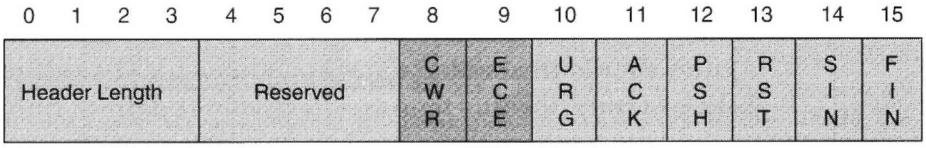
Ova eksplicitna indikacija se postiže označavanjem ECN polja, koje je RFC 3168 definirao kao 6 i 7 bitne na DS polju, a prije su bili nedefinirani. ECN polje se postavlja pomoću krajnjih sustava i od strane usmjerivača koji eksplicitno indicira kada dolazi do zagušenja (CE). Moguće oznake (koje se nazivaju kodne točke) ECN polja su prikazane u Ilustraciji 2.28.

Ilustracija 2.28 pokazuje da postoje dvije vrijednosti ECN polja koje indiciraju ECT; bilo koja može biti korištena od strane krajnjih sistema i usmjerivači bi trebali obje tretirati kao jednake. Tako, iako ECN polje ima četiri moguće vrijednosti, učinkovito definira samo tri stanja. Razlog dvjema vrijednostima koje indiciraju ECT je uglavnom baština prve eksperimentalne definicije

ECN u [RFC 2481]. RFC 2481 definira da se prvi bit ECN polja koristi za ECT a drugi za CE, dakle kodna točka 01 nije bila nedefinirana; ovo je RF 3168 izmijenio, kao što Ilustracija 2.28 pokazuje, čime je RFC 2481 zastario.

ECN zahtjeva sljedeća ponašanja u ECN sposobnim krajnjim sustavima i usmjerivačima:

Prije korištenja ECN-a, transportni protokol će možda izazvati pregovaranje među krajnjim sustavima, da bi odredio da li su oba ECN sposobna. U slučaju TCP-a, ovo se izvršava za vrijeme uspostavljanja sesije, koristeći dvije nove oznake u TCP zaglavlju, ECN-Echo (ECE) i smanjeni prozor zagušenja (CWR) oznake, koje su definirane u RFC 3168 a prikazane su na Ilustraciji 2.30.



Slika 6: TCP zaglavlje ažururano sa ECN oznakama

Pregovori o korištenju ECNa između dvaju TCP krajnja sistema, A i B, gdje je A začetnik, zahtjeva da kada A šalje TCP SYN prema B, namješta i ECE i CWR oznake da bi naznačio da je ECN sposoban. Ako je B također ECN sposoban, odgovara sa SYN-ACK sa ECE oznakom postavljenom i CWR oznakom nepostavljenom.

Sa dovršenim ECN pregovaranjem, i A i B mogu proizvesti pakete na ovoj TCP sjednici sa postavljenim ECTom, čime pokazuju da oboje podržavaju ECN.

- Usmjerivač koji primi ECT paket koristi mehanizam kao što je RED kako bi odredio da li treba postaviti CE; modificirano RED ponašanje za podršku ECN je na slijedeći način:
  - Kada nema zagušenja, tj. kada je trenutna prosječna dubina reda ispod minimuma konfiguracijskog praga (qminth), paket je smješten u red. ECT paketi koji su primljeni kada je CE bio već postavljen su nepromijenjeni a paket je normalno stavljen u red.
  - Ako postoji umjereno zagušenje, tj trenutna prosječna dubina reda (qavg) je iznad qminth i ispod qmaxtnt paket će biti označen sa CE (umjesto da ga se odbaci, što bi bio slučaj kod ne-ECT paketa) sa rastućom, ali nasumičnom, vjerojatnošću, koristeći formulu definiranu u prijašnjem poglavlju.
  - Ako postoji ekstremno zagušenje, tj. dubina trenutnog prosječnog reda (qavg) je iznad definiranog maksimalnog praga (qmaxth) tada će ECT paket uvijek biti odbačen, kao i za ne-ECT pakete.
- Nakon primanja paketa sa postavljenim CE-om, primatelj postavlja ECN-Echo oznaku u TCP ACK poruku za pošiljatelja
- Nakon primanja TCP ACK sa postavljenom ECE oznakom, pošiljatelj primjenjuje iste algoritme kontrole zagušenja kao što bi se primjenjivali sa ne-ECT krajnjim sistemom u prisutnosti jednog odbačenog paketa. Pošiljatelj također postavlja CWR oznaku u TCP zaglavlju slijedećeg paketa poslanog pošiljatelju da bi potvrdio njegovo primanje i reakciju ECN-Echo oznake.

Iako je ECN dizajniran da bude skalabilan, nije bio široko primjenjivan. Krajnji korisnici neće imati nikakve koristi od ECNa, ako nije omogućen u TCP stogovima njihovih krajnjih sistema i u usmjerivačima mreža koje koriste. Jedan od često citiranih razloga za nedostatak primjene ECNa je problem „kokoši i jajeta“, u smislu dostupnosti implementacija koje poržavaju ECN:

- Potpora ECNu od strane proizvođača usmjerivača neizbježno će zahtjevati napore razvoja i nije vjerojatno da će do ovoga razvoja doći, osim ako imaju zahtjeve za potporu od njihove tvrtke ili SP klijenata.
- Nije vjerojatno da će tvrtke ili SP klijenti pitati svoje dobavljače usmjerivača da dodaju potporu za ECN, dok god imaju potporu krajnjih sistema TCP stogova
- Proizvođači TCP stogova nemaju poticaja za razvoj potpore za ECN ako nema potpore od prodavatelja usmjerivača

Drugi često citirani razlog za nedostatak primjene ECN-a bile su brige oko subverzivnog potencijala upotrebe ECN kapaciteta, gdje paketi krivo ukazuju na ECN sposobnost, npr. Ako se paketi sa krivo označenim ECT-om susretnu sa umjerenim zagušenjem kod ECN sposobnog usmjerivača, usmjerivač može podesiti CE kodne točke umjesto odbacivanja paketa. Ako transportni protokol ustvari nije ECN sposoban ili ne odgovara definiranim ECN ponašanjima, onda transportni protokol možda neće smanjiti brzinu slanja, kao što je predviđeno ECN-om. Posljedice ove radnje su dvostruke:

- Krajnji sistemi koji krivo tvrde da su ECN sposobni primaju nižu vjerojatnost gubitka paketa kada dođe do umjerenog zagušenja nego drugi koji točno pokazuju da nisu ECN sposobni.
- Ako krajnji sistemi koji krivo tvrde da su ECN sposobni ne reduciraju svoju brzinu slanja kad bi to trebali zbog CE označavanja, razina zagušenja se može povećati, te povećati brzinu označavanja paketa ili odbacivanja koje utječe na sve protoke.

Dakle, dobrobiti ECN-a se jedino očituju kada svi krajnji sistemi surađuju u izvršavanju ECN ponašanja.Ako se ovo ne može osigurati, dobrobiti ECNa se također ne mogu osigurati. Slični razlozi se često navode kao uzrok nedostatka primjene ekvivalentnih mehanizama drugog sloja koji se koriste za adaptivno oblikovanje, kao što je eksplicitno prosljeđujuće obavještavanje o zagušenju (*forward explicit congestion notification* FECN) u komutaciji okvira i Explicit Forward Congestion Indication (EFCI) u ATM-u.

Diffserv Modeli tuneliranja (*Diffserv Tunneling Models*)

Postoji više načina „tuneliranja“ IP prometa unutar samog IP prometa, gdje tuneliranje uključuje učahurenje tj. enkapsulaciju primljenog IP paketa unutar zaglavlja drugog IP paketa na ulazu tunela, tako da paketi unutar tunela imaju dva zaglavlja (zapravo, barem dva zaglavlja – budući da je moguće imati tunele unutar tunela). Takvo tuneliranje se uglavnom koristi za kreiranje virtualne ili simulirane fizičke veze između dviju mreža preko posredničke veze. Paketi koji su unutar tunela, npr. između izvora i odredišta tunela, usmjeravaju se koristeći ISKLJUČIVO samo vanjsko zaglavlje paketa. Na odredištu tunela vanjsko IP zaglavlje se skida, otkrivajući donji IP paket (i moguće zaglavlja drugog sloja), koji se tad normalno prosljeđuje. Postoje brojne IP tehnike tuneliranja kao što su:

- Jednostavni IP-u-IP tuneli kao što su [RFC 2003] i GRE [RFC 2784]
- Više-protokolni tuneli, kao što su IP u PPP [RFC 1661] u L2TP [RFC 2661]
- Sigurne tehnike tuneliranja kao što su IPSec [RFC 2401].

Koja god da se tehnika tuneliranja koristi, kada se koristi sa Diffserv, ako se tunel ne koristi od-kraja-do-kraja (npr. od izvora do odredišta prometa), onda budući da DSCP donjeg „tuneliranog“ IP paketa nije vidljiv čvorištima na stazi tunela, treba uzeti u obzir načine kako se DSCP tunela (vanjskog) zaglavlja paketa postavi na izvoru tunela, u odnosu na unutarnji (tunelirani) paket.

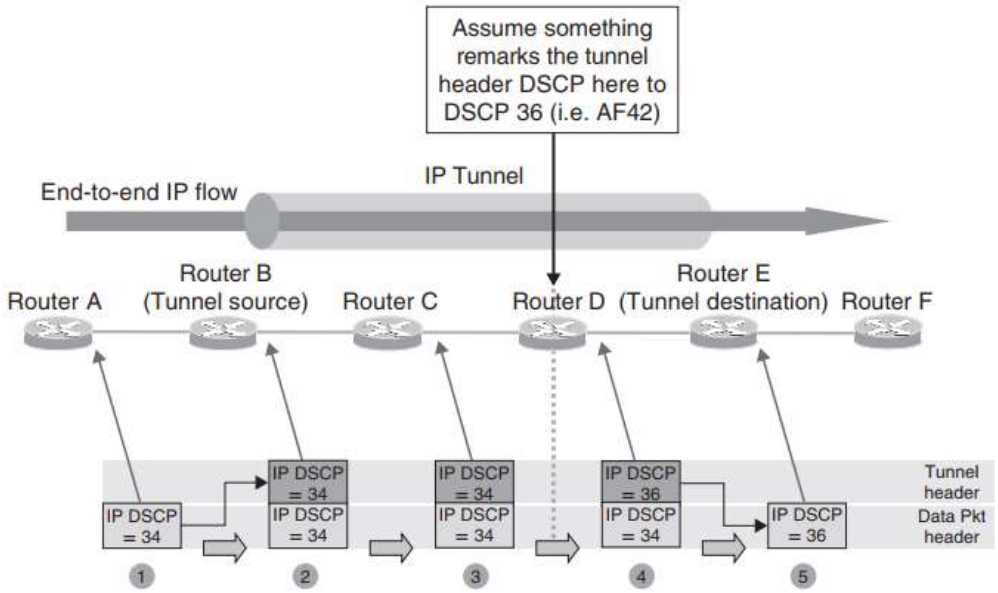
Uz to, ako je DSCP tuneliranog paketa promijenjen (tj. ponovno označen) od strane posredničkog čvorišta, negdje između izvora i odredišta tunela, treba uzeti u obzir načine kako i da li se uopće DSCP donjeg IP paketa mijenja u odnosu na vanjski (tj. tunelirani) DSCP na odredištu tunela, te da li je skinuto „tunelirano“ IP zaglavlje, koje sadrži ponovno markirane DSCP vrijednosti.

Primijećeno je da su individualni IP tuneli jednosmjerni. Ako je dvosmjerno ponašanje potrebno, onda će tunel biti potreban u svakom smjeru i odgovarajući modeli tunela će trebati biti primijenjeni na svaki tunel.

IP jednoliki Model

Kod jednolikog modela, sva klasifikacija, označavanje, i ponovno označavanje se izvode samo na DSCP polju zaglavlja vanjskog IP paketa. Na izvoru tunela, DSCP vrijednost donjeg IP paketa podataka se kopira na DSCP vrijednost zaglavlja IP tunela, i onda se na izlazu tunela DSCP zaglavlja IP tunela kopira natrag na DSCP vrijednost donjeg zaglavlja IP paketa podataka. Na ovaj način, DSCP vrijednost donjeg IP paketa se propagira kroz bilo koji dodani sloj zaglavlja tunela, te ako se vanjski DSCP ponovno markira, ova vrijednost se prosljeđuje prema dolje, donjem IP paketu kada se zaglavlje tunela skine na odredištu tunela.

Promotrite primjer prikazan u Ilustraciji 2.31 i slijedeći opis:



Slika 7: IP tunel jednolikog modela

1. Prije ulaska u IP tunel, u ovom primjeru, IP paketi podataka se označavaju sa DSCP 34 (tj. AF41)
2. Na izvoru tunela (Usmjerivač B), dodaje se zaglavlje IP tunela i DSCP vrijednost zaglavlja IP podatkovnog paketa (DSCP 34) se kopira u DSCP zaglavlja tunela, tj. DSCPi tunela i zaglavlja podatkovnog paketa je 34.
3. Na izlazu iz usmjerivača B i posredničkih usmjerivača između izvora i odredišta tunela, npr. kod usmjerivača C, kod DSCP klasifikacije pakete tunela, provjeravati će samo DSCP vrijednost zaglavlja tunela (vanjsko zaglavlje tunela gdje se koristi više slojeva tunela), koji je u ovom slučaju DSCP 34 i slučajno je isti kao i DSCP donjeg podatkovnog paketa.
4. Pretpostavimo da neka funkcija usmjerivača D ponovno označava neke ili sve tunelirane pakete u DSCP 36 (tj. AF42); ponovno označavanje ima utjecaja samo na DSCP zaglavlja tunela, dakle DSCP (krajnjeg) zaglavlja tunela je sada DSCP 36 (tj. AF42), dok će DSCP donjeg IP paketa podataka još biti DSCP 34 (tj. AF41). Usmjerivač D i bilo koji slijedeći usmjerivač između izvora i odredišta tunela, kada DSCP klasificira pakete tunela, provjeravati će samo DSCP vrijednost zaglavlja tunela, koja je sada DSCP 36.
5. Na izlazu tunela, zaglavlje tunela se skida i DSCP vrijednost zaglavlja IP tunela se kopira natrag u DSCP vrijednost donjeg zaglavlja IP podatkovnog paketa, koji je sada DSCP 36 i koji će se koristiti od strane svih slijedećih usmjerivača kada DSCP klasificira pakete.

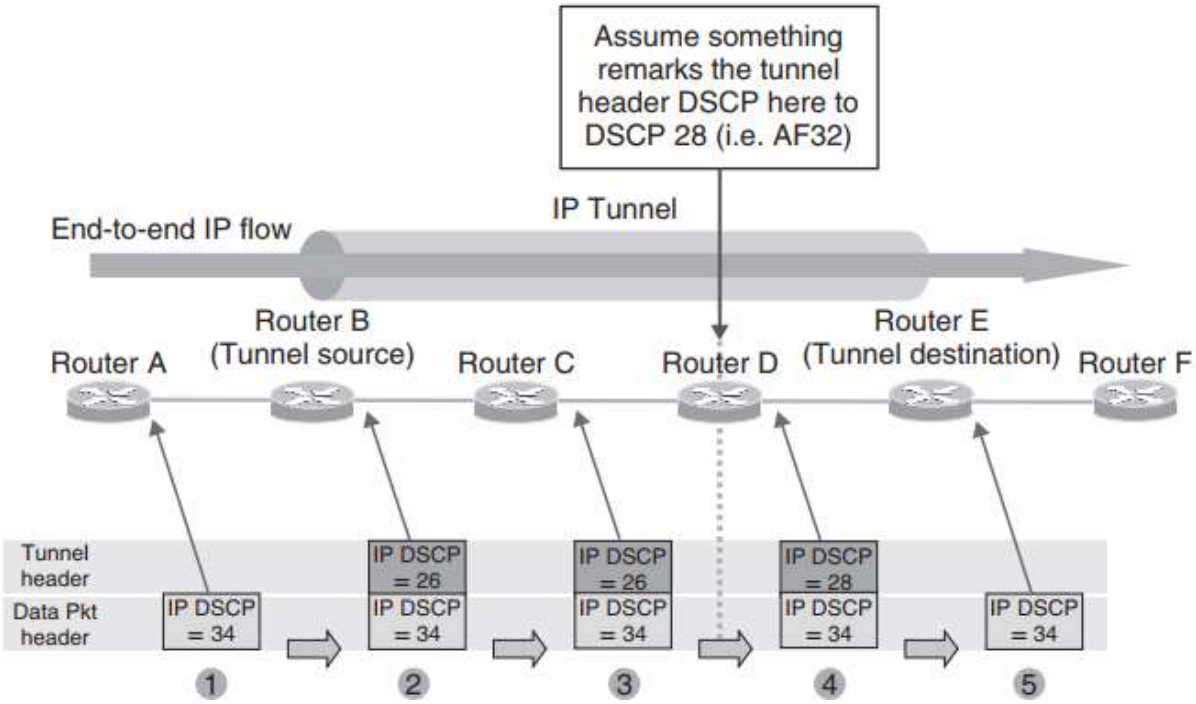
Sa jednolikim modelom, za svaki paket postoji jedan dio Diffserv informacije koji se prenosi od-kraja-do-kraja, što se može putem promijeniti, te koji je uvijek zastupljen sa DSCPom zaglavlja vanjskog IP-a. Dakle, kada koristimo jednoliki model, kod IP tunela ustvari nema

razlike u rezultatnom Diffserv ponašanju u usporedbi sa situacijom kada tunel nije prisutan. Također, nema razlike u slučaju kada se koristi više slojeva IP tunela. Kod jednolikog modela tuneli su transparentni Diffserv operacijama.

IP model cijevi (*IP Pipe Model*)

Za razliku od jednolikog modela, model cijevi tretira DSCP oznake na unutarnjim (podaci) i vanjskim (tunel) zaglavljima paketa kao nezavisne (iako moguće povezane) entitete. Kod jednolikog modela, van tunela, budući da nema zaglavlja tunela, koristi se IP DSCP podatkovni paket; između izvora i odredišta tunela, koristi se DSCP oznaka u zaglavlju tunela. Model cijevi razlikuje se od jednolikog modela u tome što DSCP vrijednost donjeg IP paketa nije kopirana na DSCP zaglavlje tunela na izvoru tunela (iako postavke DSCP tunela mogu biti izvedene iz DSCP vrijednosti donjeg IP paketa), niti je DSCP zaglavlje tunela kopirano natrag na donje IP DSCP pakete na odredištu tunela. Model cijevi se ujednako ponaša i tamo gdje se koristi više slojeva tunela, svaki se slijedeći sloj tunela tretira neovisno o prethodnom.

Promotrite primjer prikazan u Ilustraciji 2.32 i slijedeći opis:



Slika 8: IP tunel: model ciljevi

1. Prije ulaska u IP tunel, u ovom primjeru, IP paketi podataka se označavaju sa DSCP 34 (tj. AF41)
2. Na izvoru tunela (Usmjerivač B), zaglavlje tunela se dodaje i podešava se DSCP vrijednost IP zaglavlja podatkovnog paketa. DSCP vrijednost tunela može se izvesti (kopirati) iz DSCP vrijednosti donjeg IP paketa, ili se može podesiti neovisno o toj vrijednosti. U ovom primjeru, pretpostavljamo da je DSCP tunela podešena na DSCP 26 (tj. AF31) neovisno o DSCPu donjeg IP paketa.
3. Na izlazu prema usmjerivaču B i posredničkim usmjerivačima između izvora i odredišta tunela, npr. Usmjerivaču C, kada DSCP klasificira pakete tunela, provjeravati

će samo DSCP vrijednost zaglavlja tunela (vanjsko zaglavlje tunela gdje se više slojeva tunela koristi), koja je u ovom slučaju DSCP 26.

4. Pretpostavimo da neka funkcija usmjerivača D ponovno označava tunelirane pakete na DSCP 28 (tj. AF32).Ponovno označavanje ima utjecaja samo na DSCP na vanjskom zaglavlju tunela, dakle DSCP zaglavlja donjeg IP podatkovnog paketa je još DSCP 34 (tj. AF41). Na izlazu prema usmjerivač D i bilo kojem slijedećemem usmjerivaču između izvora i odredišta tunela, kada DSCP klasificira pakete tunela, provjeravati će samo DSCP vrijednost zaglavlja tunela, koja je sada DSCP 28.
5. Na odredištu tunela, zaglavlje tunela se skida. U slučaju modela cijevi, međutim, DSCP vrijednost IP zaglavlja tunela se ne kopira natrag na DSCP vrijednost IP zaglavlja donjeg podatkovnog paketa već je originalna DSCP vrijednost IP zaglavlja donjeg podatkovnog paketa sačuvana u tunelu.

Kod modela cijevi postoje dva odvojena dijela Diffserv informacija koje se koriste; jedan se koristi unutar granica tunela a drugi van tunela. Dakle, model cijevi omogućuje korištenje različitih shema označavanja unutar tunela. Ova sposobnost može biti korisna kada tunel predstavlja različitu Diffserv domenu od onih predstavljenih od strane mreža na objema stranama tunela. Ovo u kontekstu VPN usluge može biti osigurano od strane SP-a, gdje npr. SP koristi različitu shemu označavanja unutar svojega dijela mreže nego što to njihovi korisnici čine na rubu, istovremeno dopuštajući čuvanje sheme označavanja svojih korisnika od-kraja-do-kraja, u cijelom SP VPN servisu. Ova sposobnost se ponekad naziva „QoS transparentnost“.

Tipična implementacija standardnog usmjerivača kod primjene tunela kopirala bi DSCP vrijednost donjeg IP paketa u DSCP vrijednost tunela na izvoru tunela, ali ne bi kopirala DSCP vrijednost IP zaglavlja tunela natrag u DSCP vrijednost donjeg zaglavlja IP podatkovnog paketa na odredištu tunela.

Iako se [RFC 2983] odnosi samo na IP tehnologije tuneliranja, koncepti se također mogu odnositi na „tunele“ formirane učahurenjem u sloju 2 (link) ili MPLS zaglavljima. Ovi pristupi nisu vrsta „IP tuneliranja“, budući da ne dodaju dodatno IP zaglavlje, ali usprkos tome, može ih se smatrati vrstom „tunela“. MPLS Diffserv vrste tuneliranja opisane su u nadolazećim poglavljima.

IPV6 QoS arhitekture

Postoji općeniti nesporazum o tome da IPv6 ima u osnovi bolje QoS sposobnosti nego IPv4, što nije točno. Interserv i Diffserv IP QoS arhitekture mogu se jednako primjenjivati na IPv6 kao i na IPv4.

Jedina praktična razlika između IPv6 i IPv4 iz perspektive QoS-a jest ta što IPv6 zaglavlja paketa također uključuju 20-bitno protočno označeno polje [RFC 3697]. Oznaka protoka pomaže u nedvosmislenoj klasifikaciji protoka, jer neke informacije koje se koriste za identifikaciju protoka mogu nedostajati zbog fragmetacije ili enkripcije paketa.

PREDAVANJE 8 - MPLS QoS Arhitekture

MPLS (*Multi-Protocol Label Switching*) [RFC 3031] omogućuje nove paradigme prosljeđivanja u odnosu na uobičajene IPv4 ili IPv6, dopuštajući prosljeđivanje bazirano na drugim kriterijima, a ne samo na IP odredišnoj adresi. Kada struja prometa prijeđe MPLS mrežu (također poznata i kao MPLS domena), IP paketi (ili protokolne podatkovne jedinice [PDUovi] iz drugog protokola, budući da „M“ u kratici MPLS označava Multiprotokol) se „označavaju“ na ulaznom rubnom usmjerivaču MPLS domene (koja se naziva rubni usmjerivač ili LER). MPLS „labela“ je duga 32 bita, od lokalne je važnosti i postavlja se na originalno IP zaglavlje između zaglavlja drugog i trećeg sloja.U nekim slučajevima (npr.kod MPLS VPN-a ili MPLS prometnog inženjerstva), može se koristiti više od jedne oznake pa tako nastaje „stog labela“. Oznaka koja je „ugurana“ (*pushed*)na originalno IP zaglavlje od strane LER usmjerivača određuje put kojega će paket prijeći preko MPLS domene. Ovaj put se naziva *label switch path* (LSP). Usmjerivači unutar MPLS domene tzv.*Label Switch Route*rs-LSR neće provjeravati IP adresu odredišta unutar donjeg IP zaglavlja označenog paketa već će koristiti labelu (tj. „najvišu“ labelu ako postoji „stog labela“) da bi odredio koje sučelje i odlaznu labelu će koristiti kada prosljeđuje paket dalje slijedećem skoku na LSPu. Na izlazu iz MPLS domene oznake se skidaju sa paketa pomoću izlaznih LER-ova i paketi se dalje usmjeravaju IP pravilima.

The new forwarding paradigms made possible with MPLS enable IP networks to support new functionality. Different techniques and signaling protocols are used to determine and establish LSP paths, depending upon the particular paradigm being used. MPLS is most commonly deployed by service providers to provide one or more of the following functions:

Nove paradigme prosljeđivanja koje je MPLS omogućio pružaju IP mrežama nove funkcionalnosti. Različite tehnike i protokoli signaliziranja koriste se za određivanje i ustanovljavanje LSP staza.MPLS se od strane SP-ova najčešće koristi za slijedeće:

- Za omogućavanjevišestrukim privatnim virtualnim mrežama (VPN-ovi) prijenospo jednoj IP/MPLS mreži. Ovo mogu biti VPN-ovi sloja 3, kao što su oni koji koriste BGP MPLS VPN kao što je opisano u [RFC 4364], ili VPN-ovi sloja 2 kao što su oni definirani u IETF L2VPN radnoj skupini.
- Za omogućavanjeprometnog inženjerstva (*Traffic Engineering*-TE) koje koriste MPLS RVSP-TE kako je definirano u [RFC 3209],.
- Da bi osigurao brzi oporavak od pada elemenata mreže koristeći MPLS TE Fast Reroute (FRR) kao što je definirano u [RFC 4090].

Kod više-protokolnog mijenjanja oznaka postoji uobičajena pretpostavka da MPLS ima bolje QoS sposobnosti nego IPv4 i IPv6 što nije točno. Interserv i Diffserv IP QoS arhitekture mogu se primjenjivati i na MPLS, ali sa nekim praktičnim razlikama od IPv4 i IPv6.

MPLS i Interserv/RSVP

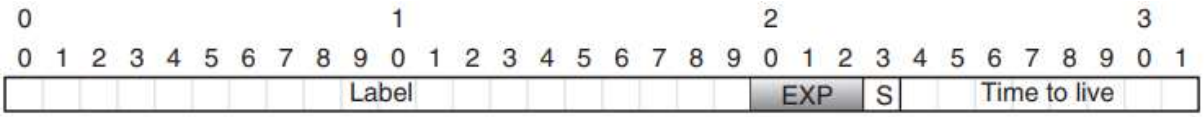
Interserv zahtijeva kontrolu pristupa i rezervaciju resursa na osnovi pojedinog protoka- kod kojeg se protok identificira 5-torkom: izvorišnom i odredišnom IP adresom, brojevima UDP/TCP porta izvora i odredišta i IP brojem protokola. Ova polja nisu vidljiva LSR-ovima unutar MPLS domene, koji prosljeđuju označane pakete bazirane samo na vanjskoj labeli, a potpora Interservu bi zahtijevala da se LSP-ovi osiguravaju na osnovi pojedinog protoka(što

nije skalabilan pristup). U praksi, Interserv/RSVP se podržava u kontekstu osiguravanja rezervacija za agregatne protoke kroz primjenu MPLS TE tunela, kao što će u više detalja biti opisano u Poglavlju 4.

2.3.6.2 MPLS i Diffserv

Diffserv se može primijeniti na MPLS mrežu u osnovi na isti način kao i obične IP mreže, kao što je definirano u [RFC 3270]. Uvjetovanje prometa se izvodi na rubu Diffserv domene točno na isti način, iako usmjerivač na rubu MPLS domene nije neophodno i usmjerivač na rubu Diffser domene. Paketi se označavaju da bi označili određenu klasu prometa kojoj pripadaju, te se onda unutar jezgre MPLS Diffserv mreže primjenjuju različiti PHB-ovi, ovisno o označavanju.

Međutim postoje neke razlike između primjene Diffserva na obične IP pakete u usporedbi sa MPLS označenim paketima. Ove razlike potječu iz činjenice da unutar MPLS mreže, svo prosljeđivanje bazira na vanjskoj oznaci, a ne na zaglavlju IP paketa. Kako se DSCP vrijednost nalazi u IP zaglavlju paketa, koje LSR ne koristi, ne može se koristiti za PHB selekciju unutar MPLS domene. Umjesto toga postoje 3-bitna polja unutar MPLS zaglavlja, kao što je i prikazano u Ilustraciji 2.33- nazvano EXP polje- koje se koristi za klasifikaciju kada se Diffserv koristi u MPLS domeni.



Slika 1: MPLS kodiranje stogova labela: Labela = vrijednost oznake (20 bitova), EXP= EXP polje (3 bita), S= indikator dna stoga (1 bit), TTL= polje vremenaživota (8 bitova)

[RFC 3032] initially defined the EXP field for experimental use; this was subsequently updated by [RFC 3270] which redefined it for use with Diffserv, although the field is still commonly referred to as the "EXP" bits. There are two mechanisms by which the EXP field is used for PHB selection within an MPLS Diffserv network; these are described in the following sections.

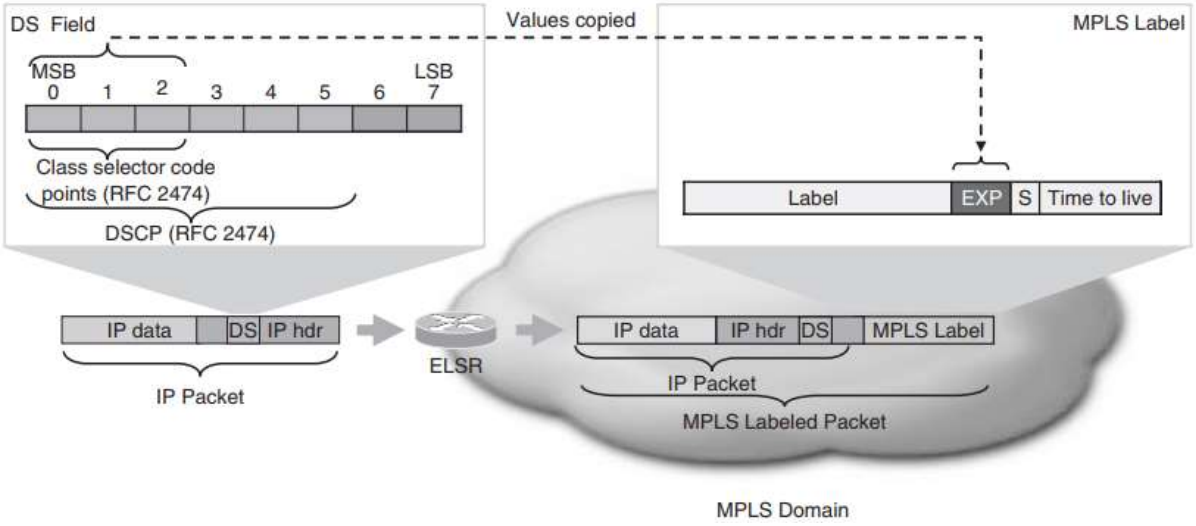
[RFC 3032] je u početku označavao EXP polje za eksperimentalnu upotrebu; što je bilo osuvremenjeno od [RFC 3270], koji ga je redefinirao za upotrebu sa Diffservom, iako se polje još uvijek uobičajeno naziva „EXP“ bitima. Postoje dva mehanizma kojima se EXP polja koriste za PHB selekciju unutar MPLS Diffserv mreže; opisani su u slijedećim odjeljcima.

***EXP Inferred PHB Selection* (EXP Izvedena PHB Selekcija)**

Najuobičajeniji pristup PHB selekciji unutar MPLS mreže je korištenje EXP polja za određivanje sa kojim PHB-om bi označeni paket trebao biti obrađen.Ovo se naziva EXP Izvedena PHB Selekcija.

EXP polje je dugo samo tri bita, te može predstavljati samo 8 diskretnih vrijednosti, dok postoje 64 moguće DSCP vrijednosti, te nije moguće tretirati EXP polje u označenim paketima kao izravno ekvivalentne DS Poljima u običnim IP paketima. Zbog toga imamo nužnu potrebu za preslikavanjem DSCP vrijednosti na EXP vrijednosti na izlazu iz LER-a, tako da određene EXP vrijednosti mogu predstavljati grupu DSCP vrijednosti, u kojem slučaju se nazivaju „PHB klasa raspoređivanja“ (PSC). Tamo gdje se EXP označavanje polja koristi za označavanje PSC-ova, LSP-ovi se nazivaju EXP-izvedeni-PSC LSP-ovi (E-LSP-ovi).

Tipično ponašanje na ulazu u LSR je kopiranje bitova od 0 do 2 sa DS polja- koji su kodne točke selektora klase (CS) (koji su funkcionalni ekvivalentni bitovima prioriteta)- na 3 bita EXP polja na MPLS labeli, kao što je i prikazano na Ilustraciji 2.34.



Slika 2: Kopiranje CS kodnih točaka na EXP polije

Tipično ponašanje primjenjeno na LSR unutar MPLS domene jest kopiranje EXP polja od labele-do-labele. Ako su nametnute dodatne oznake (tj. koristi se oznaka labelnog stoga), tipično ponašanje jest kopiranje EXP polja prema gore u stogu. Dakle, gdje su ovakva ponašanje podržana, CS oznake kodnih točki donjih IP paketa se širepreme gore kroz stog. Ako su gornje labele odbačene, tipično ponašanje jest ne kopirati EXP polje niz stog ili na CS kodne točke. Stoga, ako se oznake EXP polja promijene unutar MPLS mreže, ova promjena se ne propagira normalno niz stog, već se donje CS kodne točke i DSCP vrijednosti sačuvaju kroz MPLS domenu. I drugačija ponašanja su moguća; o njima se raspravlja u Odjeljku o Diffserv MPLS načinima tuneliranja.

***Label Inferred PHB Selection* (PHB Selekcija Izvedena iz labela)**

Korištenje E-LSP je norma u MPLS Diffserv razvojima; međutim, ako su 8 razlikovne PSC oznake nedovoljne da bi podržale broj PHB-ova potrebnih za dizajn MPLS Diffserva - definira se alternativni pristup.

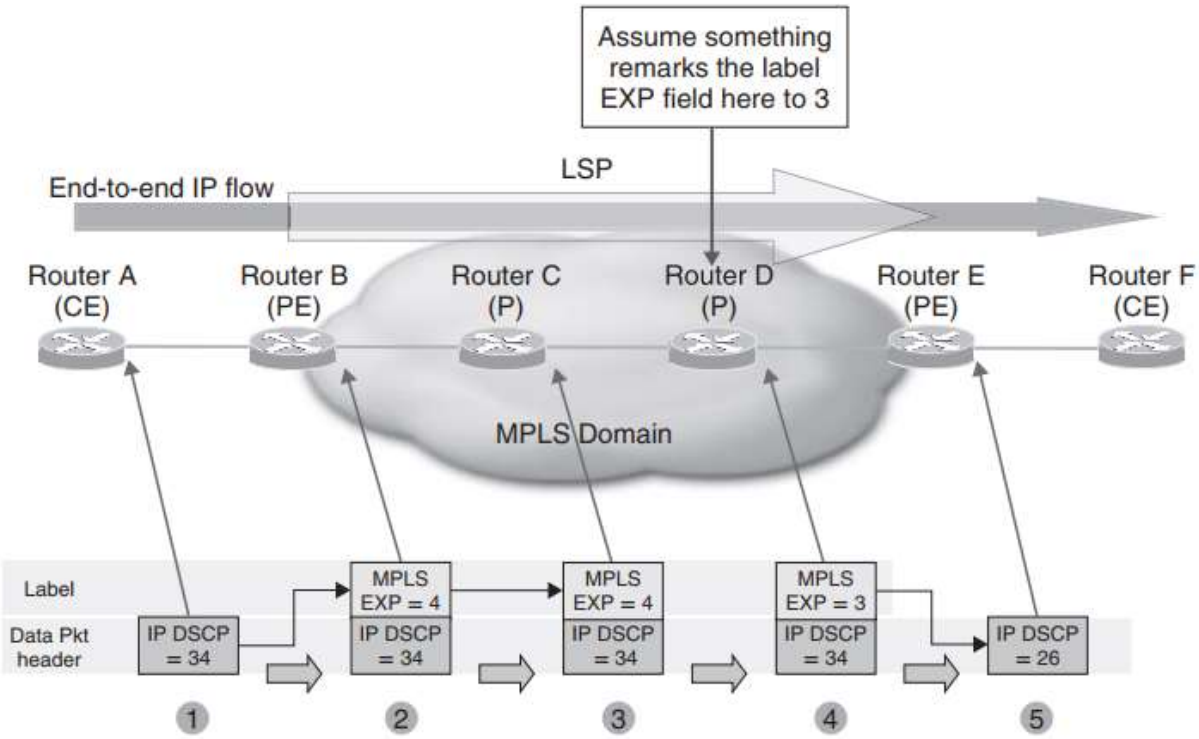
Kod E-LSP, jedan LSP se može koristiti za prijenos paketa označenih sa različitim PSC-ovima.Međutim, [RFC 3270] također definira shemu kod koje LSP nosi samo jedan PSC. LSP-ovi koji koriste ovu shemu se nazivaju label-only-inferred-PSC LSP-ovi (L-LSP-ovi). EXP polje se može koristiti za preferenciju odbacivanja koje se LSR aplicira na označeni paket (vidi AF PHB).

MPLS Diffserv Modeli Tuneliranja

[RFC 3270] razmatra specifučne aplikacije Diffserv modela tuneliranja za MPLS. Postoji više konceptualnih sličnosti između Diffserv modela tuneliranja korištenih za IP tuneliranje i onih koji se koriste za MPLS, gdje se MPLS LSP-ovi koriste umjesto IP tunela. Za razliku od IP tunela, MPLS LSP-ovi su jednosmjerni. Uz to, u usporedbi sa IP tunelima, posrednička čvorišta na putu LSP-a kontroliraju samo „gornju“ labelu. Također postoji niz razlika koje su posljedica

implicitnih razlika između IP i MPLS. [RFC 3270] definira tri Diffserv modela tuneliranja, koji su opisani u slijedećim odjeljcima.

MPLS jednoliki model (unifom model)
Jednoliki model za MPLS je konceptualno sličan IP tuneliranja. Pogledajmo primjer prikazan u Ilustraciji 2.35 i slijedeći opis. U ovom primjeru, koji opisuje slučaj prosljeđivanja od-IP-do-MPLS-a, dodaje se samo jedna razina labela, koju npr. može dodjeliti LDP protokol [RFC 3036].



Slika 3: MPLS Diffserv modeli tuneliranja: Jednoliki model

Izvan MPLS domene, npr. u usmjerivaču 1, pretpostavimo da su IP podatkovni paketi označeni sa DSCP 34 (tj. AF41)

Na ulazu u LER odnosno PE (usmjerivač B), ubacuje se početna LSP labela te se postavlja njena EXP vrijednost. EXP se može izvoditi iz DSCP vrijednosti donjeg IP paketa, međutim, kako EXP polje iznosi samo 3 bita a DSCP 8 bitova, nije moguće kopirati cijelu DSCP vrijednost na EXP polje (kao što je slučaj kod IP tunela). U ovom primjeru, pretpostavljamo da su bitovi 0-2 DSCP-a kopirani na polje oznake EXP, sa ishodom da će EXP polje biti postavljeno na 4. Moguća su alternativna preslikavanja između donjeg DSCP i EXP polja.

U slučaju MPLS-do-MPLS prosljeđivanja, ako se koristi jednoliki model, EXP vrijednost će biti kopirana kroz „stog“ , kako se budu umetali dodatni slojevi labela.

Posrednički usmjerivači na LSP-u, npr. usmjerivač C, izvršiti će izmjenulabele paketa na temelju vrijednosti labele prvobitne tj. dolazne labeleukoliko se primjenjuje funkcija „switch“ tj. zamjeni. EXP se *po default*-u kopira sa ulazne labele na izlaznu labelu. Dakle u ovom primjeru, paket bi imao EXP vrijednost 4 na izlazu iz usmjerivača C. Ako postoji stog (složaj)

labela, kada se klasificiraju paketi EXP poljem, LSR-ovi će kontrolirati samo EXP polje vanjske tj. najgornje labele.

Pretpostavljajući da neka funkcija u usmjerivač D ponovno markira pakete na LSP-u iz EXP 4 prema EXP 3, ako postoji stog labela, ponovno markiranje utječe samo na EXP vrijednost najgornje labele. Dakle, EXP vrijednost labele je sada EXP 3, dok je DSCP vrijednost u zaglavlju donjeg IP podatkovnog paketa još uvijek DSCP 34 (tj. AF41). Usmjerivač D i bilo koji slijedeći usmjerivač na LSP-u, kod klasifikacije labeliranih paketa pomoću EXP polja, kontrolirati će samo EXP polje vanjske labele, koje je sada EXP 3.

U ovom slučaju, pretpostavljamo da se ne koristi tzv penultimate hop popping (PHP) i stoga je oznaka skinuta na LER izlazu, što je zadnji skok LSP-a, u ovom slučaju usmjerivač E. DSCP vrijednost polja donjeg IP paketa može biti ponovno označena po vrijednosti izvedene iz EXP vrijednosti polja skinute labele. Ako je EXP vrijednost polja bila kopirana natrag do bitova 0-2 DSCP polja, rezultantna DSCP vrijednost sada običnog IP paketa na izlazu prema usmjerivaču E bi bila DSCP 26 (tj. AF31), iako su moguća alternativna preslikavanja između EXP polja i DSCP vrijednosti donjeg paketa. Nakon što se labele uklone, na izlazu prema usmjerivaču E i prema slijedećim usmjerivačima donji DSCP-ovi se mogu koristiti za klasificiranje paketa.

Tamo gdje sekoristi PHP, labela se uklanja na pretposljednjem skoku na LSP-u (usmjerivaču D), u kojem slučaju, kako ni jedna labelane dolazi do usmjerivača E.Usmjerivač D bi trebao izvoditi sve potrebno preslikavanje/kopiranje sa EXP-a na DSCP.

Namjera kod jednolikog modela jest ta da nema stvarne razlike u rezultantom Diffserv ponašanju pri uporabi MPLS-a u usporedbi sa slučajevima kada se MPLS ne koristi. Međutim, jedan faktor koji sprečava totalnu transparentnost MPLS-a prema Diffserv operacijama (za razliku od IP slučajeva tuneliranja), je slučaj da je MPLS EXP polje dugo samo 3 bita dok je DSCP dugo 8 bitova; dakle može biti potrebe za preslikavanjem sa DSCP vrijednosti na EXP vrijednosti i natrag na DSCP vrijednosti, za razliku od jednostavnog kopiranja koje se koristi u IP slučajevima tuneliranja.

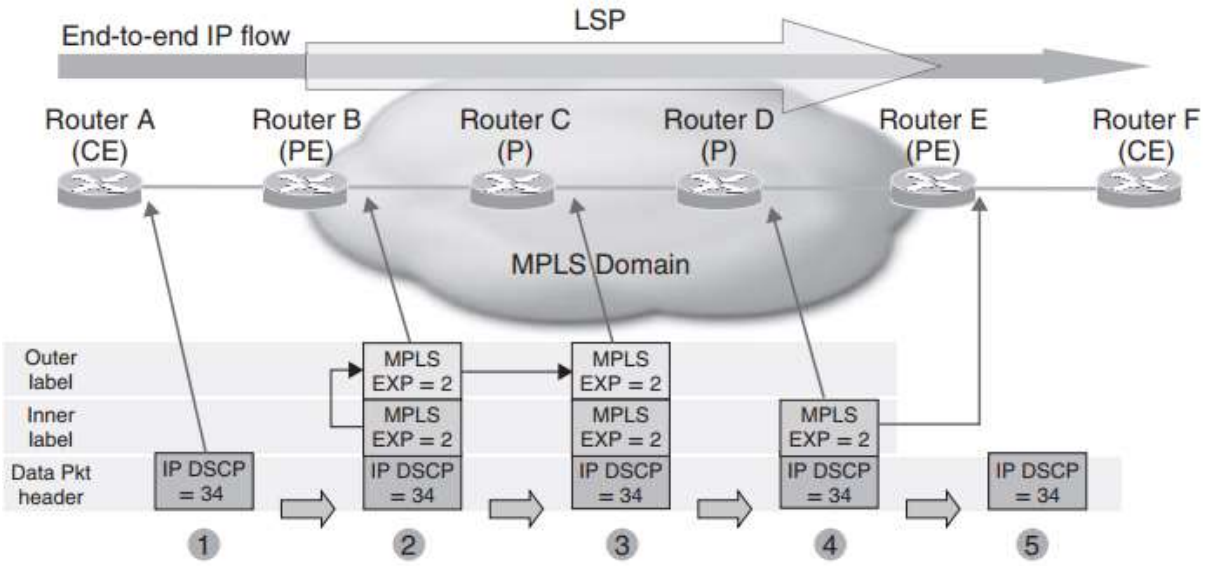
U praksi, nije uobičajeno ponovno označavanje (*re-marking*) unutar MPLS domene.Takve uvjetovane funkcije se obično izvode na rubu Diffserv domene. Dakle, jednoliki model se rijetko koristi u kontekstu MPLS-a, a [RFC 3270] ga definira kao neobaveznog.

MPLS Model Cijevi (*MPLS Pipe Model*)

Model cijevi za MPLS je konceptualno sličan IP slučaju tuneliranja, gdje se MPLS LSP-ovi koriste umjesto IP tunela, iako postoje neke razlike uzrokovane razlikama između IP-a i MPLS-a. Ako promatramo slučaj jedne razine labela (tj. bez stoga labela), MPLS model cijevi tretira DSCP oznake na donjem IP paketu i MPLS EXP oznake na LSP-u, korištene od strane paketa, kao nezavisne entitete. Na početku LSP-a, podešava se MPLS EXP polje; ovo podešavanje se može izvesti iz oznaka DSCP-a donjeg paketa u slučaju IP-do-MPLS-a prosljeđivanja, ili iz MPLS EXP polja primljene labele u slučaju MPLS-do-MPLS prosljeđivanja, gdje hijerarhija LSP-ova rezultira stogom labela. Putem kroz LSP, bilo kakva klasifikacija, označavanje i ponovno označavanje se izvodi samo uz pomoć EXP polja vanjske labele. Tamo gdje se gornja labela skine, na kraju LSP-a (ili na pretposljednjem skoku, ako se koristi PHP), MPLS EXP

vrijednost odložene oznake se ne kopira na DSCP donjeg IP paketa ili na EXP polje donje labele ukoliko smo imali tog labela.

Promotrite primjer prikazan slici 4 i slijedeći opis



Slika 4: MPLS Diffserv modeli tuneliranja: model ciljevi (pipe model)

U ovom primjeru, koji prikazuje IP-do-MPLS tranziciju, koristi se stog labela, koji bi npr mogao predstavljati MPLS VPN razvoj [kao u RFC 4364], gdje Multi-protokol BGP (MGBP) [RFC 2858] propisuje unutarnju oznaku, a LDP [RFC 3036] propisuje vanjsku oznaku. U primjeru se također pretpostavlja da se PHP koristi:

1. Van MPLS domene, npr. kod usmjerivača 1 pretpostavimo da su IP podatkovni paketi označeni sa DSCP 34 (tj. AF41).
2. Na ulazu u LER (Usmjerivač B), umeće se labelni stog te se podešavaju EXP vrijednosti oznaka. EXP vrijednost unutarnje labele može se izvesti iz DSCP vrijednosti DSCP-a donjeg paketa, ili može se odrediti neovisno o toj vrijednosti. U ovom primjeru, pretpostavljamo da je EXP vrijednost postavljena na 2 neovisno o DSCP-u donjeg IP paketa. Kao i u ovom primjeru, koristi se stog labela i EXP vrijednost unutarnje (npr. MBGP, u kontekstu MPLS VPN-a) labele se kopira uzbrdo kroz stog labela na vanjsku labelu (npr. onu postavljenu LDP protokolom), dakle, i unutarnja i vanjska labela imaju EXP vrijednost 2.
3. Posrednički usmjerivači na LSP stazi, npr. usmjerivač C, zamijeniti će labele paketa bazirano na vanjskoj vrijednosti labele dolaznog paketa.Kako se oznake paketa mijenjaju, EXP se kopira sa ulazne na izlaznu labelu, dakle u ovom primjeru, paket bi na izlazu prema Usmjerivaču C imao EXP vrijednost 4. Ako postoji stog labela, te ako EXP polje klasificira labelirane pakete, LSR će kontrolirati samo EXP polje vanjske labele.
4. Kako se PHP koristi u ovom primjeru, vanjska (npr. LDP) labela se skida na pretposljednjem LSR-u na LSP-u, u ovom slučaju, Usmjerivaču D. Iako je vanjska labela skinuta, unutarnja (npr. postavljena od MBGP) labela još ostaje, te će kod

klasifikacije labeliranih paketa od strane EXP polja, Usmjerivač D na izlazu kontrolirati samo EXP polje preostale labele.

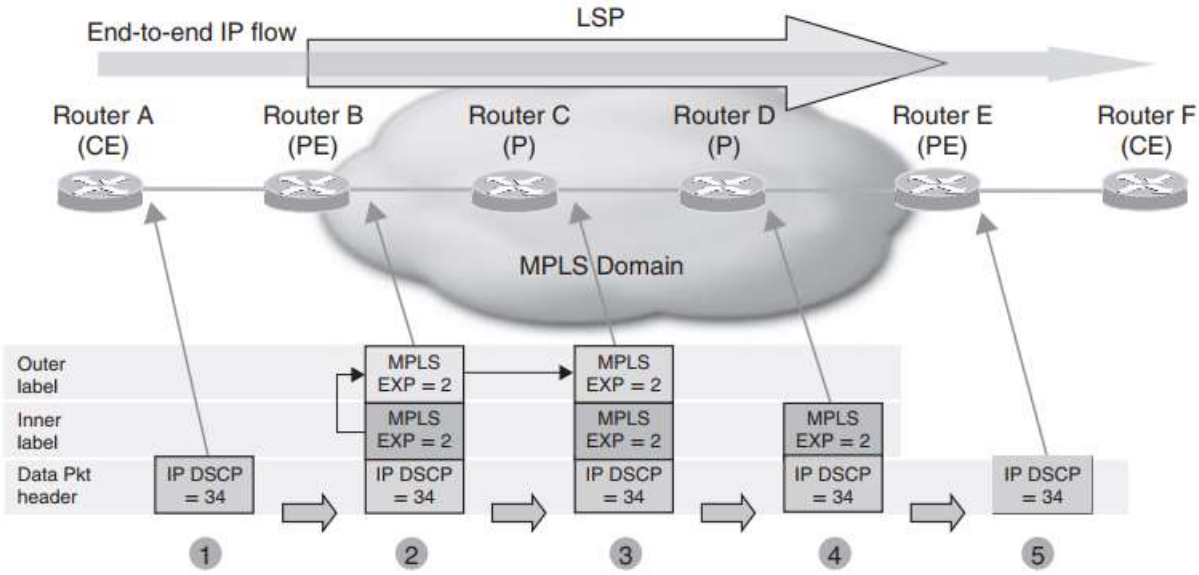
5. Usmjerivač E, izlazni LER, primiti će paket sa ovom jednom labelom (MBGP), koju će skinuti. Iako skida ovu labelu, „tunelski model cijevi“ definira da usmjerivač E zadržava vrijednost EXP polja na primljenoj oznaci, tako da može klasificirati (sad neoznačene) pakete na izlazu iz usmjerivača E u usmjerivač F. Kada se ne koristi stog labela, a koristi se PHP (penultimate hop popping), usmjerivač E ne prima labelirani već čisti IP paket, te nema EXP informacija koje bi zadržao i koristio za klasifikaciju na izlazu prema Usmjerivaču F! Stoga se„model cijevi“ ne može koristiti tamo gdje koristimo PHP bez stoga labela.

Model cijevi se često koristi u MPLS VPN razvojima te ga [RFC 3270] definira kao obaveznog!

Ulazni LSR tj. LER će obično kopirati bitove 0 do 2 DS polja na 3 bita EXP polja u MPLS labeli *po default-u*. Tipično *defaultno* ponašanje izlaznog LER-a jest ne kopirati EXP polje nadolje kroz stog labela ili na CS kodne točke pri skidanju labela.

MPLS Model Kratke Cijevi *(MPLS Short Pipe Model)*

Model kratke cijevi je varijacija modela cijevi; promotrite primjer u Ilustraciji 2.37 i slijedeći opis.



Slika 5: MPLS Diffserv načini tuneliranja: model kratke ciljevi

Koraci 1-4 za MPLS model cijevi opisan u Odjeljku prošlom odjeljku

Korak 5: Model kratke cijevi razlikuje se od modela cijevi u smislu ponašanja apliciranog na izlaznom LER-u; umjesto zadržavanja EXP vrijednosti primljene labele, vrijednost donjeg DSCP-a se koristi za klasifikaciju (sada ne-labeliranog) paketa na izlazu iz usmjerivača E u usmjerivač F.

IP multicast i QoS

Interserv i Diffserv IP QoS arhitekture su dizajnirane da podržavaju oboje, IP „unicast“ i IP „multicast“ promet.

IP Multicast i Diffserv

Potpora za osnovne mehanizme Diffserva nema razlike između one za IP multicast i za IP unicast. Multicast promet je određen odredišnom adresom paketa; osim toga, IP zaglavlja za multicast promet su ista kao i za unicast promet. Multicast replicirani paketi imaju točno isti DSCP kao i originalni paket, te će stoga biti tretirani sa istim PHBom kao i dolazni paketi njihove odgovarajuće multicast grupe. Dakle, DSCP polje se može koristiti za označavanje i klasificiranje prometa točno onako kao i što se za IP mogu koristiti unicast i Diffserv PHB-ovi.

Međutim, učinak multicast tokova prometa u mreži različit je od unicast tokova prometa; u pravilu, multicast tokovi su „točka-do-više točki“ ili „više točki-do-više točki“, jedna multicast struja iz izvora može biti replicirana na višestruke lokacije- dok su unicast tokovi točka-do-točke. Dakle, postoje dvije ključne razlike između unicast i multicast Diffserv -a:

- *Planiranje kapaciteta* u Diffserv mreži omogućuje osiguravanje dostupnih kapaciteta relativno na opterećenje mreže, potencijalno na bazi pojedine klase. Kod multicast razvoja, treba uzeti u obzir matricu prometa (matricu tokova od ulaza do izlaza), koja rezultira iz multicast replikacije. Planiranje kapaciteta se detaljnije raspravlja u Poglavlju 6.
- *Multicast SLA* - Ako primljeni unicast protok može biti ograničen na ulazu u mrežu,čime se može ograničiti učinak na mrežu, ali primljeni multicast protok se može replicirati na mnoge destinacije unutar mreže nakon primanja, te učinak na mrežu može biti uvelike pojačan. Bilo koja SLA definicija za Diffserv sposobne multicast servise moraju uzeti u obzir multicast replikacije unutar mreže.

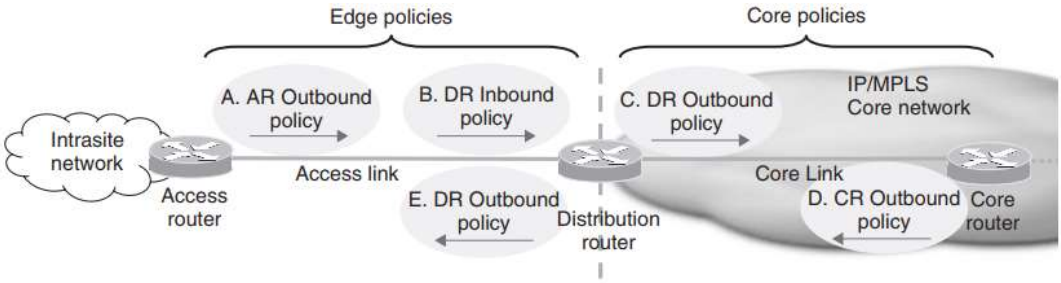
IP Multicast i Interserv/RSVP

Interserv [RFC 1633] i RSVP [RFC 2205] bili su u osnovi kreirani da opslužuju i multicast i unicast rezervacije. Posljedica je ta da RSVP daje fleksibilnu kontrolu nad načinima dijeljenja rezervacija niz grane multicast dostavnih stabala, koristeći „Wildcard Filter“ i „Shared-Explicit Filter“ stilove rezervacija da bi dopustili stapanje stanja rezervacija. Nadalje, RSVP dopušta osnovne akcije dodavanja ili brisanja jednog pošiljatelja i/ili primatelja prema ili od postojeće rezervacije.

Tipične Implementacije QoS usmjerivača u praksi

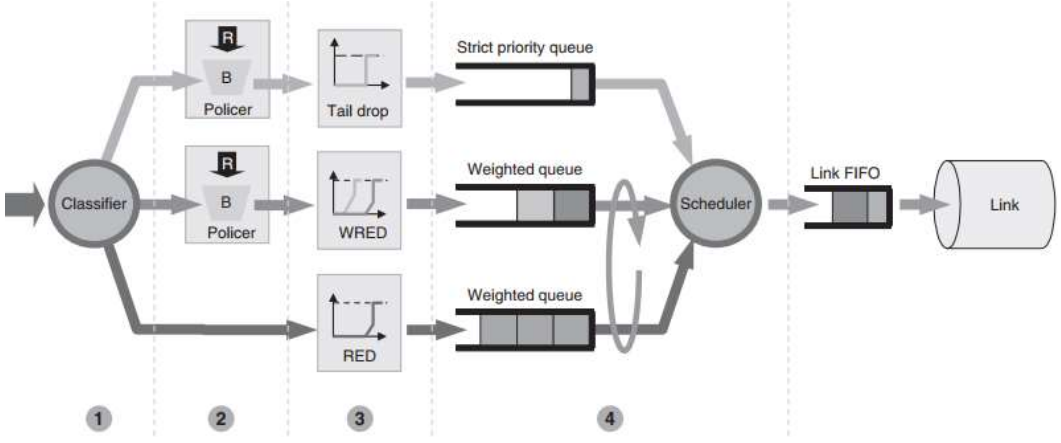
Diffserv je najšire korištena QoS IP QoS arhitektura i stoga je većina QoS implementacija usmjerivača optimizirana za Diffserv uporabu. Već smo opisali glavne podatkovne alate koji se koriste u IP QoS-u: klasifikacija, označavanje, usmjeravanje, stavljanje u red, raspoređivanje, odbacivanje i oblikovanje. U praksi, koja od ovih komponenti će se koristiti i kako će se kombinirati da kreiraju QoS politiku ovisi o tome gdje će unutar mreže biti primijenjeni- na rubu ili u jezgri- i da li će biti primijenjeni na izlazu prema sučelju ili na ulazu.

Mnoge mreže se grade sa hijerarhijom koja se sastoji od jezgrenih usmjerivača (CR-ovi), koji osiguravaju povezivost između distributivnih usmjerivača (DR-ovi), koji pak sakupljaju veze sa usmjerivača na udaljenim stranicama, a svaka od njih ima usmjerivače lokalnog pristupa (AR-ovi). Ako npr. promatramo Diffserv razvoj u ovom tipu mreže, kao što je prikazano na slici 6, pristupni link će obično biti rub Diffserv domene, sa rubnim nadgledanjem (*policy*) primjenjenim na pristupnom usmjerivaču (access router) i to na sučelju koje gleda prema jezgrenom dijelu mreže, nasuprot sučelju distribucijskog usmjerivača (koja može imati unutarnja nadgledanja u nekim slučajevima). Jezgrena nadledanja (policing) se tada obično vrše na izlazu prema jezgri i na izlaznim sučeljimana svim jezgrenim usmjerivačima.



Slika 6: Gdje se u mreži primjenjuje QOS nadgledanje

Kako se kompleksna klasifikacija i uvjetovanje izvodi na rubu Diffserv mreže, nadgledačkeQoS funkcijeprimijenjene na usmjerivače na rubu mreže (tj. pristupni i distribucijski usmjerivači) su obično kompliciranije nego one koje se koriste na jezgrenim usmjerivačima. Slika 7 pokazuje kako se različite Diffserv QoS komponente koriste zajedno u tipičnom AR QoS nadgledanju koje se primjenjuje prema vani na sučelju prema DR (tj. nadgledanje A (*policy A*) u slici 6).



Slika 7: Tipična QoS implementacija na pristupnum usmjerivaču

Promatrajući sliku 7 zaključujemo:

- Promet koji je određen za sučelje, prvo se klasificira pomoću jednostavne ili kompleksne klasifikacije. U ovom primjeru, pokazali smo tri klase, iako ih je moglo biti više ili manje.
- Najviša klasa prometa (dijagramatski) u slici 7 opslužuje se iz striktno prioritetnog reda, za najmanje kašnjenje i jitter; ovo će vjerojatno uključivati aplikacije kao što su glas i video. SR-TCM usmjerivač sa akcijom odbacivanja paketa u slučaju prekoračenja limita, primjenjuje se na klasu prije nego što se paketi stave u striktni prioritetni red, kako bi se osiguralo postizanje maksimalne brzine za tu klasu, te da bi se spriječilo da ova klasa iscrpi pojasni širinu za ostale klase.Paketi koje nadglednik *(policer*)odbaci, ne stavljaju se u red čekanja klase. Odbacivanje repa se koristi kako bi se nametnula maksimalna granica duljine reda čekanja, a tako postavila granica za maksimalno kašnjenje paketa nastalo uslijed čekanja u redu. Ograničenje duljine reda uz odbacivanje repa može ponekad biti nepotrebno tj. redundantno ukoliko primjenjujemo nadglednike jer će i sam nadglednik prije toga ograničiti tj. „popeglati“ praskove prometa, a na taj način indirektno će i ograničiti duljinu reda čekanja, tj. prouzročeno kašnjenje uslijed čekanja u redu.
- Srednja klasa prometa se opslužuje sa reda ponderirane pojasne širine. SR-TCM usmjerivač se može primijeniti na klasu prije nego što se paketi stave u red, da bi se uspostavila maksimalna brzina za ugovoreni promet unutar klase. Ovo se može postići npr. usklađenom akcijom prijenosa (ako promet nije prethodno markiran ovo se može kombinirati sa označavanjem unutar ugovora), te narušiti akciju prijenosa + označiti van ugovora. WRED se može koristiti za maksimalizaciju protoka za TCP aplikacije unutar klase te za primjenu drugačijih pravila odbacivanja paketa za ugovorni promet u odnosu na promet van ugovora, koristeći agresivniji WRED profil za promet van ugovora.
- Donja klasa prometa u Ilustraciji 2.39 se opslužuje iz ponderiranog reda pojasne širine. RED se koristi za maksimalizaciju protoka za aplikacije unutar klase bazirane na TCP-u.
- Raspoređivač osigurava da se gornja klasa tretira sa prikladnim prioritetom, te da srednje i crvene klase prime neki osigurani minimum pojasne širine, u skladu sa konfiguriranim težinskim faktorima.
- U većini praktičnih implementacija usmjerivača, hardver „linijski upravljač“(*"line driver*") će imati posla sa slanjem paketa na stvarnu liniju, a raspoređivač će opsluživati svoje redove postavljajući ih u redove hardverskog linijskog upravljača na izlaznom sučelju, poznatom kao FIFO sučelje.

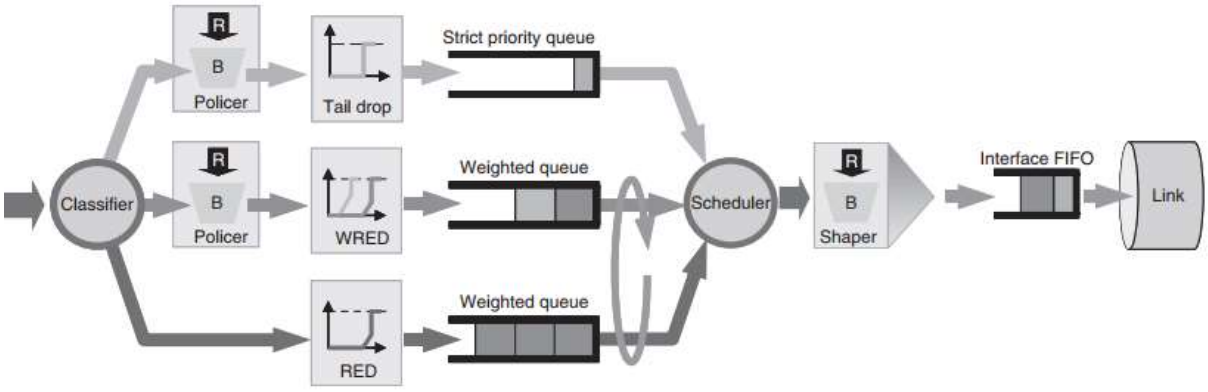
Iz navedenog opisa, razvidno je da postoji implicitni redosljed QOS akcija:

1. Prvo se provodi klasifikacija kako bi se odredila klasa paketa.
2. Nakon toga vrše se funkcije nadgledanja i označavanja temeljem pravila za svaku klasu.Paketi koji su odbačeni od strane nadglednika, neće biti stavljeni u red čekanja, pa samim time i neće biti podložni akcijama odbacivanja repa ili (W)RED odbacivanjima. Paketi ne bi trebali biti ponovno klasificirani u ostale klase na ovom koraku, inače bi postojala mogućnost petlje, kod koje se paket ponovno označava u

jednu klasu, zatim ponovno klasificira u drugu, gdje se također ponovno markira, i opet ponovno klasificira u drugu klasu itd.

3. Odbacivanje repa ili (W)RED odluke izvode se prije nego se paketi postave u odgovarajuće redove. Ukoliko su drugom koraku bila primjenjena pravila nadgledanja i označavanja, važno je da se WRED i pravila odbacivanja primjenjuju u skladu sa tim oznakama i pripadajućim pravilima.
4. Nakon tih akcija, dolazimo do donošenja odluka o raspoređivanju paketa i njihovu postavljaju u HW red na izlaznom FIFO sučelju.

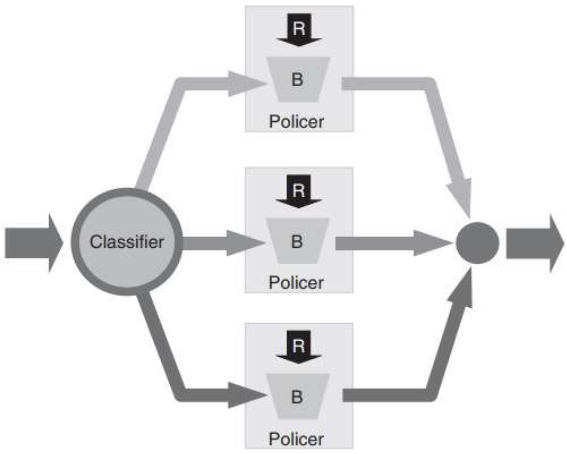
Gore opisana izlazna QoS implementacija mogla bi biti dalje nadograđena dodavanjem agregatnog oblikovatelja , tamo gdje,se zahtijevaju usluge ispod-linijske brzine, kao što prikazuje slika ispod.



Slika 8: Pristupni usmjerivač sa izlaznom QOS implementacijom sa ispod-linijskim oblikovanjem brizne

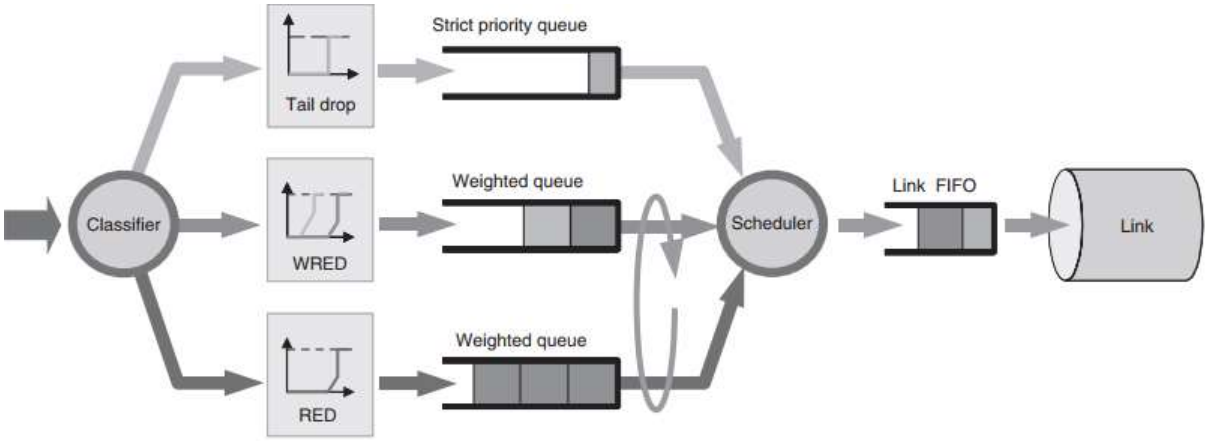
Izlazna QoS pravila (*policies*) iz DR usmjerivača na sučeljima usmjerenim prema AR-u će obično biti slična, samo bez primjene nadglednika na ponderirane redove pojasne širine, obzirom je taj promet već bio pod utjecajem uvjetovanja prometa na ulazu u Diffserv domenu.

Ovisno o određenim izvedbama, QoS pravila se mogu primjenjivati na ulazu u DR na sučeljima usmjerenim prema AR-u (tj. usmjerenje B u slici 6) da bi se izvelo uvjetovanje na ulazu u Diffserv domenu i touglavnom u slučaju kada pristupna veza predstavlja granicu „povjerenja“ između osiguravatelja mrežne usluge i klijenta. Konceptualno, izlazni (*egress*) pristup QoS implementacijama prikazan na slici 7 mogao bi također biti implementiran na ulazu (*ingress*) u usmjerivač, ali to u praksi nije često. Ulaz u sučelje rjeđe predstavlja točku združivanja za promet nego izlaz.Ako promet nije agregiran onda neće doći do zagušenja, te neće biti potrebe za implementacijom raspoređivanja ili postavljanja redova čekanja na ulazu u usmjerivač. Umjesto toga, na ulazu u sučelje usmjerivača uobičajenije je dati podršku samo primjenu pravila određene klase za izvođenje uvjetovanja (*per-class conditioning*), u slučajevima kada se SR-TCM ili TR-TCM primjenjuje na svaku klasu. Slika 9 prikazuje tipičnu QoS implementaciju koja se aplicira na promet na ulazu u distribucijski usmjerivač nasuprot AR sučelja (tj. usmjerivač B u slici 7).



Slika 9: Tipični QOS implementacija na ulazu u distribucijski usmjerivač

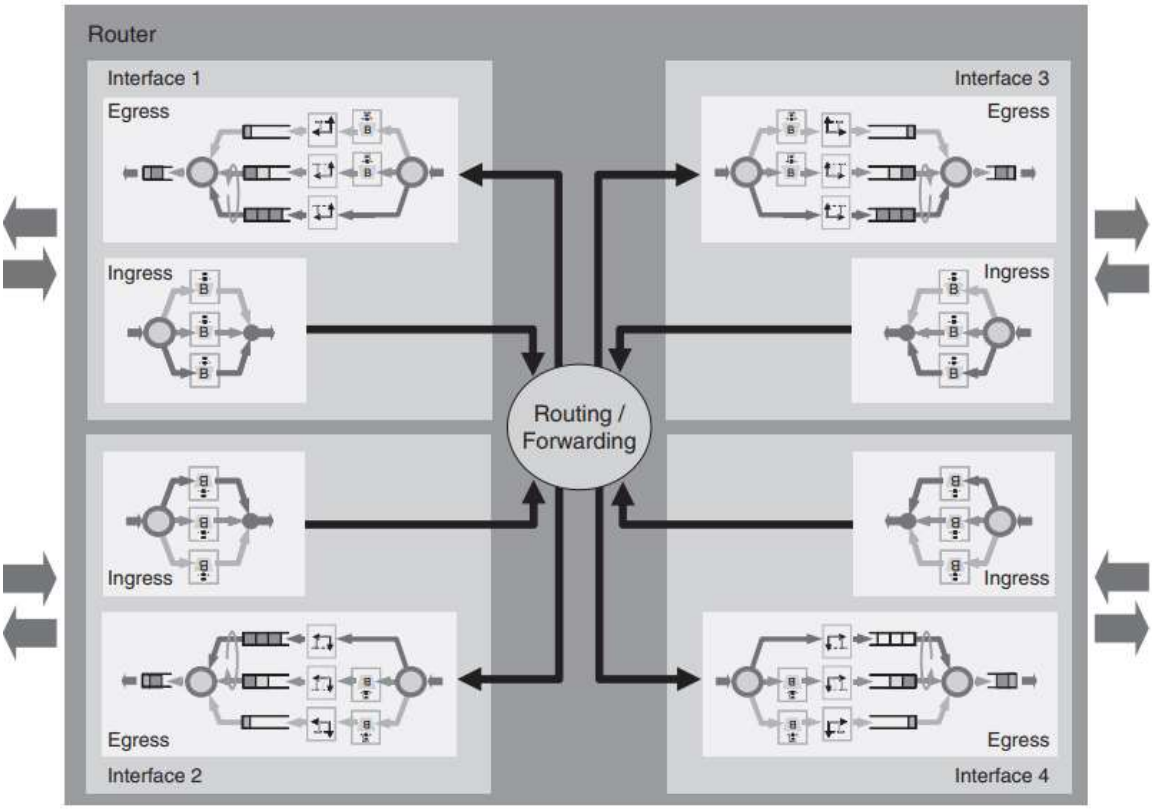
Tipična QOS implementacija na izlazu iz jezgrenog usmjerivača (tj. usmjerenje D na slici 6), kako je prikazano na slici 10, bi obično bila jednostavnija podpodjela implementacije pristupnog usmjerivača; bez nadglednika (*policer*s) koji se koriste na ponderiranim redovima pojasne širine, te bez potpore za oblikovatelje agregatnih tokova.



Slika 10: Tipična QOS implementacija izlaza iz jezgrenog usmjerivača

Ista implementacija bi također bila korištena na izlazu prema sučeljima okrenutim prema DR jezgri (tj. usmjerenje C na slici 6). Uglavnom ne postoje nikakva QoS pravila koja se koriste na ulazu u sučelja jezgre.

Kad promatramo cjelinu, tipična QoS implementacija distribucijskog usmjerivača koja podržava više pristupnih sučelja prikazana je na slici 11.



Slika 11: Tipična QOS implementacija distribucijskog usmjerivača

Ovisno o arhitekturi usmjerivača, QoS mehanizmi se mogu implementirati centralno u usmjerivaču, ili na distributivnim platformama, mogu biti implementirani na linijskim karticama sučelja. Na platformama, koje imaju centralizirani prespojni sklop, prespojni sklop može biti mjesto združivanja prometa te se mehanizmi stavljanja u red i raspoređivanja mogu implementirati na ulazu u sami prespojni sklop. Ako Diffserv EF/AF prosljeđujuća ponašanja imaju utjecaja na izvedbu prosljeđivanja usmjerivača, usmjerivač će podržavati manju brzinu agregatnog protoka sa omogućenim Diffservom, te će posljedično, cijena izvedbe mreže biti viša. Usmjerivači sa visokim performansomama obično implementiraju EF/AF prosljeđujuća ponašanja u ASIC-u, tako osiguravajući da nema degradacije prosljeđivačkih performansi povezanih sa potporom Diffserv funkcionalnošću.

QoS sloja 2

Iako je fokus ove knjige na IP QoS (tj. sloju 3), IP mreže koriste tehnologije podloženih slojeva 1 i 2 da bi osigurali povezivost između čvorišta sloja 3 (tj. usmjerivača). Stoga, u gradnji od-kraja-do-kraja usluga sa ugovorenim SLA obvezama, važno je da su tehnologije podloženih slojeva 1 i 2 kadra podržavati zahtjeve mreže potrebne za isporuku ugovorenih SLA-ova. Međutim, SLA-ovi dostavljeni na IP sloju su implicitno ograničeni SLA-ovima tehnologija podloženog sloja 2; npr., ne bi bilo moguće isporučiti IP uslugu koja podržava VoIP sa ograničenim kašnjenjem, jitter-om i gubicima paketa, koristeći podloženu mrežu sloja 2, koja nije osigurala SLA-ove za ograničenim kašnjenjem, jitter-om i gubicima paketabarem jednako dobro (obično i bolje) nego što je zahtijevano za IP uslugu, tj. ATM ABR uslugu.

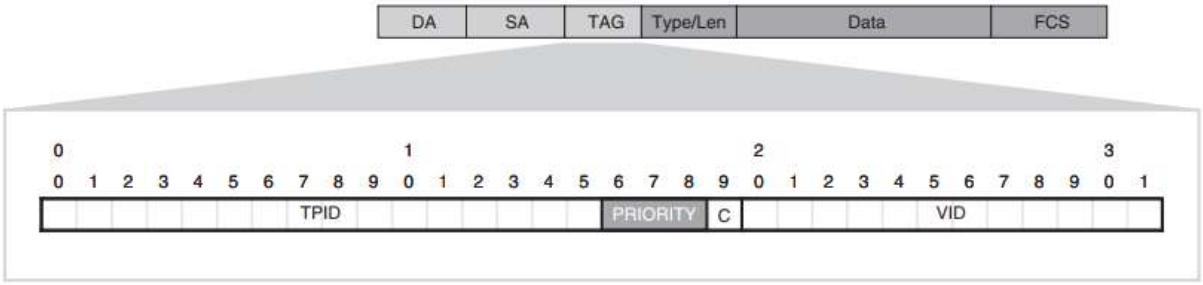
Neke od-točke-do-točke tehnologije drugog sloja, kao što su iznajmljene linije bazirane na TDM-u ili Sinkroniziranoj Optičkoj Mreži (SONET)/Sinkroniziranoj Digitalnoj Hijerarhiji

(SDH) mrežama, obično imaju dobro definirane SLA-ove na drugom sloju, koji su kadri podržavati aplikacije sloja 3 sa čvrsto određenim SLA zahtjevima. Takve veze obično imaju definirano kašnjenje, definiranu postotak greške bitova (BER) te određenu minimalnu pojasnu širinu pojasa na drugom sloju, što je obično jednako maksimalnoj pojasnoj širini za uslugu. U ovim slučajevima, Intserv ili Diffserv pravila za postavljanje u redove čekanja mogu se pridružiti direktno na sučelje koje predstavlja vezu; u slučaju primjene Diffserva pravila, prikaz bi bio sličan onome prikazanom na Ilustraciji 2.40.

Drugi načini se mogu primijeniti na više-pristupne tehnologije sloja 2, kao što su ATM, komutacija okvira i Ethernet, koje imaju neke svoje eksplicitne QoS sposobnosti na sloju 2; u takvim slučajevima od-kraja-do-kraja IP SLA-ovi se mogu postići suradnjom QoS funkcija sloja 3 i QoS podloženog sloja 2, što je opisano u slijedećim poglavljima.

Ethernet

Originalne IEEE 802.3 specifikacije za Ethernet ne uključuju nikakve odredbe za diferenciranu kakvoću usluge, tj. podržavaju samo jednu klasu usluga. Naredni 802.1Q [802.1Q] projekt u IEEE 802 standardnom procesu dodaje potporu za VLAN označavanje. Okvirni format 802.1Q dodao je i 4-bajtnu „VLAN oznaku“ originalnom Ethernet zaglavlju, od čega je 3 bita definirano kao „korisničko prioritetno polje“, kako je i prikazano na slici 12.



Slika 12: 802.1Q Format okvira. DA= adresa odredišta, SA= adresa izvorišta, FCS= slijed provjere okvira, TPID= identifikator oznaka protokola (16 bitova), PRIORITY= korisničko prioritetno polje (3 bita), C= kanonički indikator formata (1 bit), VID= VLAN identifikator (12 bitova)

Upotreba korisničkog prioritetnog polja, pripisivanje indikacije prioriteta svakom okviru, definirana je 802.1P projektom (te se naziva i „802.1P“ polje), a rezultati su spojeni u 802.1D [802.1D] Annex G. Korištenje korisnički prioritetnog polja je analogno upotrebi DSCP polja u IP i EXP polju u MPLS mreži. Polje se koristi za indikaciju „prioriteta“ okvira, koji se koristi za određivanje proslijeđujućeg ponašanja tog okvira na svakom mosnom skoku. Kako je polje dugo 3 bita može predstavljati 8 različitih oznaka.

Dodatak G 802.1D se smatra samo „informativnim“, te osigurava samo visoku razinu opisa ponašanja koje bi se trebalo primjenjivati, bazirano na oznakama korisničkog prioriteta. 802.1D Annex G priznaje da se svih 8 oznaka ne može koristiti u bilo kojem određenom razvoju te specificira striktno prioritetno ponašanje kao minimalnu implementaciju gdje je razvijeno samo nekoliko klasa. Priznaje potrebu za potporom rasporeda koji mogu osigurati minimalnu sigurnost pojasne širine gdje je podržan veći broj klasa. U praksi, kod interpretacije specifikacija, većina proizvođača Ethernet preklopnika (*switch*) danas podržava rasporede

Diffserv tipa, sa striktnim redom prioriteta (tj. Kao EF) i više ponderiranih redova pojasne širine (tj. Kao AF), kojima se mogu dodijeliti različite vrijednosti korisničkih vrijednosti.

Dakle, u praksi je često moguće koristiti ove sposobnosti i tretirati Ethernet mreže, koje su komponente mreža od-kraja-do-kraja, gotovo kao bilo koji drugi dio Diffserv domene, ali sa EF i AF sličnim ponašanjima, primijenjenim na temelju klasifikacije 802.1Q polja korisničkog prioriteta. Kod MPLS EXP polja, budući da je polje korisničkog prioriteta dugo 3 bita te stoga može predstavljati samo 8 različitih vrijednosti, dok postoje 64 moguće DSCP vrijednosti, pa kada se određena vrijednost korisničkog prioriteta koristi kao komponenta u od-kraja-do-kraja Diffserv mreži, može predstavljati grupu DSCP vrijednosti.

Komplementarne tehnologinje

Komplementarno sa IP QoS tehnologijama, postoji skup dodatnih tehnika i tehnologija koje su se razvile unutar IP tehničke zajednice te koje dalje omogućuju IP mrežama razvijanje sa ciljem potpore strogo određenim SLA obvezama. Iako ove tehnologije nisu detaljno obrađene u ovoj knjizi, u nastavku su nabrojane.

Brza IGP konvergencija

Razvoj u implementaciji i korištenju IGP-ova rezultiralo je značajnim poboljšanjima IGP vremena konvergencije, bez ikakvog kompromiosa sa stabilnosti upravljačkog protokola. Ovo je za rezultat imalo poboljšanje vremena konvergencije od nekoliko stotina milisekundi u dobro dizajniranim IP mrežama, što znatno smanjuje gubitke povezivosti nakon kvarova mrežnih elemenata (npr. link ili čvor). Ovo smanjenje vremena konvergencije omogućuje postavljanje ciljeva za većom dostupnošću te manje postotke gubitaka paketa koje se nude SLA kroz sve klase usluga. Zbog toga se brza IGP konvergencija također preporuča kao osnova za više-servisne IP mrežne dizajne.

Tehnologije brzog preusmjeravanja

Razvoji shema lokalne zaštite i za IP i za MPLS generički nazvano Tehnologije brzih preusmjeravanja (FRR) - omogućuju daljnja smanjenja gubitaka povezivosti nakon greški mrežnih elemenata.

MPLS brzo preusmjeravanje (*Fast Re-Routing*-FRR) i prometno inženjerstvo

Korištenje MPLS prometnog inženjeringa (*Traffic Engineering* - TE) za kontrolu pristupa biti će opisano je u slijedećim poglavljima, kao i upravljanje pojasnom širinom.

Situacije gdje primjena QoS mehanizama ne pomaže

U zaključku ovoga poglavlja, naglašavamo činjenicu da QoS nije lijek svim mrežnim boljkama. Nedvojbeno će biti slučajeva kada, i uz korištenje QoS mehanizama SLA zahtjevi neće moći biti ispunjeni u određenoj mreži, te će se i druge tehnike morati razmotriti.

Mrežni inženjering. U nekim slučajevima možda će biti potrebno ponovno izgraditi mrežu da bi se osiguralo da će SLA zahtjevi aplikacije biti ispunjeni. Npr., satelitska veza može biti zamijenjena zemaljskom mrežom, da bi se smanjilo kašnjenje s-kraja-na-kraj.

Inženjering aplikacija - Mogu postojati slučajevi kada je prikladnije (isplativije) ponovno izgraditi aplikaciju, ili način na koji aplikacija koristi mrežu, tako da se smanje mrežni zahtjevi SLA aplikacija, nego ponovno graditi mrežu da bi omogućila originalne zahtjeve aplikacije. Npr. ako se spremnik za eliminaciju varijabilnog kašnjenja na krajnjem video sistemu postavi nepotrebno široko, može nepotrebno pridonijeti ukupnom kašnjenju, što može povećati vrijeme promjene kanala ili VoIP odgovor iznad prihvatljivih granica. U ovom je slučaju pravi pristup rješavanju ovog problema reduciranje spremnika protiv smetnji na krajnjem video sistemu, a ne pokušavanje reduciranja kašnjenja mreže.

PREDAVANJE 9 – Resource reservation protocol (RSVP)

Što je i čemu služi RSVP protokol?

- Protokol za rezervaciju resursa (RSVP) je signalizacijski protokol mrežnoga sloja (3. sloj) koji omogućuje aplikacijama rezervaciju mrežnih resursa za usmjerene (unicast) i skupne (multicast) tokove podataka.
- RSVP protokol se koristi u hostovima i usmjerivačima za postavljanje zahtjeva za QoS i pružanjem specifičnih razina QoS-a za različite vrste podatkovnih tokova.
- RSVP protokol definira na koji način aplikacije postavljaju zahtjeve za rezervacijama resursa mreže, kao i za oslobađanje rezerviranih resursa mreže kada nisu više potrebni.
- RSVP protokol rezervira potrebne resurse u mreži u svakom čvoru na putu od izvora do odredišta podatkovnog toka.
- RSVP nije usmjerivački protokol (iako je protokol 3. sloja), već je prilagođen za rad sa postojećim standardnim usmjerivačkim protokolima.
- RSVP protokol u svojoj osnovnoj varijanti se rijetko koristi u današnjim telekomunikacijskim mrežama, ali od veljače 2003. godine je nadograđen sa TE (Traffice engineering) prometnim inženjerstvom, te je kao takav našao primjenu u QoS orijentiranim mrežama (poglavito u MPLS mrežama).

Kratki razvojni pregled:

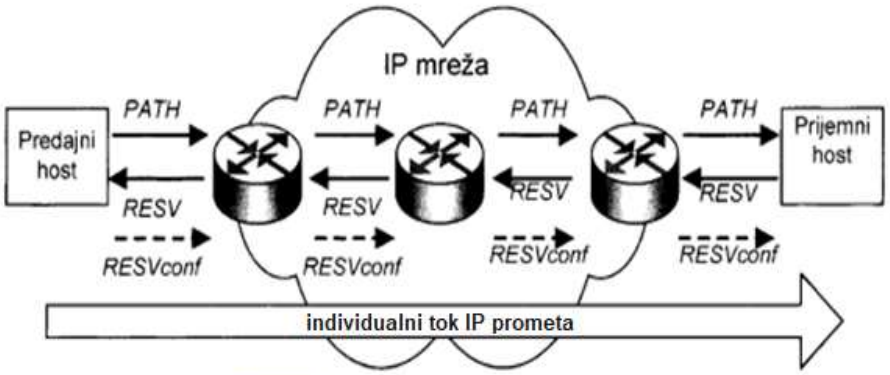
- RFC2205 : Verzija 1 RSVP protokola definirana je od strane IETF u rujnu 1997. godine. Sadržavala je samo upravljanje pristupom mreži (admission traffic control) temeljena samo na raspoloživosti potrebnih resursa
- Tek od RFC2750 je uvedena funkcija upravljanja pristupom mreži u potpunosti sa svim funkcionalnostima.
- RFC2210 definira upotrebu RSVP sa upravljanjem opterećenja prema RFC2211 i zajamčenim QoS upravljačkim uslugama prema RFC2212, te se uvodi se pojam Integriranih Usluga odnosno IntServ kao arhitekture koja određuje zajamčenu QoS kvalitetu usluge u mrežama.
- Protokol za rezervaciju resursa (RSVP) je signalizacijski protokol mrežnoga sloja (3. sloj) koji omogućuje aplikacijama rezervaciju mrežnih resursa za usmjerene (unicast) i skupne (multicast) tokove podataka.
- RSVP protokol se koristi u hostovima i usmjerivačima za postavljanje zahtjeva za QoS i pružanjem specifičnih razina QoS-a za različite vrste podatkovnih tokova.
- RSVP protokol definira na koji način aplikacije postavljaju zahtjeve za rezervacijama resursa mreže, kao i za oslobađanje rezerviranih resursa mreže kada nisu više potrebni.
- RFC3473 - u siječnju 2003. uvedeno GMPLS (Generalized Multi-Protocol Label Switching) proširenje sa RSVP-TE
- RFC3936 - u listopadu 2004. godine definirani su postupci za modificiranje RSVP-a temeljeno na najboljim modelima iz primjene u praksi

- RFC4495 - RSVP proširenje na „Smanjenje propusnosti rezerviranog toka“ (Reduction of Bandwidth of a Reservation Flow), da se omogući upravljanje propusnosti postojeće rezervacije u cilju smanjenja propusnosti, umjesto potpunog odbacivanja (tearing down) rezervacije i oslobađanja potrebnih resursa na mreži.
- RFC4558 - RSVP zasnovan na ID čvorova sa „Hello“ porukama među susjednim čvorovima

Glavne značajke RSVP protokola:

- RSVP postavlja zahtjeve za rezervacijom resursa mreže za usmjereno (unicast) i za skupno (multicast) odašiljanje jedan-na-više. RSVP se dinamički prilagođava promjenama pripadnosti multicast grupama, te promjenama ruta.
- RSVP je jednosmjerni (simplex), postavlja rezervacije na jednosmjerne tokove podataka.
- RSVP protokol nije usmjerivački, ali je prilagođen radu sa standardnim usmjerivačkim tokovima.
- RSVP je orijentiran ka prijemnoj strani na način da prijemnik pokreće i održava rezervaciju resursa za određeni tok podataka
- RSVP održava „meko stanje“ rezervacije resursa hostova i usmjerivača (na čvorovima mreže je potrebno periodično obnavljanje rezervacija), osigurava automatsku dinamičku prilagodbu promjeni pripadnosti multicast grupama kao i promjenama ruta na mreži.
- RSVP protokol definira rezervacijske stilove (svaki stil predstavlja skup rezervacijskih parametara), a u budućnosti je moguće dodavanje novih stilova prilagođenih zahtjevima novih aplikacija, kroz nove revizije protokola.
- RSVP omogućava transparentne operacije kroz usmjerivače koji ne podržavaju RSVP.
- RSVP podržava IPv4 i IPv6.
- Protokol za rezervaciju resursa (RSVP) je signalizacijski protokol mrežnoga sloja (3. sloj) koji omogućuje aplikacijama rezervaciju mrežnih resursa za usmjerene (unicast) i skupne (multicast) tokove podataka.
- RSVP protokol se koristi u hostovima i usmjerivačima za postavljanje zahtjeva za QoS i pružanjem specifičnih razina QoS-a za različite vrste podatkovnih tokova.
- RSVP protokol definira na koji način aplikacije postavljaju zahtjeve za rezervacijama resursa mreže, kao i za oslobađanje rezerviranih resursa mreže kada nisu više potrebni.

Osnovna specifikacija RSVP odnosi se na INDIVIDUALNI TOK IP PROMETA!!



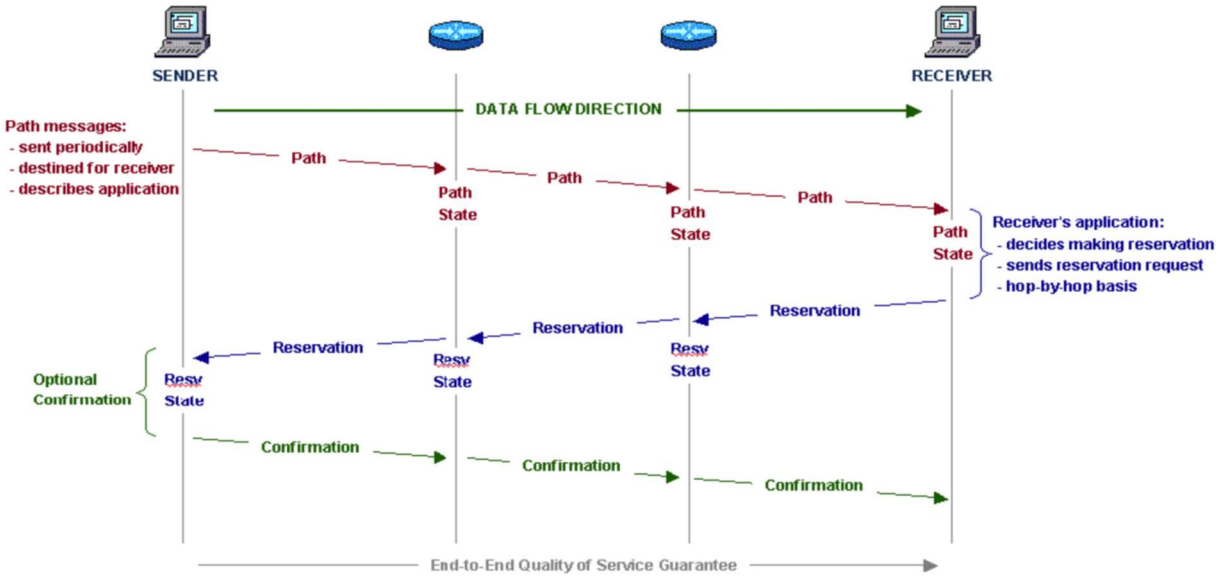
Jednostavni RSVP scenarij

Slika prikazuje jednostavni scenarij u kojemu promet teče od pošiljatelja do primatelja.

Na izlaznim linkovima prema prijamniku RSVP postavlja rezervacije za podatkovni promet. RSVP tretira tok podataka od prijemnika prema pošiljatelju kao logički neovisan o protoku od pošiljatelja prema primatelju. Prema tome, rezervacija za podatke od pošiljatelja do primatelja je nezavisna od rezervacije od prijemnika prema pošiljatelju. Budući da RSVP uspostavlja rezervaciju za jednosmjerne tokove, rezervacije prometovanja mogu biti u jednome (bilo kojem) ili u oba smjera.

RSVP je QoS signalizacijski protokol skok-po-skok. To znaci da se RSVP poruke prenose od jednoga čvora prema drugome kroz sve RSVP-podržane čvorove duž podatkovnoga puta.

Mehanizam uspostavljanja rezervacije prikazan je na slici



RSVP-a rezervaciji resursa u scenariju usmjerenoga odašiljanja odvija se u slijedećim koracima:

1. Računalo pošiljatelja obično poznaje karakteristike vlastitog prometa kojega odašilje preko mreže, kao što su brzina prijenosa podataka i odstupanje od brzina prijenosa podataka. Pošto prenosi podatke, pošiljateljev RSVP modul periodički šalje poruke RSVP puta (path messages), koje sadrže slijedeće:
2. Opisuju promet generiran od strane pošiljatelja
3. Održavaju stanje na svakom od među-RSVP-opremljenih čvorova duž podatkovnog puta. Poruke o stanju na putu šalju se s odredišnom adresom prema primatelju i preusmjeravaju se kako se podaci šalju prema primatelju.
4. Poruke o stanju na putu bilježe stanje puta u svakome usmjerivaču kroz koji prolaze. Pomoću ovoga mehanizma za uspostavu puta, svi uređaji na putu postaju svjesni svojih susjednih RSVP čvorova za protok podataka.
5. Kada RSVP modul prijamnika obavijesti svoju aplikaciju da je dobio RSVP poruku o stanju na putu, aplikacija prijemnika odlučuje hoće li rezervirati resurse.
6. Nakon donošenja odluke o zahtjevu za rezervaciju resursa mreže, aplikacija prijemnika šalje zahtjev lokalnome RSVP modulu za uspostavu rezervacije.
7. RSVP protokol zatim prenosi zahtjev kao Resv poruke prema svim čvorovima duž puta podataka, koji je usmjeren prema izvoru podataka. Rezervacija je napravljena na osnovi skokova, pa svaki posredni čvor provjerava ima li dovoljne resurse te odlučuje može li se zahtjev odobriti. Ako je rezervacija uspješna, postavlja se Resv stanje, a rezervacijski zahtjev se prosljeđuje prethodnome skoku na podatkovnome putu.
8. Primatelj može zatražiti obavijest o statusu rezervacije. U tome slučaju, kada pošiljatelj dobije Resv poruku od primatelja, on prijemniku šalje Resv poruku potvrde.
9. Ako primatelj ne šalje nikakve podatke, onda će početi slati poruku o stanju na putu prema pošiljatelju. U tomu slučaju, ponavljaju se koraci od 1 do 6 s prijemnikom u ulozi pošiljatelja, odnosno pošiljatelja u ulozi prijemnika.

Rezervacijski stilovi

Zahtjev za rezervacijom resursa obuhvaća skup parametara objedinjenih u „rezervacijski stil“.

- Jedna rezervacijska opcija se primjenjuje na sve rezervacije za različite pošiljatelje unutar iste sjednice: uspostavlja se zasebna rezervacija za svakog pošiljatelja podataka, ili se jedna rezervacija dijeli (shared) na sve pakete odabranih pošiljatelja.
- Druga rezervacijska opcija upravlja izborom pošiljatelja: to može biti izravan (explicit) popis odabranih pošiljatelja ili višeznačni (wildcard) popis koji obuhvaća sve pošiljatelje koji pripadaju istoj sjednici. U izravnom odabiru pošiljatelja, svaki filter mora određivati točno određenog pošiljatelja, dok kod višeznačnog odabira pošiljatelja nije potrebna specifikacija filtera.

Odabir pošiljatelja	Pojedinačni (distinct)	Dijeljeni(shared)
Izravni (explicit)	Fiksni filter (Fixed-Filter)	Dijeljeni-izravni filter (Shared-Explicit)
Višeznačni (wildcard)	(neodređeno)	Višeznačni filter (Wildcard-Filter)

Tablica : Rezervacijski atributi i stilovi

WF - Višeznačni filter (*Wildcard-Filter*) stil

- WF stil sadržava slijedeće opcije: dijeljena (shared) rezervacija i višeznačni (wildcard) odabir pošiljatelja.
- WF stil rezervacija stvara jednu rezervaciju koja se dijeli na podatkovne tokove od svih odabranih pošiljatelja.
- Ovaj tip rezervacije se može promatrati kao dijeljenje cjevovoda (pipe), čija veličina odgovara najvećem zahtjevu za rezervaciju resursa poslanom od svih pošiljatelja, neovisno o broju pošiljatelja koji cjevovod koriste.
- WF stil se širi do svih pošiljatelja, i automatski se proširuje na nove pošiljatelje ako dođe do njihove pojave na mreži.

FF - Fiksni filter (*Fixed-Filter*) stil

- FF stil sadržava slijedeće opcije:

- pojedinačne (*distinct*) rezervacije i
- izravno (*explicit*) odabrani pošiljatelji.

➢ Stoga u osnovi FF rezervacijski stil zahtjeva pojedinačne rezervacije resursa za pojedinačne pošiljatelje, ne dijeleći rezervacije resursa sa drugim pošiljateljima iz iste sjednice.

➢ Ukupna rezervacija resursa je zbroj svih pojedinačnih rezervacija pojedinih pošiljatelja.

SE – Dijeljeni izravni (*Shared-Explicit*) stil

➢ SE stil sadržava slijedeće opcije:

- dijeljena rezervacija i
- izravno (*explicit*) odabrani pošiljatelji.

➢ SE rezervacijski stil generira jednu rezervaciju koja se dijeli na odabrane pošiljatelje. Za razliku od WF stila, SE stil dozvoljava prijemniku izravno određivanje popisa pošiljatelja.

Primjena stilova

➢ Dijeljene rezervacije, generirane WF i SE stilovima, prikladne su za skupne aplikacije (multicast) u kojima je malo vjerojatno da će svi pošiljatelji odašiljati istovremeno.

➢ Paketizirani zvuk je dobar primjer aplikacije prikladne za dijeljene rezervacije. Kako ograničen broj ljudi razgovara istovremeno, svaki prijemnik može izdati WF ili SE rezervacijske zahtjeve za dvostrukom većom propusnosti po pošiljatelju (*over-speaking*).

➢ S druge strane, FF stil je prikladniji kod prijenosa videa, jer se rezervacije kreiraju pojedinačno za tokove od različitih pošiljatelja

RSVP-TE primjena u mpls mrežama

DiffServ arhitektura predstavlja efikasno i skalabilno rješenje za osiguranje QoS u IP mrežama.

U cilju optimiziranja prijenosnih resursa, ova arhitektura se kombinira sa MPLS tehnologijom koja omogućuje TE funkcionalnosti kao što su rezervacija resursa, tolerancija na pogreške i optimizacija iskorištenosti resursa.

Integracija DiffServ i MPLS arhitekture predstavlja atraktivno rješenje problema osiguranja QoS za više medijski promet uz efikasno iskorištenje mrežnih resursa.

Jedan od najvećih izazova ove arhitekture je odabir signalizacijskog protokola, s obzirom da ne postoji generički signalizacijski protokol.

Standardizirana su tri signalizacijska protokola koja se mogu koristiti u MPLS mrežama:

- Label Distribution Protocol (LDP),
- Constraint-based Routing Label Distribution Protocol CR-LDP
- **RSVP-TE**

Kako LDP pruža jedino osnovne funkcionalnosti i ne podržava TE mehanizme, ne može se koristiti u DS-TE mrežama.

Preostala dva rješenja omogućavaju TE funkcionalnosti kao što su uspostava Label Switched Path (LSP), rezervacija propusnog opsega za LSP, te Fast Re-routing (FRR) mehanizmi, što predstavlja ključ za ispunjavanje QoS zahtjeva.

U praksi se preferira proširivanje postojećih protokola kada god je to moguće, prvenstveno zbog napora koji je potrebno uložiti u dizajn, standardizaciju, razvoj i otklanjanje pogreški novih protokola.

Iz tog razloga je RSVP-TE odabran kao MPLS signalizacijski protokol, dok se odustalo od daljnjeg razvoja CR-LDP protokola.

RSVP-TE koristi RSVP poruke za uspostavu, održavanje (osvježavanje) i prekid TE LSP-a, te signalizaciju pogrešaka.

RSVP-TE se koristi u MPLS okruženju koje se razlikuje u odnosu na okruženje za koje je dizajniran originalni RSVP.

U MPLS mrežama ne dolazi do česte i brze promjene LSP-a.

Kao rezultat, RSVP-TE ne mora manipulirati velikim brojem novih ili modificiranih poruka. Većina razmijenjenih poruka predstavljaju poruke osvježavanja, koje se upravljaju mehanizama definiranim u preporuci RFC2961.

Radi svega navedenog RSVP protokol predstavlja primarni QoS signalizacijski protokol u IP mrežama.

Osnovna načela RSVP-TE u MPLS mrežama

Razvoj RSVP-a potaknut je definiranjem IntServ arhitekture, ali pošto je RSVP protokol u osnovi modularan, to ga čini neovisnim o arhitekturi, te se može primjenjivati i u drugim signalizacijskim aplikacijama. Tako mreže mogu koristiti RSVP prilikom uspostave LSP-a.

RSVP modul komunicira sa 2 lokalna modula:

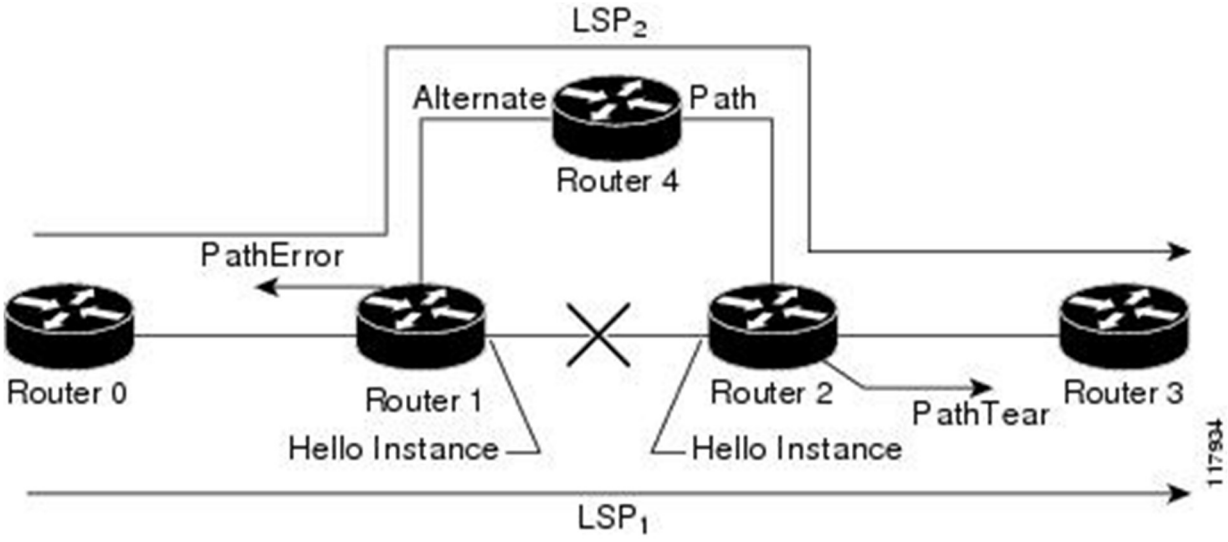
- Upravljanje pristupom mreži (*Admission control*) koji određuje ima li čvor dovoljno raspoloživih resursa da osigura zahtijevani QoS
- Upravljački skup pravila (*Policy control*) osigurava autorizaciju QoS zahtjeva.

RSVP koristi koncept sjednica sa određenim brojem pošiljatelja i primatelja. RSVP sjednica obuhvaća tok podataka s točno određenim odredištem i protokolom transportnog sloja. U slučaju višeodredišnih (multicast) destinacija, sjednica može obuhvaćati više rezervacija. Rezervacije su jednosmjerne. RSVP se temelji na periodičnoj transmisiji i obradi Path i Resv poruka za uspostavu i održavanje rezervacija. Pošiljatelji generiraju Path poruke, primatelj rezervira potrebne resurse na mreži Resv porukama, koje mrežni čvorovi prosljeđuju skok-po-skok metodom do pošiljatelja. ResvConf poruka se šalje primatelju kao potvrda uspješne rezervacije resursa. RSVP protokol također posjeduje mehanizam za **eksplicitni prekid rezervacije**, što ubrzava odziv protokola u odnosu na istek vremenskog intervala tzv. *mekog-stanja*. RSVP porukama *PathTear* i *ResvTear* prekida *meko-stanje*

RSVP protokol također definira i poruke ResvErr i PathErr za notifikaciju pogrešaka.

Poruke *Bundle* i *Srefresh* reduciraju količinu informacija, koje razmjenjuju susjedni čvorovi u mreži radi osvježavanja *mekog-stanja* na mreži, na način da u sebi sadrže više standardnih RSVP poruka grupiranih u jednu poruku.

U novijim revizijama RSVP protokola koriste se Hello poruke preko kojih se na brz način otkriva ispad susjednih RSVP čvorova



Problemi kod prijenosa RSVP poruka

- RSVP nema mehanizam kontrole isporuke poruka, te se kod gubitka poruka na retransmisiju čeka vrijeme isteka intervala osvježavanja *mekog-stanja* od 30 sekundi. Ovo se rješava uvođenjem timer mehanizma osvježavanja na način da se vrši retransmisija dok prijemni čvor ne potvrdi prijem poruke.
- Svaka RSVP poruka nosi informaciju o samo jednoj sjednici.
- U mrežama sa velikim brojem RSVP sjednica može doći do preopterećenja usmjerivača i potencijalnog zagušenja na mreži. Ovo se rješava mehanizmom reduciranja poruka između susjednih čvorova.
- Ako veličina RSVP poruke prelazi MTU, poruka se fragmentira i za ovo ne postoji rješenje. Usmjerivači ne mogu obrađivati fragmente RSVP poruka.

Nedostaci RSVP protokola

- Resv stanja se moraju održavati u svakom usmjerivaču za svaku sjednicu.
- RSVP optimizira različite operacije spajanja poruka prilikom višeodredišnih (multicast) rezervacija što izaziva obradu velikog broja Resv poruka.
- Signalizacijske poruke se ne koriste samo za održavanje stanja, nego i za rješavanje problema gubitka poruka, kao i za otkrivanje promjena putanja. Obrada svih ovih dodatnih poruka nije zanemarivo opterećenje za usmjerivače.
- RSVP koristi iste Path i Resv poruke za iniciranje novih i osvježavanje postojećih rezervacija na mreži, što rezultira povećanjem veličine poruka osvježavanja.
- Ovo se reducira skok-po-skok metodom, ali istodobno može utjecati na povećanje broja izvora pogrešaka.
- Preporukom RFC2961 se reducira redudantnost osvježavanja uvođenjem novog tipa RSVP poruka (Bundle, Srefresh).

Prednosti RSVP protokola

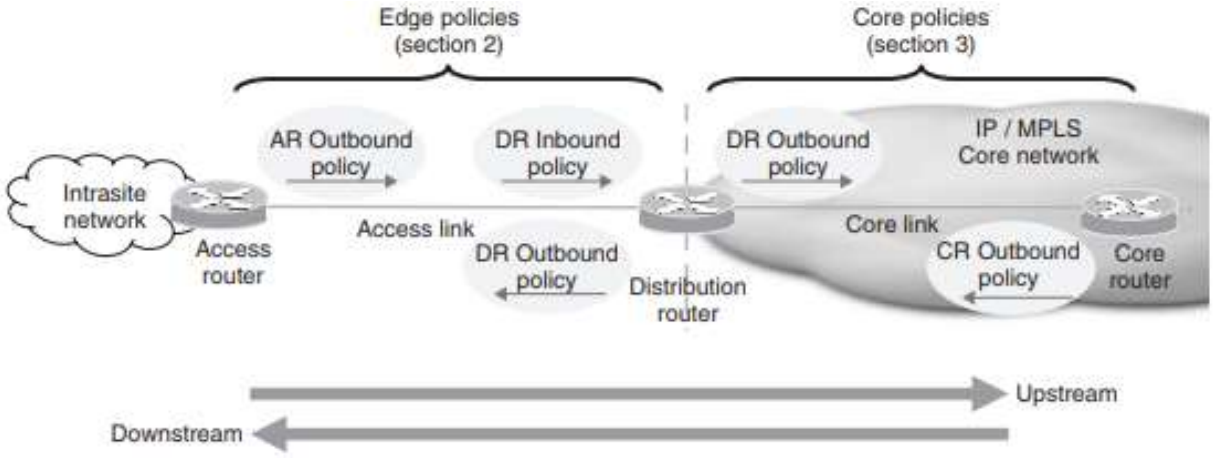
- Najveća prednost RSVP protokola je u mogućnosti aplikacije da točno definira rezervacijske zahtjeve za rezerviranje resursa na mreži, te da za prihvaćenu rezervaciju dobije čvrstu garanciju kvalitete usluge.
- Dodatne prednosti RSVP protokola su: pouzdanost, prilagodljivost i dinamička promjena rezervacije *mekog-stanja*.
- Prilagođenost primatelju je važna prednost RSVP protokola, naročito za višeodredišne skupine (multicast).
- QoS upravljački uređaji određuju kako postaviti parametre mreže da se postigne tražena kvaliteta usluge, dok RSVP pruža mogućnost distribucije tih parametara.
- RSVP tretira QoS parametre kao nevidljive poruke koje se isporučuju usmjerivačima, koji ih interpretiraju po potrebi. Ovakvo logičko odvajanje QoS kontrolnih uređaja i sredstava za distribuciju pojednostavljuje RSVP tako da je postao prilagodljiv novim, budućim mrežnim tehnologijama i promjenama istih.

PREDAVANJE 10 – Uvođenje DiffServ arhirtekture

SLA zahtjeve zadovoljavamo pomoću QoS mehanizama te arhitektura koje se koriste u mrežnom inženjerstvu a najraširenija je Diffserv. Posebno je raširena u mrežama privatnih korporacija i mrežama pružatelja usluga (*Service provider*) koji poduzećima osiguravaju VPN (*VirtualPrivateNetwork*) usluge.

Temelj rada Diffserva je da on svakom paketu dodjeljuje određenu/e klasu/e u svrhu udovoljavanja SLA zahtjeva.

- Diffserv se može primjeniti na rubu i u jezgri mreže.
- Rub Diffserv domene predstavlja granicu između klijenta i pružatelja usluga.
- „Politike" koje se primjenjuju na rubu mreže su kompleksnije od onih koje se primjenjuju u jezgri.
- Na rubovima Diffserv mreže, vrši se klasifikacija i uvjetovanje prometa izvođenjem kompleksnih Qos funkcija po klijentu.
- U jezgri mreže, gdje su propusnosti veza velike (ali i količina prometa), SLA zahtjevi za klasu prometa se mogu okarakterizirati kao zahtjevi za širinom pojasa, i problem SLA garancija može se učinkovito svesti na osiguravanje dovoljne širine pojasa, koja može biti na bazi pojedine klase ili usluge.



Mreže su hijerarhijski građene tako da se sastoje od jezgrenih usmjerivača CR (*Core Routers*), koji povezuju distributivne usmjerivače DR (*Distribution Routers*), a oni povezuju skupine usmjerivača tj. mreže na udaljenim mjestima, od kojih svaka ima lokalni pristupni usmjerivač AR (*Access Routers*).

Kod Diffserv dizajna pokušavamo zadovoljiti sljedeća tri cilja:

- Osiguravanje ispunjavanja različitih SLA zahtjeva za svaku odgovarajuću klasu
- Optimizacija korištenja pojasne širine
- Zadržavanje jednostavnosti dizajna koliko je god moguće

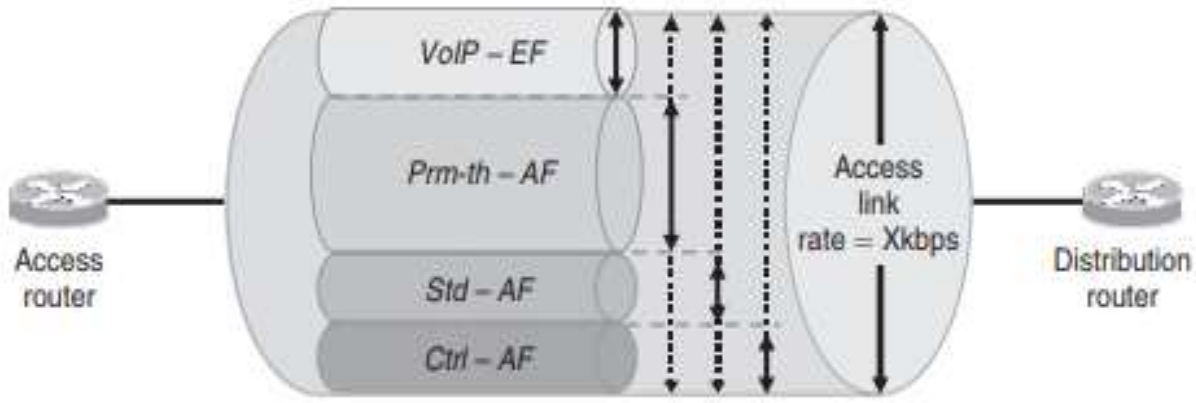
Razvijanje DiffServ-a na rubu mreže

Postavlja se pitanje zašto je „rub" važan za ispunjavanje SLA obveza.

U svakoj mreži postoji izbor da li koristiti QoS mehanizme, pa tako i kod mreža koje definira Diffserv. Da bi podržavali usluge i aplikacije sa strogim SLA zahtjevima bez QoS mehanizama, dostupni kapacitet trebao bi biti pre-kapacitiran u odnosu na maksimalni ponuđeni promet. Međutim, iako su se s vremenom na rubu mreže pristupne brzine povećale, a troškovi smanjili, zahtjevi aplikacija za pojasnim širinama postaju sve veći i veći, te „prekapacitiranost" pokazuje da nije održiva u praksi.Troškovi pristupnih veza su značajna komponenta mrežnih troškova te klijenti, da bi smanjili rashode, često odgađaju unapređivanje tih veza što je duže moguće; posljedično, pristupne veze su često nisko dimenzionirane i sklone zagušenju. Ako se ne osigura rješavanje zagušenja, podržavanje "real time" usluga sa strogim zahtjevima kašnjenja, smetnji i gubitka bit će nemoguća u slučajevima kada dolazi do zagušenja.

Uzmimo slučaj gdje koristimo liniju brzine od X kb/s a koja povezuje AR (*Access Router*) i DR (*Distribution Router*) i gdje se podržavaju četiri usluge svaka sa različitim SLA-om:

1. **VoIP klasa** - Ova klasa cilja na interaktivne aplikacije sa zahtjevima definiranja pojasne širine, niskog gubitka, i strogih zahtjeva za kašnjenje.
2. **Premium podatkovna klasa** sa optimiziranim protokom (Prm-th) - Ova klasa cilja na poslovne aplikacije koje bi trebale dobiti prioritetni pristup raspoloživim pojasnim širinama, ali koje nemaju definiran zahtjev za kašnjenjem; Npr. ovo može uključivati aplikacije prijenosa poslovno rizičnih dokumenata.
3. **Standardna klasa (Std)** - Standardna klasa koristi se za sav drugi promet, koji nije već bio klasificiran kao VoIP ili Prm-th. Na primjer, ova klasa se može koristiti za e-mail i web aplikacije.
4. **Kontrolna klasa (Ctrl)** - Pružatelji usluga (ISP) koriste Ctrl klasu, a posvećena je kontroli mrežnog prometa osiguravajući da je propusnost pristupne veze zagarantirana za osnovne funkcije kao što su usmjerivački protokoli i telnet ili SNMP pristup AR-u. Postojanje ove klase osigurava da zagušenje pristupne veze koju uzrokuje klijent, ne može utjecati na sposobnost SP-a da se nosi sa isporukom usluge.



Prikaz primjene Diffserv-a u slučaju kada davatelj usluga posjeduje i upravlja sa AC usmjerivačem

VoIP klasa

- SP i klijent obostrano pristaju na ugovor koji definira predviđenu ulaznu brzinu ICR (*Ingress committed rate*) od stranice klijenta do SP-a i postignutu izlaznu brzinu ECR (*Egress committed rate*) od SP-a do stranice klijenta.
- SP „osigurava" ugovor ograničavanjem brzine VoIP prometa prema/od stranice klijenta koristeći mehanizam „spremnika žetona" sa brzinom Rv i predviđenom širinom praska By, te će SP odbaciti neodgovarajući promet.
- Klijent će odabrati brzinu Ry a SP će ga ponuditi do definiranog postotka brzine pristupne veze. SP će obično ograničiti maksimalni postotak pojasne širine pristupne veze koji je dostupan za ovu klasu da bi osigurao da se predviđeno kašnjenje klase može postići.
- Također će postojati i definirana minimalna brzina veze, ispod koje SP neće nuditi ovu klasu, npr. 256 kb/s, zbog povećanog kašnjenja serijalizacije zamišljeno kašnjenje za ovu klasu ne može se postići na nižim brzinama.
- By će biti postavljen na temelju ponuđene obveze kašnjenje klase; maksimalna vrijednost praska učinkovito ograničava maksimalno kašnjenje prometa u klasi.
- Za „prilagođeni promet" SP će garantirati maksimalno jednosmjerno rubno segmentno kašnjenje, Lv.
- Rubno segmentno kašnjenje je samo jedna komponenta kašnjenja s-kraja-na-kraj koja utječe na VoIP poziv.
- Dakle, prije definiranja rubnog segmentnog kašnjenja, mora biti definirano maksimalno prihvatljivo kašnjenje s-kraja-na-kraj za određenu VoIP uslugu.
- Mrežni QoS dizajn bi tada trebao uzeti ovaj proračun i raspodijeliti ga na različite komponente mrežnog kašnjenja (propagacijsko kašnjenje kroz jezgru, kašnjenje u redovima zbog zagušenja, te serijalizacija kašnjenja pristupne veze) i kašnjenja krajnjih korisnika (uzrokovano VoIP kodekom i de-jitter spremnikom).

Primjer proračuna raspodijele VoIP kašnjenja:

- Pretpostavlja se da ciljano kašnjenje s-kraja-na-kraj iznosi 100 ms,
- Dodajući značajnih 50 ms sigurnosne granice na G.114 postižemo ciljanih 150 ms da bi se osiguralo da većina korisnika bude vrlo zadovoljna.
- Treba imati na umu da u mnogim situacijama mogu postojati dodatna kašnjenja uzrokovana tandemskim kodiranjem (ponovljeno kodiranje i dekodiranje signala), što se treba uzeti u obzir u ukupnom proračunu kašnjenja.

- Također mogu postojati slučajevi gdje se usluga može protezati višestrukim mrežama, a određena mreža "posjeduje" samo dio ukupnog s-kraja-na-kraj proračunatog kašnjenja, dakle u praksi je često vrlo važno smanjiti kašnjenje u svim dijelovima mreže kada se koriste VoIP usluge.

Nadalje, oduzmimo značajne doprinose fiksnim komponentama kašnjenja od proračuna kašnjenja s-kraja-na-kraj, i utvrdimo ostatak, koji se dodjeljuje raznim komponentama kašnjenja:

- 25 ms se oduzima zbog kašnjenja kodeka, pretpostavljajući G.711 -20 ms. Drugi kodeci mogu uzrokovati veće kašnjenje i tako zauzeti veći proračun kašnjenja s-kraja-na-kraj; kodeci nižih propusnosti (tj. veće kompresije) obično uzrokuju veće kašnjenje.
- Interval paketizacije jasno utječe na kašnjenja kodeka, dakle veći intervali paketizacije će implicitno rezultirati većim kašnjenjima kodeka.
- Propagacija kašnjenja se često proračunava za najveću udaljenost u mreži.
- U ovom primjeru pretpostavljamo da je minimalno kašnjenje po hopu relativno zanemarivo, što ne mora uvijek biti slučaj; a ako nije, onda ga je potrebno uključiti u proračun naveden iznad.

Dakle, ostatak koji se treba raspodijeliti na različite komponente kašnjenja jest:

- **Proračun s-kraja-na-kraj** **100 ms**
- Propagacija veze -40 ms
- Primjer kašnjenja kodeka -25 ms
- Preostalo za proračun promjenjivog kašnjenja (jitter) 35 ms

Dodijeljujemo 5 ms proračuna promjenjivog kašnjenja na jezgru, gdje su brzine veza veće nego pristupne.

Ovo ostavlja 30 ms proračuna promjenjivog kašnjenja za pristupne veze; 15 ms se dodjeljuje na ulaz, a 15 ms na izlaz.

- Dakle, Lv se kreće u rasponu od 15 ms do 50 ms, ovisno o određenom zamišljenom kašnjenju s-kraja-na-kraj, i proračunu kašnjenja za specifični mrežni dizajn. Lv se obično specificira za definiranu veličinu paketa.
- Za VoIP klasu nude se omjeri gubitka s-kraja-na-kraj manji od 0.1%.
- Jednom klasificiran i usmjeren, prilagođeni promet će biti označen sa Diffserv vrijednošću kodnih točaka (DSCP) - **Dv**.

Prm-th klasa

- SLA za Prm-th klasu se definira u smislu određene pojasne širine i dostupnosti sa obavezom čuvanja slijeda toka. Jitter nije važan za ovu klasu te nije definiran.

- SP se obavezuje na minimalnu širinu pojasa za klasu, Rt, koja se obično namješta na 80% do 90% preostale pojasne širine pristupne veze, nakon što se usluži VoIP klasa.
- Budući da Prm-th klasa ima veću raspodjelu pojasne širine od Std klase, pa ako postoje jednaka ponuđena opterećenja u obje klase, promet u Prm-th klasi trebao bi dobiti bolju uslugu. Ovo krajnjem korisniku daje mogućnost dodjeljivanja nekih aplikacija Prm-th klasi, tako da dobiju bolju uslugu nego aplikacije u Std klasi.
- Prm-th klasa je sposobna za ponovno korištenje neupotrjebljene pojasne širine iz bilo koje druge klase, sve do dostupne pojasne širine. Zbog toga su klasa kašnjenja i gubitka ovisni o stvarnom ponuđenom profilu prometa klijenta za klasu, što je van kontrole SP-a.
- Dostupna propusnost klase za aplikacije bazirane na TCP-u ovisi o stvarnom omjeru gubitka i RTT-u kojeg doživljava promet unutar klase.
- Ugovor će također definirati kriterij klasifikacije kojega će SP koristiti da bi identificirao klasu i odredio da će prilagođeni promet biti označen sa definiranom DSCP vrijednošću, - **Dt**.

Std klasa

- Kod Std klase SLA se definira u smislu određene pojasne širine, dostupnosti, i obaveze za očuvanje slijeda toka. Jitter nije važan za ovu klasu.
- SP se obvezuje na minimalnu pojasnu širinu klase, Rs, koja je obično postavljena na 10-20% od preostale pojasne širine pristupne veze, nakon što se VoIP klasa usluži.
- Ova klasa može ponovno koristiti neupotrjebljenu pojasnu širinu bilo koje druge klase, sve do pojasne širine dostupne mreže.
- Kao i kod Prm-th klase, SP ne osigurava obavezu za kašnjenje i gubitak za Std klasu na rubu mreže.
- Dostupna propusnost klase opet ovisi o stvarnoj stopi gubitka i RTT-u koji se događa u klasi, a ovisi o pojasnoj širinom pristupne veze. SP može osigurati obavezu za gubitak i kašnjenje duž jezgre.
- Ugovor također predviđa da će promet Std klase biti označen sa definiranom DSCP vrijednošću, - **Ds**.

Ctrl klasa

- Ctrl klasa osigurava minimalan udio pojasne širine pristupne veze, npr. ~1%, iako obično sa minimumom od ~8 do 16 kb/s. Klasa također ima sposobnost ponovnog korištenja pojasne širine iz drugih klasa koja može biti nezauzeta, sve do pojasne širine dostupne veze.

Diffserv Meta-Jezik

Da bi se olakšao opis Diffserv dizajna koristimo meta-jezik:

- **policy <policy_name>** - Definira početak Diffserv politike, koja se može primjenjivati na određeno sučelje ili logičku vezu
- **class <class_name>** - Definira početak definicije klasifikacijskog kriterija i akcija primijenjenih na promet klase unutar Diffserv politike
- **classify [not] <criteria>** - Definira klasifikacijski kriterij za određenu klasu. Iako je moguć veći broj kompleksnih i jednostavnih kriterija, definiramo samo jednostavni kriterij "DSCP <D>" i "EXP <E>." Tamo gdje se primjenjuju višestruki kriteriji klasifikacije, između klasifikacijskih kriterija se pretpostavlja logička OR operacija.
- **EF** - Označava da će klasa biti dodijeljena redu usluženom sa EF PHB-om.
- **AF (<m>)** - Označava da će klasa biti dodijeljena redu usluženom sa AF PHB-om, sa osiguranim minimalnim omjerom m.
- **mark DSCP (<D>)** - Definira DSCP oznake koje će biti podešene za pakete u određenoj klasi.
- **SR–TCM (<cir>, <cbs>, <ebs>)**
  - green-action <action>
  - yellow-action <action>
  - **red**-action <action>
  - Primjenjuje RFC 2697 oznaku jednobrzinskog trobojnog markera (SR-TCM) na klasu sa određenom obavezom brzine informacije (CIR), obaveznom veličinom praska (CBS), i prekomjernom veličinom praska (EBS). Moguće posljedične akcije su "ispuštanje" ili "odašiljanje" ili „odašiljanje i označavanje DSCP (D)”
- **TR-TCM(<cir>, <cbs>, <pir>, <pbs>)**
  - green-action <action>
  - yellow-action <action>
  - **red**-action <action>
  - Primjenjuje RFC 2698 označavanje pomoću dvobrzinskog trobojnog markera(TR-TCM) na klasu sa određenom brzinom informacije (CIR), određenom veličinom praska (CBS), maksimalnom brzinom informacije (PIR) i maksimalnim praskom (PBS). Moguće rezultirajuće akcije su "ispuštanje" ili "odašiljanje" ili `odašiljanje i označavanje DSCP (D)`.
- **Drop** - Ova akcija će odbaciti pakete koji odgovaraju određenom uvjetu.

- **Transmit** - Ova akcija će prenijeti pakete koji odgovaraju određenom uvjetu, bez mijenjanja DSCP oznaka paketa.
- **transmit-and-mark DSCP (<D>)** - Ova akcija će postaviti DSCP oznake paketa koji odgovaraju određenom uvjetu i prenijeti ih.
- **shape (<r>, <b>)** - Dodjeljuje token oblikovatelj klasi s određenom brzinom r i praskom b.
- **tail-drop-limit (<t>)** - Dodjeljuje tail-drop ograničenje redu klase, odbacujući pakete primljene za tu određenu klasu.
- **RED (CSCP <D>, <minth>, <maxth>, <w>, <pmax>)** - Primjenjuje RED profil za promet sa naznačenim DSCP-om unutar reda klase, s definiranim minimalnim pragom (minth), i maksimalnim pragom (maxth), eksponencijalna konstanta (w) i vjerojatnost gubitka paketa maxth(p_{max}). Multiplicirani RED profili se mogu primijeniti na iste redove da bi se postigao WRED.
- **RED (EXP <D>, <minth>, <maxth>, <w>, <pmax>)** - Primjenjuje RED profil za promet sa naznačenim MPLS EXP unutar reda klase.

Dizajn kod rubnih veza visokih brzina

- Pristupnim vezama s velikom brzinom smatramo one gdje je brzina veze dovoljno velika da se od fragmentacije veze i isprepletenih mehanizama ne traži da ublaže utjecaj serijalizacijskog kašnjenja prilikom pružanja podrške uslugama sa niskim SLA ograničenjima za kašnjenje; to se obično događa pri brzinama veze od oko 1 Mb/s i više.
- Danas su to gotovo sve pristupne veze!

Primjer za VoIP:

- VoIP promet je unaprijed DSCP označen na izvoru (oznaka se kasnije koristi za klasificiranje prometa u Diffserv domeni).
- EF znači ubrzano prosljeđivanje na način da se zatraži najniže kašnjenje od raspoređivača.
- Nadglednik klase, primjerice, može biti jednobrzinski trobojni marker (SR-TCM) definiran u RFC 2697, sa CIR = RVI, CBS = Bv, sa EBS = 0 (npr. suvišni prasak se ne koristi u ovom slučaju) i primjenom 'green' akcije za prijenos i 'red' akcije za odbacivanje.
- SR-TCM dodjeljuje maksimalni Rv i prasak Bv na tijek prometa, a sav višak prometa se odbacuje.

Policy outbound-high-speed-edge-policy

```
class Voip
      classify DSCP (Dv)
      SR-TCM (Rv, Bv, 0)
      green-action transmit
      red-action drop
      EF
class Prm-th
      classify <criteria>
      AF (Rt)
      mark DSCP (Dt)
      RED (DSCP(*), <minth>, <maxth>, <w>, <pmax>)
class Ctrl
      classify DSCP {Dc, 48}
      AF (Rc)
      RED (DSCP(*), <minth>, <maxth>, <w>, <pmax>)
class Std
      classify *
      AF (Rs)
      mark DSCP (Ds)
      RED (DSCP(*), <minth>, <maxth>, <w>, <pmax>)
```

Primjer za Prm-th:

- Kod Prm-th klase pretpostavlja se da se koriste složeni klasifikacijski kriteriji za razvrstavanje paketa u klase. Takvi kriteriji se mogu bazirati na izvornoj ili odredišnoj adresi, na izvornoj ili odredišnoj adresi UDP/TCP portova ili na *deep packet inspection/stateful* (DPO/SI). DSCP svih klasificiranih paketa je postavljen na **Dt**.
- SLA obveza kod Prm-th klase je osigurana korištenjem klase sa AF PHB-om koji osigurava minimalnu širinu pojasa Rt. Pretpostavljajući da se koristi raspored za očuvanje rada(*work-conserving*), Prm-th klasa će imati pristup svim nekorištenim kapacitetima kada se budu usluživale VoIP, Std i Ctrl klase podataka.
- Pretpostavka je da je većina prometa Std klase TCP/IP promet, pa se kao kontrolni mehanizam unutar klasnog reda radije koristi RED nego da se vrši „odbacivanje sa kraja (tail-drop)“, što osigurava veću TCP propusnost povećana pri pojavi zagušenja.

Primjer za Ctrl:

- Promet je razvrstan u Ctrl klasu na osnovu DSCP klasifikacije, pod pretpostavkom da je unaprijed označena na izvoru:
  - ili kao DSCP Dc, od sustava upravljanja mrežom (OA & M)
  - ili kao DSCP 48 od strane protokola usmjeravanja krajnjih sustava.
- Obveze kod Ctrl klase su osigurane kroz korištenje klase s AF PHB, s zajmčenom minimalnom širinom pojasa od 1% brzine veze, premda je minimalno potrebno ~8-16 kb/s da se sa zagušenog pristupnog linka koju stvori korisnik osigura pristup AR-u.
- Brojne aplikacije za kontrolu i upravljanje mreže koriste TCP stoga se RED koristi unutar reda Ctrl klase kako bi se povećala propusnost TCP-a.

Primjer za Std:

- Wildcard klasifikacijski kriterij koji se koristi za Std klasu osigurava da sav promet koji nije klasificiran u VoIP, Prm-th, ili Ctrl klase (koje dolaze prve u Diffserv politici) bude klasificiran u Std klasu. DSCP svih paketa stavljenih u klasu se postavlja na **Ds**.
- SLA obveza je osigurana kroz korištenje klase s AF PHB s minimalnom širinom pojasa Rs-a.
- Pretpostavljajući da je korišten raspoređivač za očuvanje rada, Std klasa će imati pristup svim nekorištenim kapacitetima kada se VoIP, Prm-th i Ctrl podatkovne klase opslužene.
- RED je korišten unutar reda klase da bi se osigurao da je TCP promet unutar klase maksimalan kada dođe do zagušenja.

Rubna SLA usluga ima za cilj ograničiti maksimalno jednosmjerno rubno kašnjenje na 15 do 50 ms za VoIP.

Čak i ako se za implementaciju EF PHB-a za promet osjetljiv na kašnjenje, kao što je VoIP, koristi raspored strogog prioriteta, novopridošli prioritetni paket mora čekati dok se uslužuje bilo koji ne prioritetni paket, prije nego što ga raspoređivač može poslužiti.

Utjecaj rada raspoređivača i FIFO sučelja na kašnjenje prioritetnog paketa je značajniji za sporije pristupne veze.

U praktičnoj primjeni, može doći do dodatnog kašnjenja jer se nekoliko ne-prioritetnih paketa može staviti u red prije prioritetnih.

Stoga, „spore“ veze definiramo kao one u kojima poremećeni učinak ne-EF prometa na EF promet, zbog karakteristika i programa rasporeda i FIFO sučelja, prelazi dozvoljeno kašnjenje za VoIP klasu, ili općenito, klasu sa najstrožim limitima kašnjenja.

DiffServ klase ako pružatelj usluge ne upravlja sa pristupnim usmjerivačem (AC)

Dizajni o kojima je do sada bilo riječ bili su oni iz konteksta usluga “upravljanog pristupnog usmjerivača“, tj. **tamo gdje mrežni davatelj usluga (obično VPN davatelj usluga) posjeduje i upravlja pristupnim usmjerivačkim uređajem**. Naravno, on upravlja i distributivnim i jezgrenim usmjerivačima, te naposljetku osigurava klijentu SLA garancije s-kraja-na-kraj od pristupnog usmjerivača do pristupnog usmjerivača.

Kod usluge neupravljanog pristupnog usmjerivača, mrežni davatelj usluga posjeduje (i upravlja) jezgrene i distributivne usmjerivače, **ali ne posjeduje i ne upravlja pristupnim usmjerivačima**. Usluge neupravljanih pristupnih usmjerivača su atraktivne za krajnje korisnike koji žele zadržati kontrolu pristupnog usmjerivača.

Postoje dvije velike razlike u smislu razvoja upotrebe usluga neupravljanih pristupnih usmjerivača, kada se uspoređuju sa ponudama upravljanih usluga.

- Prvo, budući da mrežni SP ne posjeduje niti upravlja pristupnim usmjerivačem, ne može osigurati da će konfiguracija primijenjena na pristupnom usmjerivaču biti kadra ispuniti SLA obveze od pristupnog ka distribucijskom usmjerivaču.
- Drugo, da bi mrežni SP zaštitio svoju mrežu od krivih konfiguracija pristupnog usmjerivača, morat će provoditi ulaznu „politiku“ na ulaznom sučelju u DR, uključujući kompleksnu klasifikaciju po klijentu i zahtjevne funkcije u smislu osiguranja ograničenja brzine, koja je prije bila dodijeljena pristupnim usmjerivačima.

Dodavanje premium podatkovne klase sa optimiziranim kašnjenjem(Prm-delay)

- Prm-th (*Premium data throughput-optimized class*) više ne podržava SLA za kašnjenje ili gubitak zbog toga što ulazna maksimalna brzina klase nije podržana od nadglednika, te stoga stvarno kašnjenje i gubitak klase ovise o ponuđenom profilu prometa klijenta za tu klasu, što je van kontrole SPa.
- Da bi se ponudila premium podatkovna propusno optimizirana klasa (Prm-delay) sa definiranim SLA-om za gubitak i kašnjenje, maksimalna brzina i prasak za klasu moraju biti primjenjeni s nadglednikom.
- Takva Prm-delay klasa cilja na poslovno-kritičke interaktivne aplikacije sa zahtjevima kašnjenja kao što su SNA,SAP R/3 te Telnet te aplikacije za unos podataka o trgovanju na tržištu.
- Prm-delay SLA se definira u smislu garantiranog limita kašnjenja i gubitka, sa specificiranom pojasnom širinom i dostupnošću. Propusnost se izvodi iz postotka gubitka. Klasa može podržavati obvezu za očuvanje slijeda pojedinog toka.
- Kao i kod VoIP klase, SP i klijent sklapaju ugovor sa definiranim ICR-om i ECR-om, koji su simetrično određeni u ovoj studiji slučaja (tj. ICR=ECR), iako to nije neophodno.
- SP osigurava ugovor ograničavanjem brzine Prm-delay prometa prema/od klijenta koristeći „nadglednika žetona” sa brzinom Rd i praskom Bd; neusklađeni promet koji prolazi nadglednika biti će ispušten od strane SPa.
- Za usklađeni promet, SP će se obvezati na maksimalno jednosmjerno kašnjenje rubnog segmenta, Ld, tipično u rasponu 30-80 ms (za definiranu veličinu paketa) i postotak gubitka s-kraja-na-kraj tipično manji od 0.1 %.

Visokobrzinska rubna mjera

```
class VoIP
classify DSCP (Dv)
SR-TCM (Rv, Bv, 0)
green-action transmit
red-action drop
EF
class Prm-delay
classify <criteria>
SR-TCM (Rd, Bd, 0)
green-action transmit-and-mark DSCP (Dd)
red-action drop
AF (Rd)
class Prm-th
classify <criteria>
AF (Rt)
mark DSCP (Dt)
RED (*, <minth>, <maxth>, <w>, <pmax>)
class Ctrl
classify DSCP {Dc, 48}
AF (Rc)
RED (*, <minth>, <maxth>, <w>, <pmax>)
class Std
classify *
AF (Rs)
mark DSCP (s)
RED (*, <minth>, <maxth>, <w>, <pmax>)
```

- DSCP svih paketa klasificiranih u klasu je podešen na **Dd**.
- Obveza kašnjenja Prm-delay klase se dostiže korištenjem klase sa AF PHB postupkom, koji osigurava minimum osiguranja pojasne širine klase Rd, te ograničenjem prosječne brzine dolaska Rd sa nadglednikom, tako da brzina dolaska ne prijeđe brzinu usluživanja klase.
- Ovo se može postići pomoću SR-TCM-a sa Rd brzinom, Bd veličinom praska, sa EBS=0 i primjenom zelene akcije prijenosa i oznake DSCP i crvene akcije odbacivanja.
- SP specificira SLA ugovor nadglednikovim najgorim dopuštenim praskom Bd, tako da se prasak usluži unutar obveznog kašnjenja klase Ld, tj. Bd/Rd + Ls < Ld, u kojem Ls predstavlja najgori slučaj kašnjenja usluge AF prometa (koji bi bio veći nego kod EF prometa), zbog raspoređivača i FIFO sučelja.

Dodavanje premium podatkovne klase optimiziranog prometa sa limitom gubitka (Prm-loss)

- Premium klasa podataka optimiziranog kašnjenja Prm-delay (*premium data delay-optimized class*) dodala je nadglednika konfiguraciji Prm-th klasi da bi limitirala maksimalnu brzinu i prasak klase, ispuštajući viškove tako da se može podržavati SLA za gubitak i kašnjenje.
- Posljedica načina upotrebe nadglednika sa Prm-delay klasom bio je taj da je klasa bila nesposobna ponovno iskoristiti neiskorištenu pojasnu širinu iz drugih klasa unutar iste politike.

- Stoga, da bi ponudio premium podatkovnu klasu sa optimiziranim kašnjenjem koja ima ograničenje gubitka (Prm-loss), te koja također ima sposobnost ponovne upotrebe neiskorištene pojasne širine iz drugih klasa unutar iste politike, nadglednik se primjenjuje da bi označio određenu količinu prometa kao unutar ugovora, a sve ostalo je van ugovora;
- SLA za gubitak je limitiran samo za promet unutar klase.
- Prm-loss SLA se definira izrazom određenog postotka gubitka, sa specificiranom pojasnom širinom i dostupnošću.
- Takva klasa ima za cilj iste aplikacije kao Prm-th klasa, ali samo kada je prisutna obveza limitiranja gubitka. Praktične razlike između Prm-loss klase i Prm-th klase se dakle najviše odnose na način na koji je SLA ponuđen krajnjem korisniku.
- SP ograničava ugovor limitiranjem brzine Prm-loss prometa prema/od korisniku koristeći označavanje nadglednikom sa brzinom R1 i praskom B1;
- Neusklađeni promet će biti označen kao „van ugovorni" od strane SPa. Brzina R1 će biti odabrana od korisnika, a SP će je nuditi u ovisnosti o mogućnostima pristupne brzine veze.
- Za usklađeni (unutar ugovora) promet, SP će se obvezati na gubitak s-kraja-na-kraj koji će obično iznositi manje od 0.1%

Mjera visoke brzine ruba

```
class VoIP
classify DSCP (Dv)
SR-TCM (Rv, Bv, 0)
green-action transmit
red-action drop
EF
class Prm-loss
classify <criteria>
SR-TCM (R1, B1, 0)
green-action transmit-and-mark DSCP (Dlin)
red-action transmit-and-mark DSCP (Dlout)
AF (R1)
RED (Dlin, <minth>, <maxth>, <w>, <pmax>)
RED (Dlout, <minth>, <maxth>, <w>, <pmax>)
class Ctrl
classify DSCP {Dc, 48}
AF (Rc)
RED (*, <minth>, <maxth>, <w>, <pmax>)
class Scd
classify *
AF (Rs)
mark DSCP (Ds)
RED (*, <minth>, <maxth>, <w>, <pmax>)
```

Dodavanje video klase

Limitiranje jednosmjernih kašnjenja od 100-200 ms obično je usmjereno ka prijenosu video aplikacija. Postoji više dizajna koji bi se mogli koristiti:

- **Prenos videa istom klasom kao i VoIP** - Kao potporu takvim dizajnima, neki prodavatelji imaju implementacije koje dopuštaju diskretnu politiku višestrukih podskupova prometa koji se opslužuju iz istog reda čekanja klase. Problem kod niskih brzina – veliki video paketi koji su sada smješteni u isti red čekanja sa VoIP paketima, mogu povećati kašnjenje VoIP prometa.
- **Prenos videa klasom koja koristi AF red** - Sa ovim pristupom, limit kašnjenja koju video prometu možemo osigurati varira ovisno o korištenom algoritmu raspoređivanja, ali također može ovisiti o broju ostalih AF redova korištenih u određenoj implementaciji i prometu u tim redovima, a na vezama male brzine postoji mogućnost da ne postignemo zahtijevane ciljeve kašnjenja sa ovim pristupom.
- **Multi-level prioritetni program raspoređivača** – Neki uređaji mogu podržavati višestruke prioritetne redove. Kada se istodobno podržavaju usluge glasa i videa, npr., korištenje najvišeg prioritetnog reda za promet glasa, a red sljedećeg prioriteta za promet videa bi omogućilo da promet glasa ima najniže kašnjenje i smetnje, dok bi promet videa imao ograničeno kašnjenje i gubitke, neovisno o načinu rada raspoređivača, konfiguraciji i opterećenju ostalih AF redova.

U praksi, izbor opcije vjerojatno će ovisiti o prirodi ponuđene usluge, te o sposobnostima mrežne opreme koja se koristi.

Rubni SLA sažetak

Klasa		Maksimalna brzina (i praska)	Minimalna širina pojasa	Kašnjenje	Gubitak	DSCP
VoIP		Rv(Bv)	Rv	L_v	Typically ~0.1%	D_v
Prm-th		X	R_t	n/a	n/a	
Std		X	R_s	n/a	n/a	D_s
Ctrl		X	1%	n/a	n/a	D_c, 48
Prm-delay		$R_d(B_d)$	R_d	L_d	Typically ~0.1%	D_d
Prm-loss	In-contract	$R_l(B_l)$	R_l	n/a	Typically ~0.1%	D_{lin}
	Out-of-contract	X	n/a	n/a	n/a	D_{lout}

Koliko je klasa dovoljno?

Ne postoji jedan odgovor na pitanje koliko bi se klasa trebalo podupirati u određenom Diffserv rubnom dizajnu; odgovor ovisi o specifičnim zahtjevima:

- **SLA diferencijacija** - Potreba za diferencijacijom SLA-ova između aplikacija je primarni pokretač za podupiranje dodatnih klasa. Jasno je da nema potrebe za podupiranjem klase ako nema aplikacije koje će koristiti tu klasu. Dodatne klase se mogu postupno dodati ako dođe do potrebe za njima.
- **Odvojene klase za različite aplikacije u realnom vremenu** - može biti moguće usluživati različite aplikacije u realnom vremenu, kao što su glas i video, iz iste klase, tako smanjujući broj potrebnih klasa.
- **Odvojene klase za protokol usmjeravanja i upravljanje prometom** - Neki mrežni dizajni mogu odabrati upotrebu odvojenih klasa za protokol usmjeravanja i upravljanje prometa, iako je u mnogim slučajevima dovoljna jedna rubna klasa.
- **Odvojene klase za nosioca i signaliziranje** - Za aplikacije kao što su glas i video, postoji izbor da li aplikacija signalizacije prometa koristi istu klasu kao i nositelj prometa (medij) ili je potencijalno smještena u vlastitu klasu.

Koju shemu označavanja koristiti?

Kada se donese odluka o broju klasa koje će se podupirati, treba odlučiti o DSCP shemi označavanja koja će se koristiti za identifikaciju različitih klasa i različitih prednosti odbacivanja; jedinstvena kodna točka se treba dodijeliti svakoj prednosti odbacivanja unutar svake klase.

Kada se definira shema označavanja za određen dizajn, postoji nekoliko jednostavnih pravila koja mogu pomoći:

- Koristite samo DSCP 48 za kontrolu mrežnog prometa kao što su protokoli usmjeravanja. DSCP 48 je ekvivalentan vrijednosti 6 IP prioriteta (tj. mrežna kontrola), koja je stvarna oznaka koju koriste prodavatelji mrežne opreme za kontrolu mrežnog prometa.
- Koristite DSCP 46 za VoIP promet, koja je preporučena kodna točka za EF promet te je ekvivalentna vrijednosti 5 IP prioriteta, a to je i stvarna oznaka koju koriste VoIP prodavatelji krajnjih sustava.
- Koristite DSCP 0 za "standardnu klasu", pretpostavljajući da je ovo većina prometa, budući da se ovako izbjegava nepotrebno ponovno označavanje većine prometa.

Moguća shema rubnog označavanja, za različite dizajne klasa po preporuci [RFC 4594]:

Rubna klasa		Rubna DSCP označavanja	
VoIP		D_v	= 46 (EF)
Prm-th		D_p	= 10(AF11)
Std		D_s	= 0
Ctrl:	Routing protocols		= 48 (CS6)
	OA&M	D_c	= 16 (CS2)
Prm-delay		D_d	= 18 (AF21)
Prm-loss:	In-contract	D_{Iout}	= 10(AF11)
	Out-of-contract	D_{Iout}	=12(AF12)

Postavljanje diffserva u jezgri mreže

Da li je diffserv potreban u jezgri glavne mreže?

- Za razliku od ruba mreže gdje su pojasne širine niže, u jezgri gdje su veze pojasnih širina više, a promet je visoko koncentriran, SLA zahtjevi za promet klase mogu se prevesti u zahtjeve pojasne širine, a problem SLA osiguranja se može učinkovito reducirati na problem rezerviranja pojasne širine.
- Bez jezgrenih QoS mehanizama (Diffserv-a), možda bi dizajn mreža bio jednostavniji; međutim, ova prednost dolazi sa troškom združene prekapacitiranosti jezgrene pojasne širine i bez Diffserva ne bi bilo razlike između premium i standardne usluge te bi u nepredviđenom združivanju sav promet dijelio istu sudbinu.
- Uz Diffserv, mi možemo prekapacitirati samo npr. pojasnu širinu za VoIP ili video promet, a ostale klase ostaviti u normalnom obimu – ZNATNE UŠTEDE!

Klasa usluga jezgre i SLA specifikacije

Ukoliko je Diffserv postavljen u jezgri mreže, klase koje su podupirane na rubu trebaju se moći preslikati na klase u jezgri, koje su pak sposobne nositi se sa SLA zahtjevima definiranih klasa.

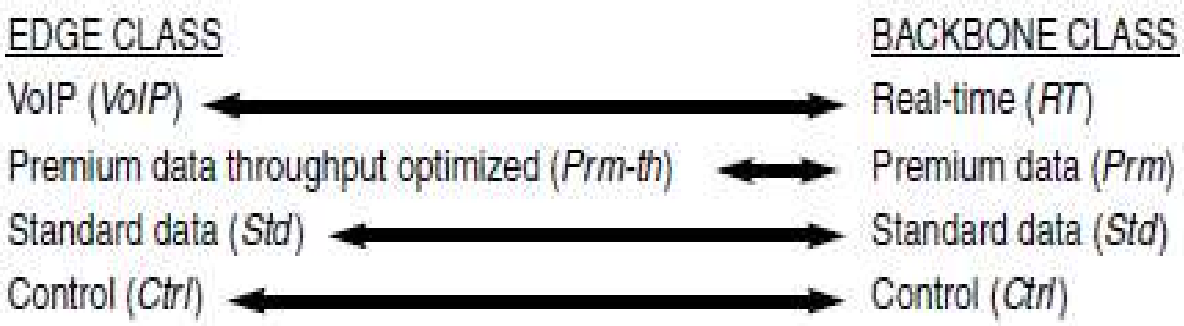
Specifikacije jezgrenih klasa:

Stvarno vrijeme (RT) - Ova klasa cilja na aplikacije kao što su VoIP i video. Osnovni SLA za ovu klasu se definira u smislu niskog kašnjenja, niskih smetnji i niskog gubitka.

Premium podaci (Prm) - Ova klasa cilja na poslovno kritične aplikacije, koje imaju zahtjeve za obvezanim kašnjenjem (iako manje stroge nego kod klasa u realnom vremenu) i niski gubitak.

Kontrolna klasa (Ctrl) - Ctrl klasa je posvećena kontroli mrežnog prometa, osiguravajući da je pojasna širina na vezi jezgre sigurna za osnovne funkcije uključujući protokole usmjeravanja i upravljanja, kao što je telnet ili SNMP.

Standardna klasa (Std) - Std klasa se koristi za sav ostali podatkovni promet, tj. sav promet osim RT, Prm ili Ctrl. SLA obaveze za takvu klasu mogu se obvezati na prosječni RTT kroz jezgru ili prosječni postotak gubitka paketa.



Preslikavanje klasa sa ruba mreže na jezgrene klase

Policy core-policy
klasa RT
klasifikacija DSCP (D_{RT})
klasifikacija EXP (E_{RT})
SR-TCM (R_{RT}, B_{RT}, 0)
zeleno-prijenos.
Crveno-prekid prijenosa
EF
klasa Prm
klasifikacija DSCP (D_p)
klasifikacija EXP (E_p)
AF (Rp)
RED (*, <minth>, <maxth>, <w>, <pmax>)
klasa Ctrl
klasifikacija DSCP (D_c, 48)
klasifikacija EXP (E_c)
AF (Rc)
RED (*, <minth>, <maxth>, <w>, <pmax>)
klasa Std
klasifikacija *
AF (Rs)
RED (*, <minth>, <maxth>, <w>, <pmax>)

RT klasa

- Uzevši u obzir Diffserv konfiguraciju RT klase na prethodnoj slici, može se pretpostaviti da je promet podataka stvarnog vremena označen ili na izvoru ili na rubu mreže na temelju jedne od DSCP oznaka unutar DRT skupa, gdje je DRT = {Dv,...} ili na temelju jedne od EXP oznaka.
- Obvezno SLA kašnjenje po skoku je osigurano korištenjem klase s EF PHB-om, tako da prima najmanje kašnjenje od raspoređivača i osiguravanjem da je brzina dolaska(koju izvršava nadglednik klase RRT-om) niža od brzine usluživanja klase.
- To se može postići korištenjem SR-TCM-a sa brzinom RRT, obveznom veličinom praska BRT, s EBS = 0 i korištenjem zelene naredbe prijenosa i crvene akcije odbacivanja.

Prm klasa

- Možemo pretpostaviti da je Prm promet označen bilo na izvoru ili na rubu mreže prema jednoj od DSCP oznaka unutar DRT skupa, gdje je DRT = {Dv,...} ili jednoj od EXP oznaka unutar Ep skupa.
- SLA za Prm klasu je osiguran korištenjem klase s AF PHB-om.
- RED kontrolni mehanizam zagušenja u koristi se unutar reda Prm klase da bi se postigla maksimalna TCP propusnost.

Ctrl klasa

- Promet se klasificira u Ctrl klasu na osnovu DSCP-a za koji se pretpostavlja da je unaprijed označena na izvoru: – ili na DSCP Da upravljača mrežom krajnjih korisnika ili na DSCP 48 usmjerivačkih protokola krajnjih korisnika ili na jedne od EXP oznaka unutar Ec skupa.
- Ctrl klasa ima osiguran minimalan udio širine pojasa pristupne veze.
- Također, ova klasa ima mogućnost korištenja širine pojasa drugih neaktivnih klasa do širine pojasa dostupne veze.
- RED se koristi unutar Ctrl klase kako bi osigurao maksimalnu TCP propusnost kad dođe do zagušenja.

Std klasa

Standardna klasa se može svrstati na dva načina:

- eksplicitno – bazirano na DSCP-u, pod pretpostavkom da je Std promet označen bilo na izvoru ili na rubu mreže preko jednog od DSCP-ova u skupu Ds ili jednog od EXP oznaka u skupu Es.
- implicitno – pretpostavljajući redoslijed klasa unutar Diffserv sustava određuje redoslijed prve sličnosti(ili prvog podudaranja) kao klasifikacijskog kriterija. Klasifikacijski kriterij slučajnog odabira koji se upotrebljava u Std klasi osigurava da se sav promet koji se ne usmjerava u klasu stvarnog vremena, Prm ili Ctrl, usmjeri u Std klasu.

Varijacije dizajna

Poboljšanja Diffserv dizajna jezgre su potrebna da bi podržavao rubni Diffserv dizajn:

- Prm-delay klasa se može povezati s klasom stvarnog vremena (RT klasom) i s jezgrenom Prm klasom.
- Dodatna AF jezgrena klasa se može dodati kako bi pružila podršku Prm-delay klasi.
- Rubna Prm-loss klasa, s ugovornim i neugovornim opcijama, može se podržavati i biti povezana s jezgrenom Prm klasom, a to zahtijeva primjenu WRED-a u redu čekanja Prm klase.

- Mogućnosti dizajna za podržavanje video klase kroz jezgru su iste kao i one za podržavanje Prm-delay klase opisane poviše. Ipak, zahtjevi vremena kašnjenja mogu biti stroži za video klasu te zahtjevi za izolaciju usluge mogu biti drugačiji

Rubna klasa		Rubna DSCP oznaka		Jezgrena klasa		Jezgrena EXP oznaka		Potrebno eksciplitno spajanje?
VoIP		D_v	= 46 (EF)	Real-time		E_{rt}	= 5	No
Prm-th		Dp	= 10(AF11)	Prm		E_p	= 1	Ne
Std		Ds	= 0	Std		E_s	= 0	Ne
Ctrl:	Protokoli usmjerivača		= 48 (CS6)	Ctrl:	Protokoli usmjerivača		= 6	Ne
	OA&M	D_c	= 16(CS2)		OA&M	E_c	= 7	Da
Prm-delay		D_d	= 18(AF21)	Prm		E_d	= 2	Ne
Prm-loss:	Ugovoreno	D_{lin}	= 10(AF11)	Prm:	Ugovoreno	E_{lin}	= 1	Ne
	Neugovoreno	D_{lout}	= 12(AF12)		Neugovoreno	E_{lout}	= 3	Da

Spajanje rubnih s jezgrenim shemama označavanja

Prilagođavanje (W)RED-a

- Algoritam ranog otkrivanja zagušenosti slučajnim odabirom (RED) je prvotno bio namijenjen poboljšanju propusnosti za aplikacije temeljene na TCP-u, za sprječavanje "globalne sinkroniziranosti" između TCP sjednica.
- Globalna sinkroniziranost je pojava zagušenja i redova čekanja što uzrokuje padove više sjednica, tako da se ukupna propusnost spusti ispod dopuštene brzine. Sve sesije potom povećavaju brzinu slanja dok se zagušenje ponovo ne pojavi i ciklus ponovi stvarajući zajedničku karakterističnu propusnost. RED teži prevenciji takvog ponašanja, tako da se održava veća ukupna propusnost.
- RED stvara odluku o odbacivanju prije stavljanja paketa u red za čekanje na temelju prosječne duljine reda i niza prilagodljivih parametara, koji time određuju osobine RED-a. RED je određen minimalnim pragom čekanja (minth), maksimalnim pragom čekanja (maxth) i vjerojatnošću odbacivanja na maxth (maxp).
- Ponderirani RED (WRED) jednostavno širi koncept i omogućuje korištenje više RED profila u istom redu, gdje se svaki profil može koristiti za jedan aspekt prometa (identificira se posebnim DSCP ili MPLS EXP oznakama). To rezultira posebnim obilježjima odbacivanja, ali i vjerojatnosti odbacivanja po profilu. WRED se koristi za razlikovanje vjerojatnosti odbacivanja između ugovornog i van-ugovornog prometa kao podrška klasama.
- Cilj prilagođavanja RED-a je povećanje iskorištenosti veze i smanjenje srednje duljine reda, čime se smanjuje kašnjenje.
- Mnogi faktori mogu utjecati na RED – broj aktivnih TCP sesija, njihova trajnost, kakav je njihov RTT, koji se blokovi TCP-a koriste i posebnosti svakog RED profila. Ovi faktori variraju od mreže do mreže, od lokacije do lokacije, a vjerojatno i od sata do sata, tako da optimalna RED prilagođenost vjerojatno nije moguća u praksi.

PREDAVANJE 11 - Kontrola dodjele kapaciteta

Spojno orijentirane mrežne tehnologije kao što su multipleksiranje vremenskom raspodjelom (TDM) i asinkroni način prijenosa (ATM) imaju sposobnost implicitnog nadzora koji se koristi u uspostavljanju staze između pošiljatelja i primatelja, kako bi se osiguralo dovoljno resursa za uspostavu veze.

Suprotno tome, sam IP nije spojna tehnologija, te nema implicitnu sposobnost nadzora.

Diffserv je danas daleko najraširenija IP QoS arhitektura u kompanijskim i SP mrežama. Diffserv nam omogućava učinkovito upravljanje kapacitetom mreže, ovisno o tipu prometa ili razredu (klasi).

Diffserv, međutim, ne podržava eksplicitne mehanizme kontrole dodjele kapactiteta.

Kako bi operateri mogli nuditi striktno ugovorene razine usluga za stvarno vremenske aplikacije (npr. glasovna usluga), nužni su mehanizmi **kontrole dodjele kapaciteta (*Capacity Admission Control* – CAC)** kako bi se osiguralo da stvarno opterećenje usluge bude u prihvatljivim granicama.

Bez mehanizama kontrole dodjele kapaciteta, ukoliko dođe do prometnog preopterećenja (zagušenje – povećanje kašnjenja – gubitak paketa - ...) **svi trenutni korisnici** neke stvarnovremenske usluge (npr. glasovne) mogu osjetiti drastičan pad kvalitete usluge.

Definicija:

Kontrola dodjele kapaciteta (CAC) je algoritam odlučivanja, koji se koristi kako bi se utvrdilo da li se novom toku može dodijeliti traženi QoS, bez utjecaja na one tokove kojima je već odobren ulazak, tako da oni i dalje zadržavaju garantiranu kvalitetu usluge.

Postoji nekoliko pristupa kontroli pristupnog kapaciteta, a nijedno od njih danas nije univerzalno razvijeno.

Različite implementacije, okružja, usluge i aplikacije predstavljaju različite zahtjeve i nije prihvatljivo rješenje nametanje istih mehanizama kontrole dodjele kapaciteta za sve situacije.

Problem možemo riješiti jednostavnom metodom prekapacitiranja svih elemenata mreže. Ukoliko raspolažemo s dovoljno velikom širinom pojasa za nadolazeće **vršno** opterećenje, tada nam CAC ne treba.

...međutim...

- Ova solucija je jednostavna, ali može biti i skupa, a ponekad čak i tehnički neizvodiva).
- Nadalje, planiranje kapaciteta nije precizno, promet kroz vrijeme stalno raste pa će se viškovi kapaciteta vremenom istopiti.
- Veliku pozornost treba posvetiti na ograničenost rezervirane širine pojasa tijekom pojava različitih mrežnih kvarova. Ukoliko dođe do ispada iz rada nekih mrežnih elemenata, a ne koristimo CAC, mreža će biti prepuštena sama sebi i ne postoji niti jedan inteligentni mehanizam koji bi uskladio njen rad i zaštitio SLA uvjete.

Idemo sada pogledati nekoliko tipičnih scenarija u kojima se mreža može zateći, a u kojima bi nam CAC bio izuzetno koristan:

Svi mrežni elementi su ispravni, ali u vršnim satima dolazi do zagušenja

U slučaju nedostatka dovoljne širine pojasa pri vršnom opterećenju CAC nam je neophodan kako se ne bi narušio kvalitete usluge.

Imamo prekapacitiranu mrežu ali i kvar jednog mrežnog elementa

Ako imamo dovoljnu osiguranu širinu pojasa za vršno opterećenje, ali samo u normalnom rad bez kvarova, CAC je potreban kako bi u slučaju u slučaju kvara nekog mrežnog elementa mogao odbiti ili preusmjeriti nove zahtjeve za uslugama, tako da oni kojima je već odobren ulazak i dalje zadrže svoju uslugu.

Kvarovi više mrežnih elemenata

Ukoliko se pri planiranju kapaciteta uzimao u obzir samo potencijalni kvar jednog elementa – CAC je potreban. U mrežama može doći i do istovremenih kvarova više elemenata jezgrene mreže što će pak dovesti do znatnijeg smanjenja kapaciteta iako se sama IP povezanost svih korisnika nije izgubila.

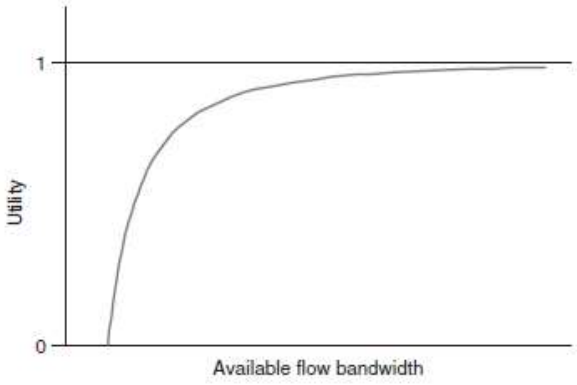
Ukoliko smo pri planiranju mreže osigurali prekapacitiranost čak i kod višestrukih kvarova mrežnih elemenata, tada kontrola pristupa nije potrebna. Međutim, to ne znači da je to poželjan pristup rješavanju problema

Prije uvođenja CAC-a treba izvršiti razmatranje da bi se odredilo da li je učestalost, trajanje i utjecaj događaja (kao što je npr. kvar mrežnih elemenata koji može dovesti do zagušenja rezultirajući sa padom kvalitete usluge) dovoljan razlog da bi opravdao trošak i složenost implementacije mehanizama kontrole dodjele kapaciteta.

Određenim uslugama smanjenje širina pojasa aplikacijskog toka smanjuje i aplikacijsku korisnost. Npr. prilikom pregledavanja web-a ukoliko je raspoloživa širina pojasa smanjena krajnji korisnik može biti nezadovoljan, ali usluga može biti prihvatljiva. Web stranica će se u konačnici učitati (usluga IZVRŠENA), ali trebalo je znatno vrijeme (korisnik NEZADOVOLJAN)

Takve aplikacije obično se nazivaju **ELASTIČNE APLIKACIJE**!

(najčešće bazirane na TCP protokolu).



Slika 1. Kvaliteta usluge elastične aplikacije ovisne o širini pojasa

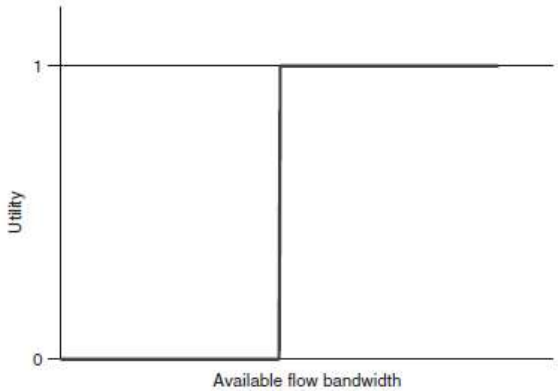
I za elastične aplikacije postoji neki prag širine pojasa, ispod koje je korisnost primjene nula, tj. aplikacija je neupotrebljiva, međutim..

kontrola dodjele kapaciteta uglavnom nije potrebna za elastične aplikacije.

Postoje i druge aplikacije za koje kada dostupna širina pojasa padne ispod prihvatljive razine, korisnost aplikacije padne na nulu.

Takva aplikacija obično se naziva **NEELASTIČNA APLIKACIJA**, a obično uključuje VoIP i video aplikacije.

Na primjer, uzmimo u obzir link koji ima kapacitet za podršku najviše dvadesetak istovremenih VoIP poziva unutar granica SLA, ako se dvadeset prvi poziv uspostavi dolazi do zagušenja i usluge svih poziva biti će degradirane.



Slika 2. Kvaliteta usluge neelastičnih aplikacija ovisne o širini pojasa

Kontrola dodjele kapaciteta uglavnom je potrebna za neelastične aplikacije.

Sustavni pristup kontroli dodjele kapaciteta

Mjerenja krajnjih točaka na CAC bazi

Mjerenjem karakteristike prometa od jedne do druge krajnje točke utvrđuje se da li se novi tok može prihvatiti na te krajnje točke.

CAC signalizacija kroz trasu „spojnog puta" između krajnjih točaka

Signalizacijski CAC protokol na mrežnoj razini uspostavlja zahtjeve i rezervira resurse preko iste staze, koja će biti korištena u prometu za tražene usluge. Ovakav oblik signalizacijske topologije još se naziva i „prospojna". Nakon uspostavljane CAC mrežne signalizacije, **mrežna čvorišta** na trasi preuzimaju odgovornost za donošenje odluka o kontrole kapaciteta.

Takvi „prospojni" pristupi, koji osiguravaju da poruke korištene za QoS signalizacije budu usmjeravane samo kroz čvorove medija, su tzv. **„oprezne topologije"**. Ovakva topologija ima dinamičan pristup, te se lako prilagodi promjenama kapaciteta mreže, zbog kvara na mrežnoj razini (npr. link i čvor).

Postoje samo dva protokola koji su definirani za prospojnu signalizaciju QoS zahtjeva u IP mrežama:

RSVP

i

NSIS

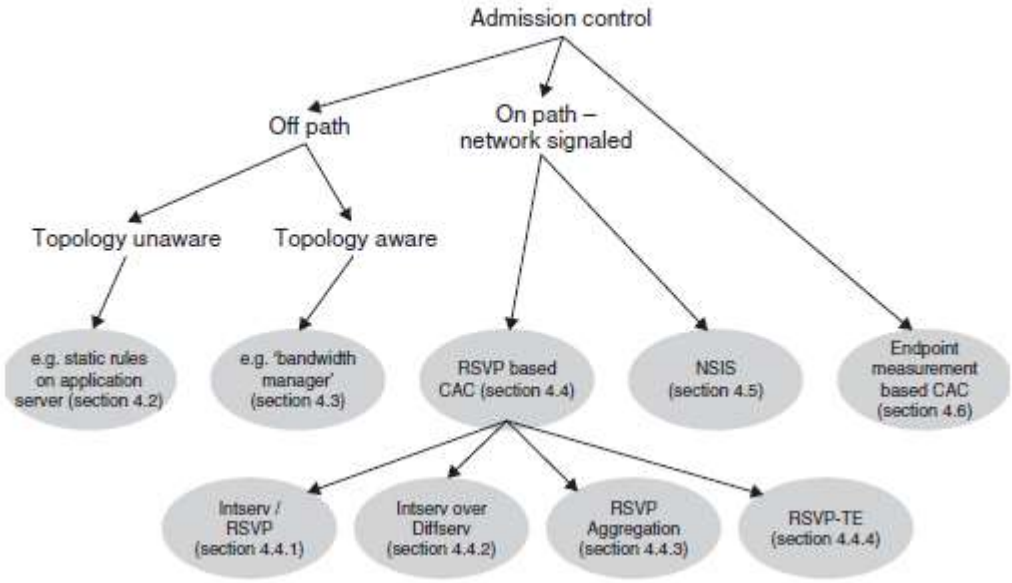
CAC signalizacija „nepovezanog (neprospojnog) puta"

Koriste se QoS signalizacijske poruke koje se prosljeđuju kroz čvorove koji ne moraju biti na stazi podatkovnog prometa. „Ne prospojeni" pristup može uzimati u obzir mrežnu topologiju ali i ne mora.

„Topologijski nesvjesan" CAC obično se sastoji od primjene unaprijed određenih granica raspoloživog kapaciteta između krajnjih točaka aplikacija.

Nesvjesne topologije, nemaju pristup stvarnoj mrežnoj razini, nisu u stanju da se prilagode na dinamičke mrežne promjene, a samim time neučinkovito koriste raspoložive kapacitete

Topologijski svjesni CAC može se dinamički prilagoditi promjenama mrežnog kapaciteta, te samim time ne javlja neefikasnost kontrole širine pojasa kao kod nesvjesne CAC topologije.



Slika 3. Sistematska IP kontrola

Osim do sada spomenutih kriterija koji su korišteni za sistematizaciju, postoji i niz drugih karakteristike, koji se mogu koristiti za razlikovanje različitih pristupa kontrole dodjele kapaciteta:

- 3.sloj - Neki pristupi kontrole pristupa rade samo u IP okruženju, npr. ne mogu se koristiti za donošenje odluka u 2 sloju mrežnih okruženja, na primjer kao što su most ili usmjerivač u ethernet mrežama.
- IP unicast i multicast usmjerivanje- Svi pristupi kontrole kapaciteta podržavaju unicast aplikaciju, ali ne i multicast. U praksi RSVP jedini trenutno ima tu mogućnost.
- Rezervacija može biti jednosmjerna ili dvosmjerna - Neke kontrole dodjele kapactiteta izričito podržavaju koncept dvosmjerne rezervacije, dok ostali pristupi zahtijevaju da su dvosmjerne rezervacije modelirane kao dvije jednosmjerne rezervacije.

Informacije potrebne za kontrolu dodjele kapaciteta

Bez obzira koja se kontrola pristupa koristi, postoji zajednički skup informacija potreban kako bi se odlučilo o vrsti kontrole pristupa:

1. Od kamo do kamo?
2. Potrebna sredstva?
3. Na kojoj razini usluge?
4. Na kojoj prioritetnoj razini?

Parametarski algoritmi

Kontrola dodjele kapaciteta koristi parametarska računanja za donošenje odluka. „Parametarski prometni zapisnici" koriste se za predstavljanje novo traženih resursa i za njihovu usporedbu s trenutno raspoloživim resursima.

Sustav kontrole dodjele vodi računa o zahtjevima koji su prihvaćeni i o preostalim slobodnim raspoloživim resursima.

Kod zaprimanja novog zahtjeva, prometni parametri za taj zahtjev se spajaju s onim iz prethodnog zahtjeva (koji je još uvijek u tijeku), te se uspoređuju sa ukupno raspoloživim resursima u zapisniku kako bi se utvrdilo može li novi zahtjev biti prihvaćen. Ovakva metoda odlučivanja ovisi o točnosti parametarskog zapisnika koji se koristi za predstavljanje prometnih zahtjeva i raspoloživih sredstava.

Najjednostavniji parametarski zapisnik koristi jednu varijablu za opisivanje profila prometa traženog zahtjeva. (npr. min širina pojasa)

- već prije rezervirani kapacitet se definiramo s „r",
- potrebni kapacitet za kojeg tražimo novu rezervaciju „n",
- ukupni dostupan kapacitet je „a"

Nova rezervacija biti će prihvaćena ako je sljedeći uvjet istinit:

$$r+n<=a$$

Mjerni algoritmi

Measurement-based admission control (MBAC) su algoritmi koji se oslanjaju na korištenje mjerenih rezultata kao što su kašnjenje, *jitter*, gubitak, korištenje prometa ili elemenata na putu između dvaju krajeva sustava za odluku hoće li prihvatiti nove zahtjeve za rezervacije.

MBAC pristup koristi mjerenja srednjih čvorova između krajnjih sustava koristeći pasivne mjerenje statistike kao što su ukupno prometno opterećenje veze ili iskorištenost klase, kako bi se procijenilo da li postoji dovoljno kapaciteta za novi zahtjev.

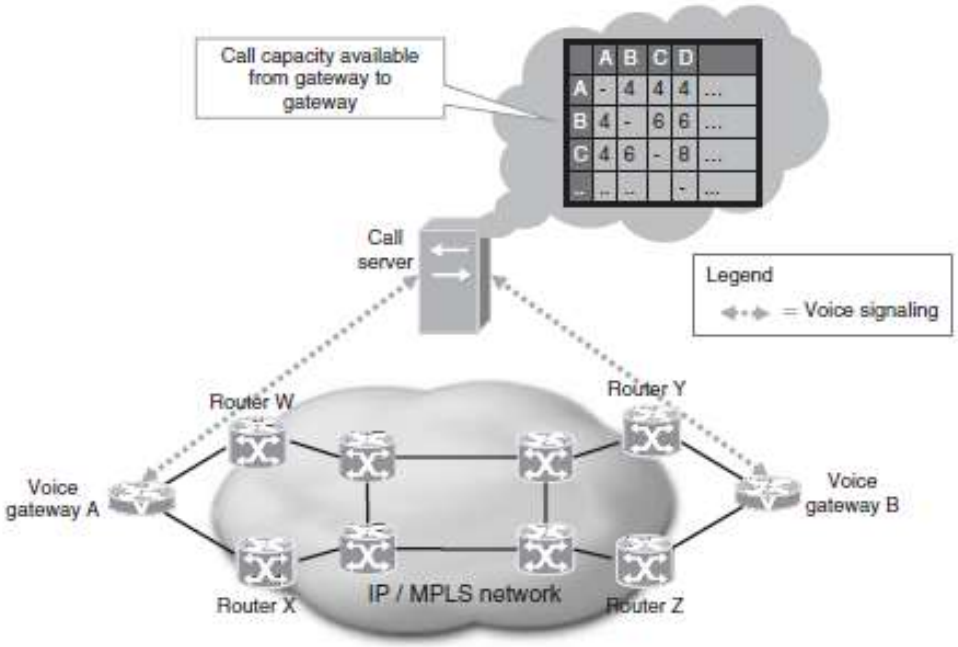
Uz najjednostavniji mjerni pristup, ako je ukupan kapacitet dostupan definiran s „a", te je mjerno opterećenje u proteklom intervalu mjerenja definirano s „m", te traženi kapacitet zahtjevan od nove usluge s „n", novi zahtjev je prihvaćen ako je sljedeći uvjet istinit:

$$m+n<=a$$

CAC ne-prospojnog puta i „nesvjesan" mrežne topologije

CAC „nesvjesne" topologije obično se sastoji od primjene unaprijed definirane granice raspoloživih kapaciteta između krajnjih točaka aplikacija.

Može se provoditi na distribuirani način (npr. na svaki VoIP pristupnik možemo postaviti ograničenje broja poziva s drugim pristupnikom) ili na centralizirani način (npr. centralizirano upravljanje širinom pojasa pomoću aplikacijskog poslužitelja poput video servera ili servera za uspostavu poziva i sl.).



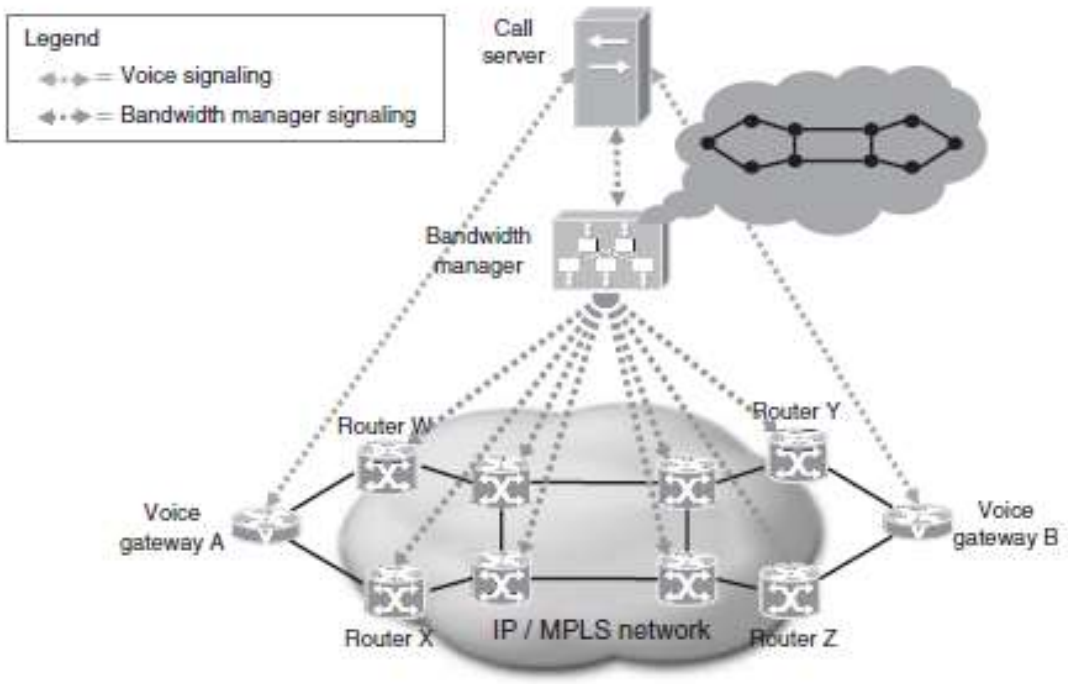
Slika 4. Topologijski nesvjestan CAC – serverski poziv

CAC ne-prospojnog puta i „nesvjesan" mrežne topologije predstavlja jedan od najjednostavnijih oblika kontrole dodjele kapaciteta, ali neizbježno, ima niz ograničenja.

Ovaj pristup može biti učinkovit u jednostavnoj topologiji, međutim, ključno pitanje sa svim nesvjesnim topologijama kontrole pristupa u cjelini je da oni ne uzimaju u obzir raspoloživost sredstava za navedene mrežne puteve koje će utjecati na zahtjev i ne mogu se prilagoditi na promjene mrežnog kapaciteta u stvarnom vremenu, na primjer uzrokovanih kvarom linka ili čvorišta.

CAC svjestan topologije ali „ne-prospojenog" puta

Ova CAC tehnologija poznata kao **„upravitelj širine pojasa"** djeluje kao posrednik između kontrole aplikacijskog prostora te mrežnog kontrolnog prostora.



Slika 5. Upravitelj širine pojasa

Takvi sustavi prate stanje mreže i pružaju mogućnost obrade *oprezne* topologije, te donose rješenja kontrole pristupa po pozivu ili po protoku.

Budući da *oprezna topologija* može dinamički prilagođavati trenutno raspoloživ kapacitet mreže ona bi mogla pružiti rješenje za većinu implementacija okruženja: za pristupnu i jezgrenu mrežu, za L2 i L3, za IP i MPLS.

Kontrola dodjele kapaciteta mjerno orijentiranih krajnjih sustava

IP *endpoint measurement-based admission control* (MBAC), oslanja se na zahtjev krajnjih točaka kako bi one same donijele odluku o kontroli dodjeljenog kapaciteta.

Korištenjem mjerenja dobivenih od ulazne do izlazne točke ispituje se mreža, te utvrđuje mogućnost postavljanja novog toka podataka tom stazom uz zadovoljavajući QoS.

Krajnja točka MBAC može se osloniti na pasivno ili aktivno praćenje prometa.

- **Aktivni nadzor** mreže uključuje slanje sintetičkih testova , odnosno "probnih" paketa preko mreže kako bi se odredile njene karakteristike (kašnjenje, jitter, gubitak informacije ili broj označenih ECN). Krajnja točka MBAC-a s korištenjem aktivnog praćenja oslanja se na mjerne rezultate aktivnih sondi.

- Kada krajnja točka treba postaviti novi tok prometa, prethodno izmjerene karakteristike mreže uspoređuje sa definiranim pragovima kako bi se utvrdilo hoće li novi tok dobiti potrebni QoS i može li on biti prihvaćen.
- Krajnja točka MBAC s korištenjem **pasivnog nadzora** oslanja se na mjerenje obilježja već postojećih medijskih tokova između krajnjih točaka. Ovdje se za mjerenja koristi protokol u stvarnom vremenu (RTP) [RFC 3550]. Na primjer, vremenske oznake i redni broj informacija u RTP zaglavlju mogu se koristiti za određivanje kašnjenja, jittera, i gubitaka primljenih paketa s kraja sustava.

Kao i kod aktivnog pristupa, te mjerene karakteristike mogu se koristiti kao osnova za izradu odluke kontrole dodjele kapaciteta.

Isključivo pasivno praćenje pristupa uzima za pretpostavku da je već ostvarena aktivna veza između dva sustava s kraja na kraj, tj. da se neki trenutni već postojeći mjerni podatak koristi za uspostavljanje novog toka, i da je odluka kontrole pristupa izvršena.

Ako ta pretpostavka nije točna tj. ne postoji neki već uspostavljeni tok od kojeg bi mogli preuzeti mjerenja, ovaj pristup može biti nadograđen s aktivnim praćenja protoka.

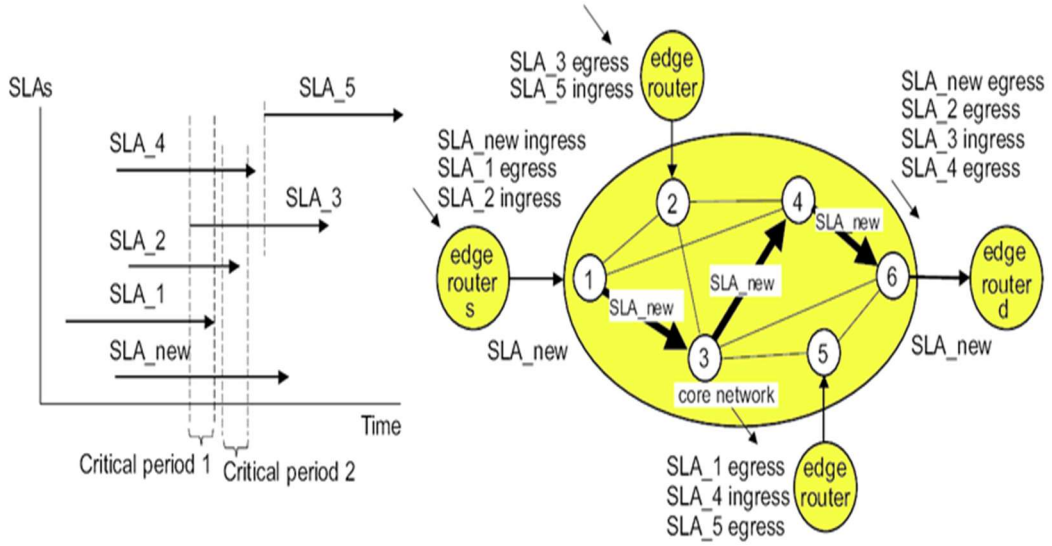
Pristup	Tipovi pristupa	Oprezna topologija ?	Multicast podrška	Jedino L3?
e.g. Video poslužitelj		Ne	Ne	Ne
Upravitelj širine pojasa	Nespojni put	Da	Ne	Ne
RSVP-bazni	Mrežna signalizacija nespojnog puta	Da	Da	Ne
NSIS	Mrežna signalizacija nespojnog puta	Da	Ne	Da
Kraj sustava MBAC	Kraj sustava MBAC	Da	Ne	Ne

Slika 7. Različiti pristupi kontroli dodjele kapaciteta

PREDAVANJE 12 - Planiranje kapaciteta jezgrene mreže

Ovo poglavlje objašnjava planiranje kapaciteta jezgre i kako prometno inženjerstvo može biti korišteno kao sredstvo za učinkovito korištenje mrežnih kapaciteta.

- planiranje kapaciteta jezgrene mreže mrežnih poslužitelja, određuje kvalitetu pružanja SLA zahtjeva
- dobro odabrana širina propusnog pojasa, utječe na smanjeno kašnjenje, varijacije kašnjenja (jitter), gubitka i veću propusnost paketa.
- u DiffServ arhitekturi svaka prometna klasa u mreži, zahtijeva svoju propusnu širinu
- planiranje se najčešće temelji na statističkim podacima, dobivenih mjerenjem jezgrenog kapaciteta veza
- nadogradnjama u sustavu se izbjegavaju moguća zagušenje



Slika 1.1. Planiranje SLA zahtjeva kroz određeni period vremena u jezgrenoj mreži

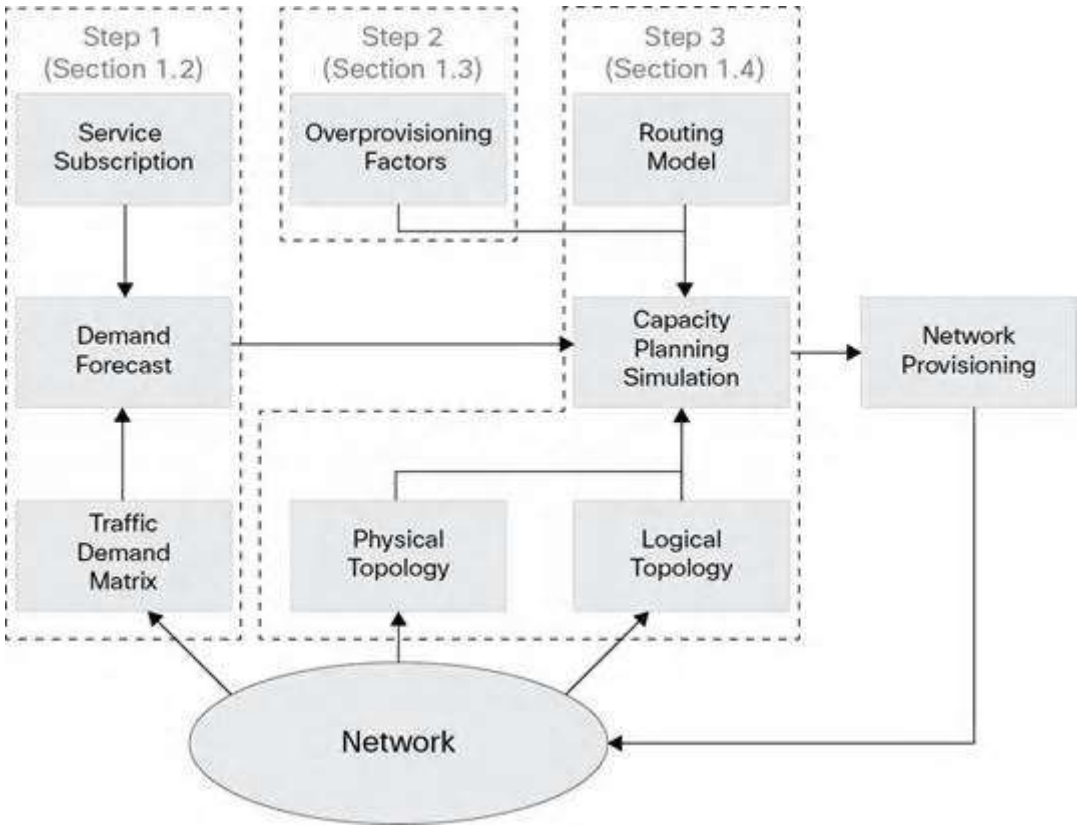
Planiranje se najčešće temelji na statističkim podacima, dobivenih mjerenjem jezgrenog kapaciteta veze.

Kada prosječno opterećenje veze prelazi preko 50%, veza se nadograđuje

Planiranje kapaciteta u jezgrenoj mreži zahtijeva mjerenja trenutačnog opterećenja mreže, koje omogućava ispravnu dodjelu širine propusnog pojasa

U slučaju DiffServ mrežne arhitekture, planiranje kapaciteta se izvodi po klasama prometnog toka.

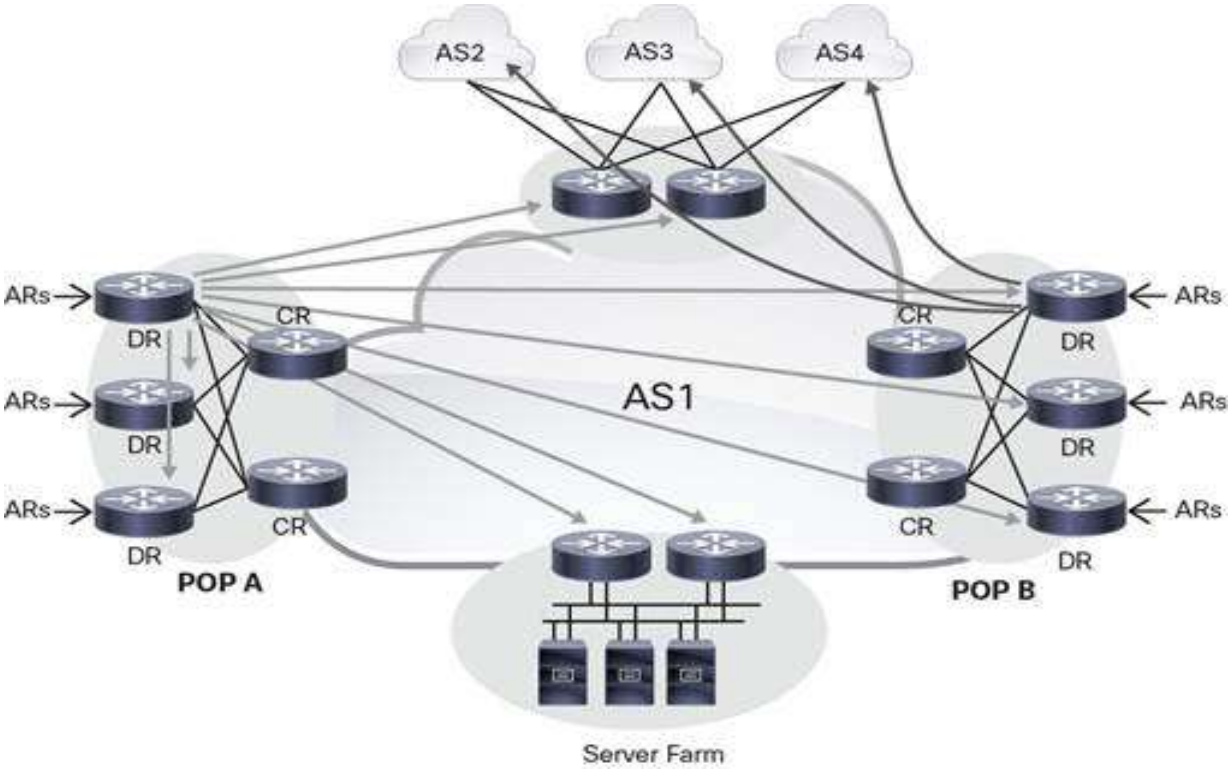
Na slici ispod je prikazana metoda planiranja kapaciteta mreže u tri koraka (mjerenje količine prometa na vezi i procjena budućih, određivanje faktora prekapaciteta (OP), simulacija i analiza)



Mjerenje količine prometa na vezi i procjena budućih

- prvi korak u planiranju kapaciteta jezgrene mreže je mjerenje trenutne i planiranje buduće količine prometa jezgrene mreže
- mjerenje količine prometa može biti prema: IP adresi, usmjerivaču, pristupnoj točki (POP), autonomnom sustavu (AS)
- procjena potražnje za kapacitetom u mreži, provodi se matematičkim metodama prema mjerenjima iz mreže. Kod DiffServ mrežne arhitekture, poželjno je imati CoS (class of service) podatke za mjerenje količine prometa prema klasama
- mjerenja podataka mogu biti unutarnja ili vanjska (unutarnja mjerenja odnose se na količinu prometa od usmjerivača do usmjerivača, a vanjska mjerenja se odnose na promet od usmjerivača do sljedećeg AS-a)
- mjerenja unutarnje količine prometa može biti korisno pri razumijevanje utjecaja nekih elemenata unutarnjoj mreži u slučaju kvara. U slučaju kvara nekog mrežnog elementa, promet se preusmjerava. Kako bi znali put preusmjeravanja prometa potrebno je imati podatke o ukupnom prometu svih usmjerivača

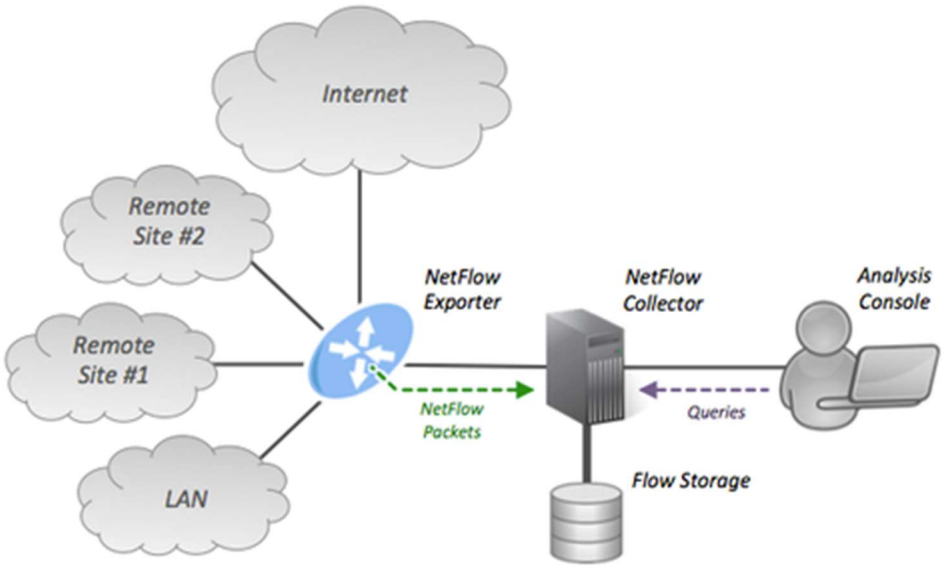
- mjerenja mogu biti od ruba do ruba, npr. od DR do DR (designated router) usmjerivača ili mogu biti od CE do CE (costumer edge) usmjerivača
- mjerenje količine prometa između DR usmjerivača mogu koristiti u slučaju kvarova unutar POP-a, o kojima može ovisit kapacitet jezgrene mreže
- podaci o količini prometa vanjskih veza, mogu biti korisni pri pružanju kapaciteta za povezivanje s drugim AS-a, također i za analizu kvarova unutarnjih veza koji mogu utjecati na vanjsku poveznicu



Slika: Arhitektura mreže za vanjska i unutarnja mjerenja potražnje prometa

- mjerenja se mogu vršiti prema IP, MPLS ili CoS prometu
- standard koji pruža podatke o ukupnoj statistici protoka IP prometa je IPFIX protokol
- mjeri promet na usmjerivačima, sondama i drugim uređajima koji se koriste IP protokolom
- statistički podatci IPFIX protokola o usmjeravanju usmjerivača, predstavljaju podatke o prometu te veze
- u slučaju BGP MPLS VPN usluge, koristi se SNMP (simple network management protocol) za mjerenje ukupnog prometa na LSP stazi ili između krajnjih PE usmjerivača
- SNMP protokol pomaže u razumijevanju MPLS jezgrene mreže
- korištenje SNMP protokola omogućava TE (traffic engineering) svakog kanala

- u praksi je uobičajeno prikupljati statističke podatke svakih 5,10 ili 15 minuta
- izmjereni podatci se koriste za određivanje količine prometa tijekom određenog intervala (tjednog, mjesečnog ili godišnjeg)
- ukupni podatci se zbrajaju i analizira se njegovo najveće opterećenje
- prema tim podatcima se donose odluke o mogućoj nadogradnji sustava.

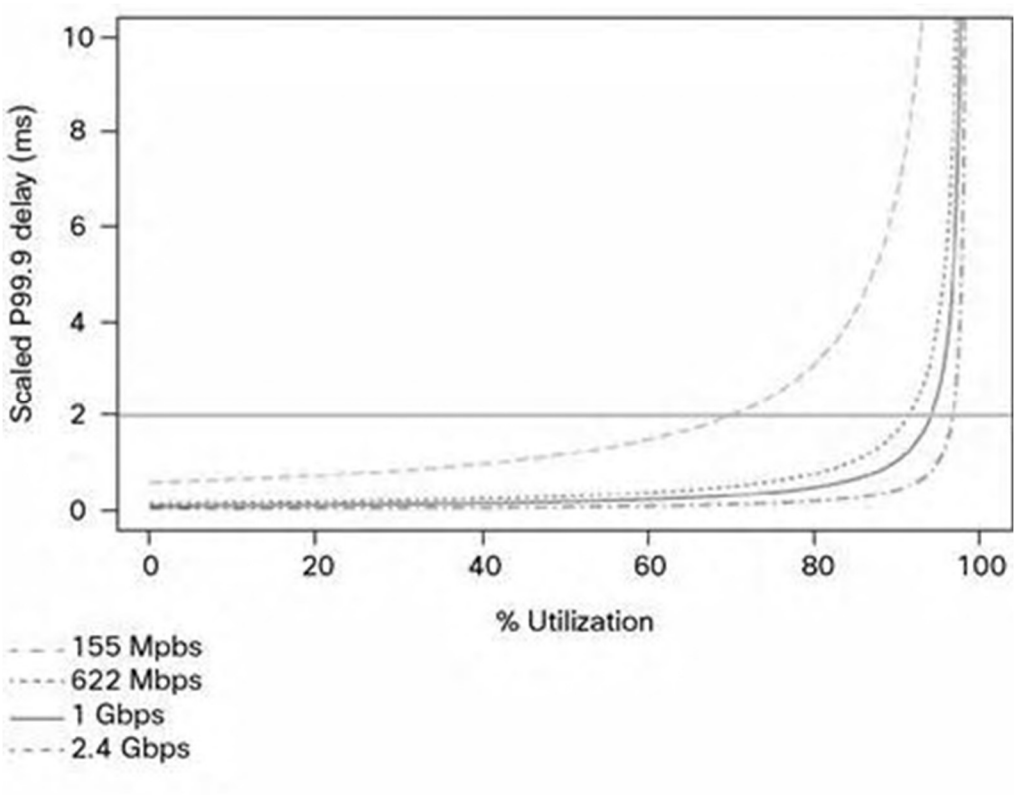


Slika: Arhitektura Netflow-a

Određivanje faktora prekapaciteta (OP)

- drugi korak u planiranju kapaciteta jezgrene mreže je određivanje faktora prekapaciteta
- kako bi se dodijelio odgovarajući propusni pojas svakoj prometnoj klasi različitih zahtjeva, potrebna su mjerenja prosječne brzine prometnog praska
- u slučaju prevelike količine prometa u određenom vremenu, može se pojaviti privremeni zastoj što uzrokuje kašnjenje i gubitke
- kako bi se osiguralo da preveliki praskovi ne utječu na SLA zahtjeve, potrebno je da se širina pojasa dodatno nadgleda u odnosu na mjerenu prosječnu količinu prometa
- prekapacitet se odnosi na vrijednost širine propusnog pojasa koja izaziva kašnjenje, jitter i gubitak paketa
- faktor prekapaciteta (OP) utječe na raspodjelu prometa na vezi i njenu brzinu
- postoje dva različita promatranja na prasak prometa u nekom periodu

- prvo razmatranje je da promet je jedinstven, što znači da je praskovit u jednom ili na cijelom periodu (nema varijacije prosječne brzine prijenosa)
- drugo razmatranje je da ulazni IP promet slijedi Poissonovu krivulju (kašnjenje se smanjuje s povećanjem propusnosti kanala), što je duže promatran distribuirani promet, to je manja varijacija prosječne brzine prijenosa i obrnuto
- na primjer, za DiffServ mrežu, ako želimo postići kašnjenje od 2 ms na vezi od 155 Mbps, tada prosječna pet minutna iskorištenost kanala ne smije biti veća od 70% ili 109 Mbps (potrebno je OP; 1/0.7 = 1.42)
- kako bi ostvarili vezu od 1 Gbps, prosječna iskorištenost ne smije biti veća od 96% ili 960 Mbps (OP = 1.04)

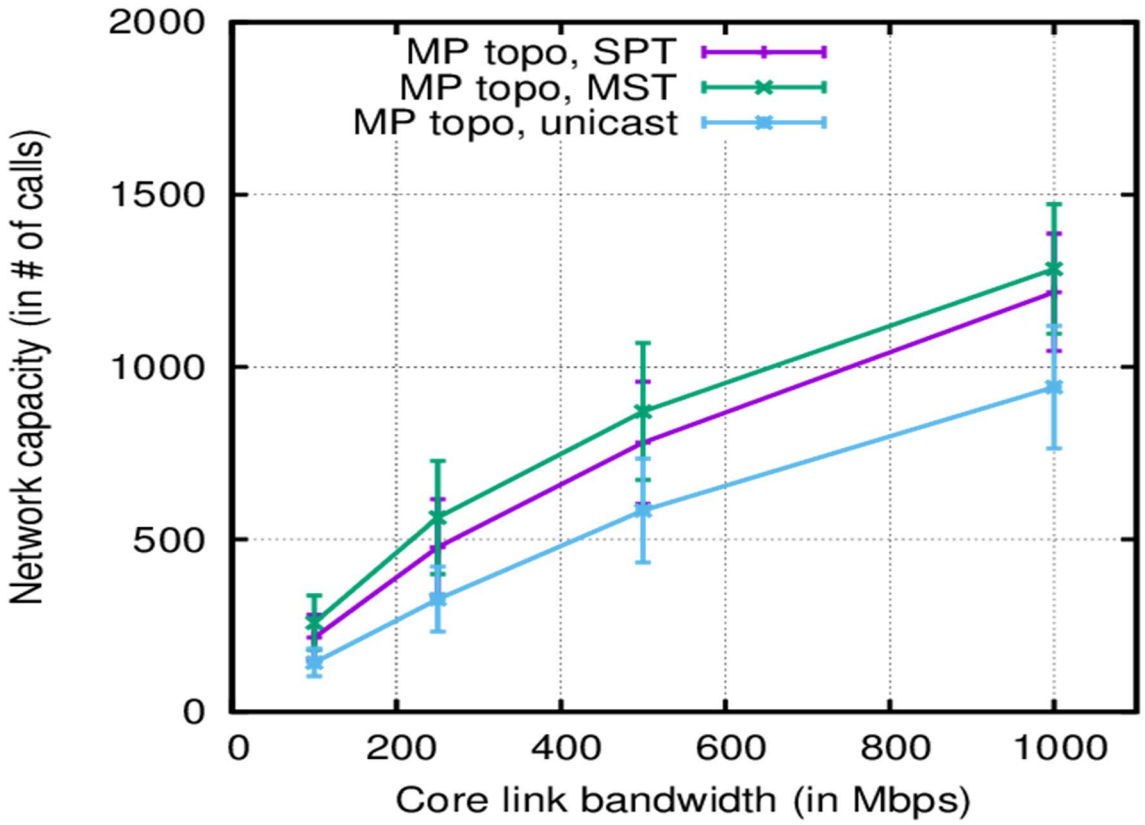


Slika: odnos prosječne iskorištenosti kanala i vjerojatnosti kašnjenja u redu čekanja. Rezultati pokazuju da su za istu razinu iskorištenosti kanala, manja kašnjenja na vezama od 1 Gbps nego za veze od 622 Mbps.

Simulacija i analiza

- treći korak u planiranju kapaciteta u jezgrenoj mreži je pokretanje simulacije koja uspoređuje dobivene podatke sa trenutnom situacijom u mreži
- slijedi analiza rezultata kako bi se odredila širina propusnog pojasa mreže uzimajući u obzir faktor prekapaciteta
- temeljem tih podatak moguće je odrediti plan pružanja SLA zahjeva

- simulacije kvara u mrži moguće je modelirati SRLG (shared risk link group) simulatorom
- može se primijeniti na zasebne veze, grupirane veze i čvorove, zajedničkih potencijalnih problema
- pomoću SRLG može se simulirati slučajni kvar POP-a
- simuliraju se i buduća opterećenja na vezi kako bi se moglo planirati održavanje SLA zahtjeva



Slika: Kapacitet prometa za tri različite jezgrene mreže

PREDAVANJE 13 – Kvaliteta usluga i VPN tehnologije

Što je VPN (*Virtual Private Network*)?

Virtualna privatna mreža (VPN) je privatna računalna mreža ostvarena uporabom infrastrukture javne telekomunikacijske mreže (primjerice Interneta).

One nam omogućuju:

- komunikaciju između korporacijskih lokalnih mreža (intranet VPN),
- povezivanje udaljenih ili mobilnih djelatnika s korporacijskom mrežom (VPN s udaljenim pristupom) i
- komuniciranje između korporacije i njenih strateških partnera, korisnika i dobavljača (ekstranet VPN).

VPN može postojati između:

- pojedinog računala i privatne mreže (client-to-server) ili
- mreže računala na udaljenoj lokaciji koja je povezana s centralnim uredom (server-to-server).

Tradicionalne VPN arhitekture

1. **Mrežno baziran VPN** (npr. L3 VPN baziran na PE rubnim usmjerivačima MPLS mreže pružatelja usluga) — VPN-ovi su kreirani i upravljani od strane javnog pružatelja mrežnih usluga
2. **CPE (*Customer Premises Equipment*) bazirani VPN** (L3 VPN baziran na korisničkim CE usmjerivačima) — VPN-ovi su kreirani od strane korisnika, a bez sudjelovanja javnog pružatelja usluga koji u ovom slučaju samo pruža prisup Internetu. U infrastrukturi javnog pružatelja usluga nije uključena niti jedna VPN funkcija. Usmjerivači javnog davatelja usluga tretiraju VPN IP pakete na isti način kao i IP pakete za pristup internetu; svi pristupni VPN podaci ostaju unutar korisnikove (kompanijske) mreže, te nisu vidljivi u mreži javnog pružatelja mrežnih usluga (npr: IPSec-based VPN).
3. **Aplikacijski VPN (*Application based*)** — VPN ili aplikacijsko-specifični tunel kreiran je između dva IP uređaja. Taj aplikacijski tunel transparentno prolazi i kroz korisnikovu opremu i kroz opremu javnog pružatelja mrežnih usluga (npr: SSL).

Sve više današnjih međunarodnih kompanija koje teže uštedama, na globalnoj razini u svojim mrežama implementiraju kombinaciju ova tri tradicionalna načina izrade VPN-a, i time dobivamo arhitekturu mreže znanu kao **hibridni VPN (Hybrid VPN).**

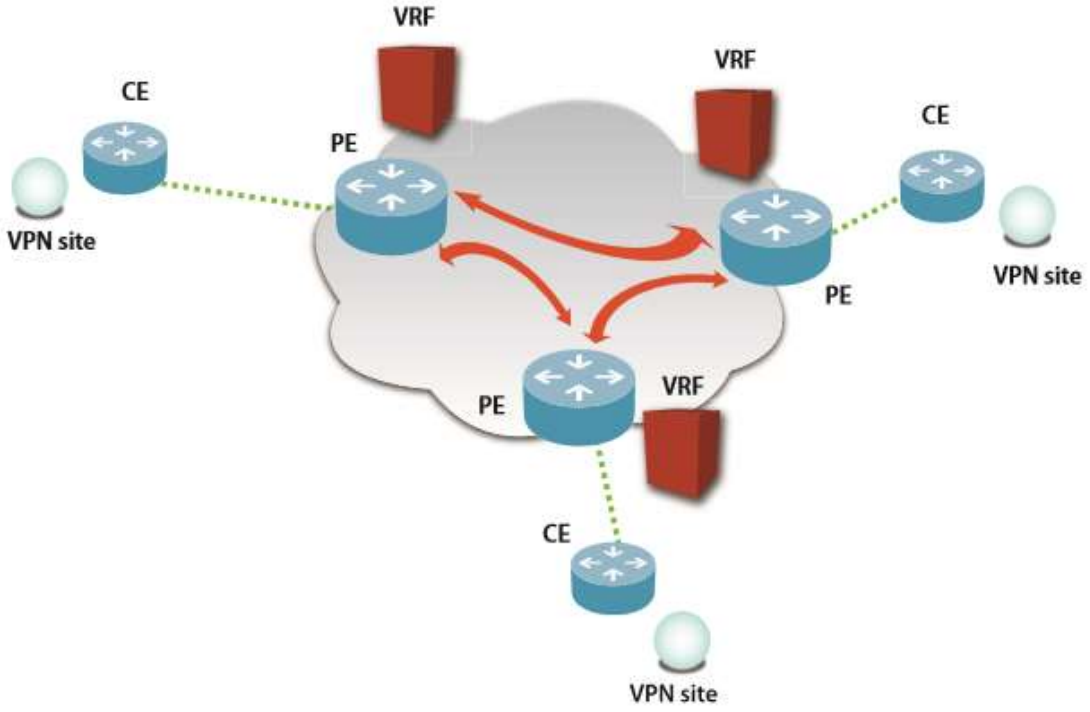
Najvažnija prednost hibridnih arhitektura:

- Mogućnost brzog i fleksibilnog reagiranja na konstantne promjene mrežnih zahtjeva od strane korisnika
- Smanjuju troškove uspostave i održavanja VPN mreža

Hibridni VPN također olakšava ispunjenje nekih zahtjeva poput lokalnog pristupa internetu, povezivanjem vlastite mreže sa drugim kompanijama (npr.dobavljačima ili drugim poslovnim partnerima), te spajanje mobilnih korisnika (radnika koji rade van ureda).

MPLS VPN

- U MPLS mrežama, ulaznim paketima dodjeljuje se labela (kratki identifikator fiksne duljine) koja određuje odredište paketa, a labelu postavlja Provider Edge (PE) usmjerivač.
- Labela na paketu mjenja se u svakom čvoru kroz koji prolazi kako bi se osiguralo da paket sigurno stigne na odredište



- Uloga *Customer Edge* (CE) usmjerivača je usmjeravanje IP prometa iz korisnikove mreže do MPLS opreme tj. do njegovog PE usmjerivača.
- Svaki CE usmjerivač uspostavlja svoju internu tablicu usmjeravanja na temelju znanja o IP mrežama na koje je spojen.
- MPLS VPN-specifične tablice usmjeravanja (VRFs) i CE tablice usmjeravanja izmjenjuju se kroz CE/PE link.

Prednosti

- Vodeća tehnologija za WAN mreže (*Wide Area Networks*).
- Integrira prednosti Internet protokola (adresiranje, dinamičko usmjeravanje, meshed network) dok istovremeno **rješava** neke od njegovih problema poput prijenosa privatnih adresa kroz mrežu, usmjeravanje po trasama koje definira korisnik ili pak razvrstavanje prometa po vrsti i dajući tim različitim vrstama različite prioritete tj. različit QoS.
- Garantira QoS – definiran SLA ugovorom

Mane i ograničenja

End-to-end usluga koju pružaju MPLS pružatelji mrežnih **usluga skuplja** je od *CPE-based* VPN-ova jer:

- zahtjeva *high-quality* uređaje za osiguranje razine usluge korisniku.
- Sve izlazne točke iz korisnikove mreže moraju biti spojene na opremu pružatelja mrežnih usluga visoko kvalitenom vezom (zakupljenim vodom visoke kvalitete) što znatno ograničava isplativost takve izvedbe u dislociranim, ruralnim ili teško dostupnim geografskim područjima.

QoS u MPLS VPN-u

- **MPLS tehnologija pruža mogućnost garantiranja QoS-a korisnicima!**
- Posao klasifikacije prometa vrši se na rubovima MPLS mreže, pa se poslovi tipa klasifikacije prometa po tipu, primjena politika, izbjegavanje zagušenja i upravljanje zagušenjima vrši na ingress sučelju PE usmjerivača tj.egress sučelju CE usmjerivača.
- **Veza na MPLS cloud je najslabija točka u site-to-site vezi**.
- MPLS pružatelj mrežnih usluga kontrolira zagušenje na PE egress sučelju (izlazna veza prema korisnikovoj mreži) podešavajući brzinu (širinu pojasa) podataka u skladu sa ulaznim krugom u korisnikovoj mreži (CE) na pojedinoj ulaznoj lokaciji.
- CE usmjerivači su niže kvalitete od PE usmjerivača, pa iako im operater isporučuje podatke dovoljnom brzinom, oni mogu kočiti brzinu podataka koja im se isporučuje. To kašnjenje može stvarati probleme u radu nekih aplikacija.
- Moguće su razlike izmjerenih brzina podataka od strane korisnika i ugovorenih brzina po klasama prometa koje se operater obvezao osigurati SLA ugovorom.

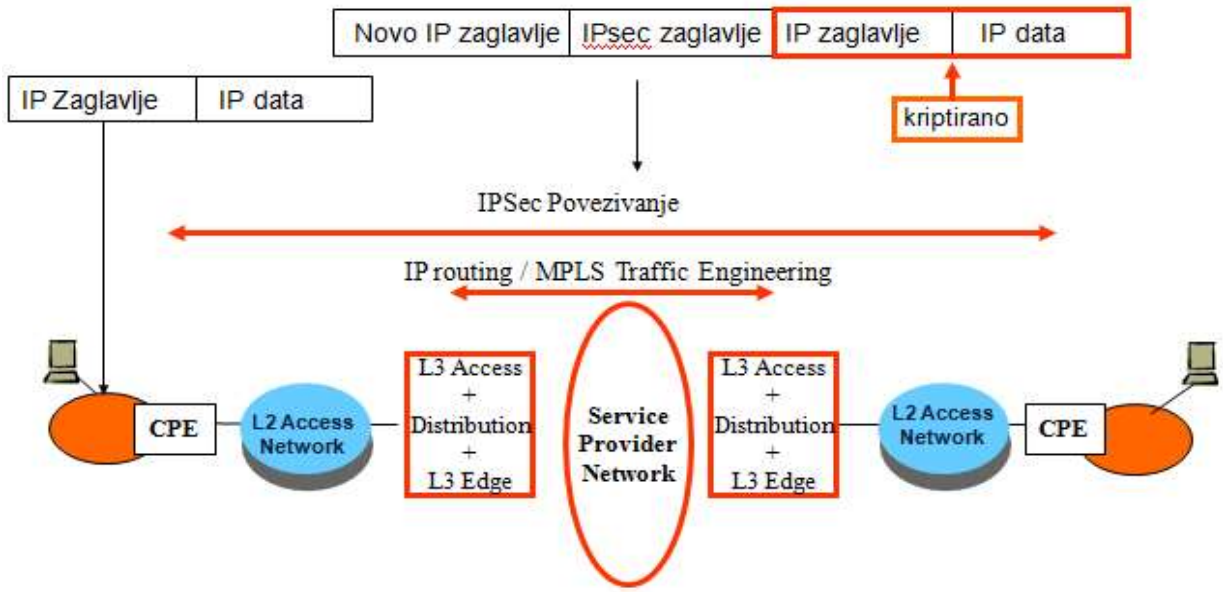
IPSec VPN

- IPSec VPN-ovi koriste **Internet protokol (IP)** za prijenos korisničkih podataka kroz transportne mreže različitih operatera u svijetu.
- Povjerljivost, integritet i autentičnost podataka osigurava se autentifikacijskim i enkripcijskim protokolima.
- U tunelskom modu, čitav IP paket je kriptiran i autentificiran te enkapsuliran u novi IP paket na novim IP zaglavljem.

Tunelski mod se koristi za kreiranje VPN-ova za:

- ✓ *network-to-network* komunikaciju (npr. Između usmjerivača koji povezuju različite mrežne lokacije),
- ✓ *host-to-network* komunikacije (npr. remote user access) i
- ✓ *host-to-host* komunikacije (npr. private chat).

IPSec može se koristiti za uspostavu VPN-ova preko Interneta ili za dodavanjem još jednog sloja zaštite na MPLS VPN. Kada se koristi preko Interneta , IPSec omogućuje point-to-point veze.



Prednosti

- Zbog toga što IPSec kreira VPN vezu kroz Internet, on se svuda može primjeniti i **predstavlja jeftinu opciju** za uspostavu VPN veze.
- IPSec omogućava extra razinu zaštite kroz enkripciju i autentifikaciju podataka i omogućava korisniku da zadrži svoj vlastiti adresni plan kroz IPSec tuneliranje među lokacijama.
- IPSec je idealan za spajanje ureda na izoliranim lokacijama kao i za uspostavu privremenih VPN-ova (sajmovi, privremeni backup, itd.).

Mane i ograničenja

- Iako je IPSec VPN implementiran kroz Internet koji je meshed mreža, on nasljeđuje kompleksnost layer 2 VPN-ova poput Frame Relay ili ATM. Do toga dolazi uslijed point-to-point IPSec tunela. Kada dodajemo neki novi tunel, korisnička oprema u uredu morati će biti rekonfigurirana kako bi se prilagodila novoj logičkoj mrežnoj topologiji.
- Karakteristike paketa mogu biti skrivene unutar IPSec tunela što onemogućava prepoznavanje klase paketa, a samim time i QoS mehanizme za prioritizaciju prometa, tj. takve mogućnosti postoje samo na rubovima mreže.
- Često je neophodna i posebna oprema kako bi neki čvor (hub) mogao dovoljno brzo odrađivati poslove enkripcije/dekripcije, a za izolirane radne stanice IPSec traži instalaciju client programa.

IPSec je layer 3 VPN tehnologija (to znači da radi neovisno o aplikaciji koja je koristiti) i obično je implementirana između rubnih mrežnih usmjerivača.

Topologije

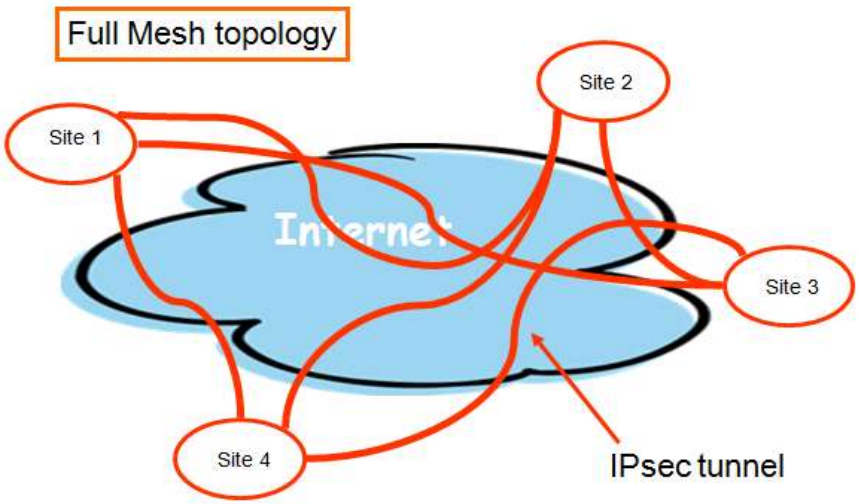
Odabir najbolje mrežne topologije osnovni je problem IPSec VPN-a.

Postoje dva osnovna tipa VPN topologije:

- ***Meshed*** (svaka lokacija je spojena putem IPSec tunela sa svakom drugom lokacijom)
- ***Hierarchical*** (svaka lokacija "spoke" spojena je IPSec tunelom na jednu specifičnu lokaciju koju nazivamo "*hub*")

Većina današnjih poslovnih IPSec VPN mreža koristi „*hub-and-spoke*" topologiju.

Potpuno *mesh* mreže (svaka lokacija direktno spojena sa svim ostalim lokacijama)



Na prvi pogled to izgleda kao idealna solucija u pogledu jednostavnosti i efikasnosti.

Međutim, broj potrebnih tunela vrtoglavo raste povećanjem broja lokacija. Ako je N broj lokacija, broj potrebnih tunela je **(NxN-1)/2**.

Primjer: za 30 lokacija mreža traži 435 veza i 29 logičkih veza mora biti konfigurirano u svakom korisničkom usmjerivaču.

Mane i ograničenja *full mesh* topologije

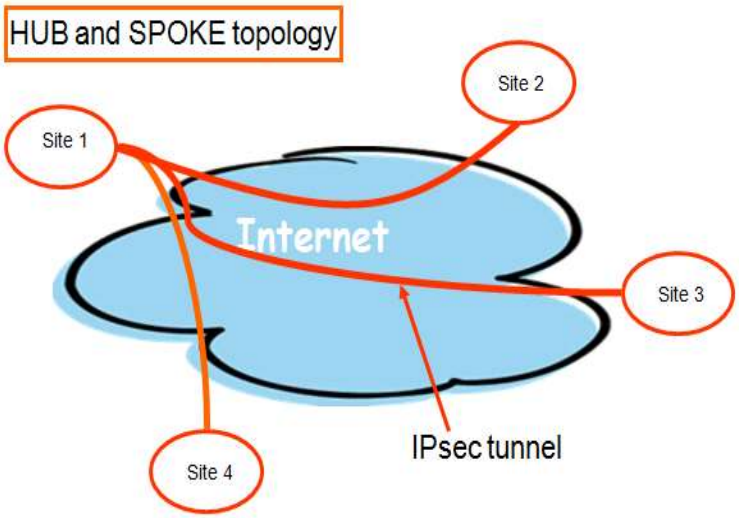
Teškoće u kompleksnosti konfiguriranja postaju limitirajući faktor za takve mreže. Kod **multicast** prometa, *full mesh* će prouzročiti znatno veći promet na izlaznom sučelju iz lokacije koja šalje mulicast jer se **podaci dupliciraju** za svaki IPSec tunel.

Na ovaj način sve veze, prema svim lokacijama, moraju imati vrlo velike kapacitete (ukoliko želimo da sve imaju mogućnost multicasta) .

U hub-and-spoke, jake veze mora imati samo hub lokacija.

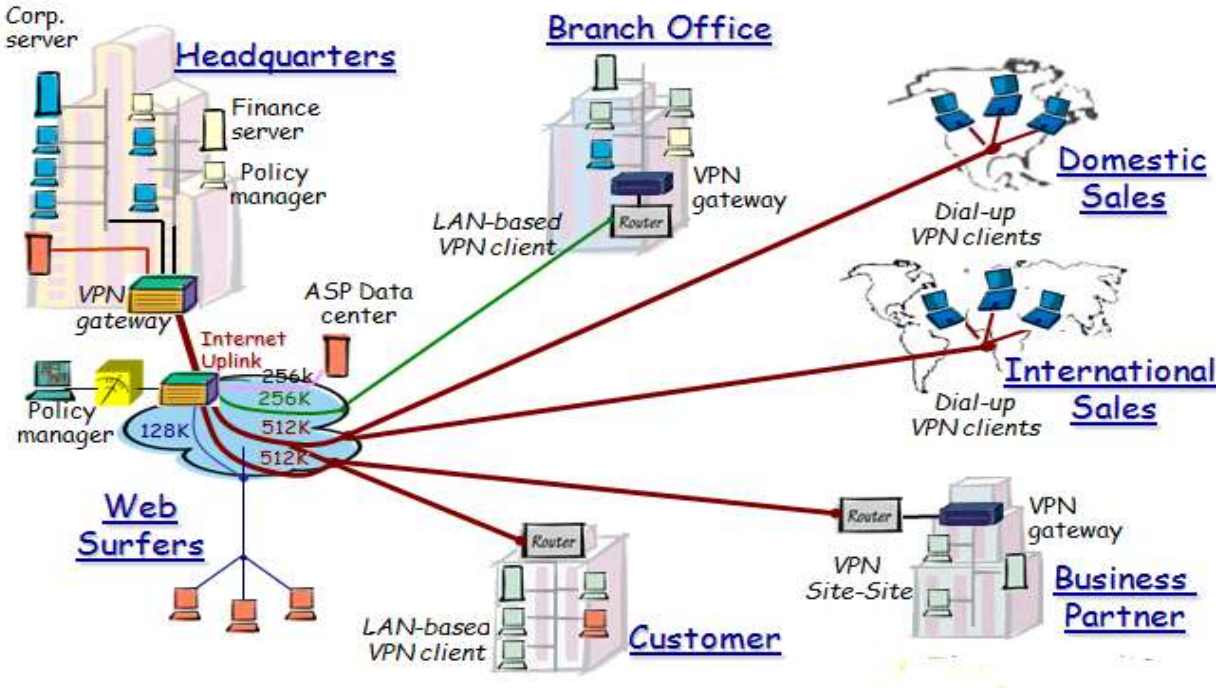
Iz prakse znamo da se ovakve mreže koriste do maksimalno 4 ili 5 lokacija.

Hijerarhijska ili "*hub-and-spoke*" arhitektura



U hijerarhijskoj topologiji, spoke lokacije su spojene sa centralnim hub-om.

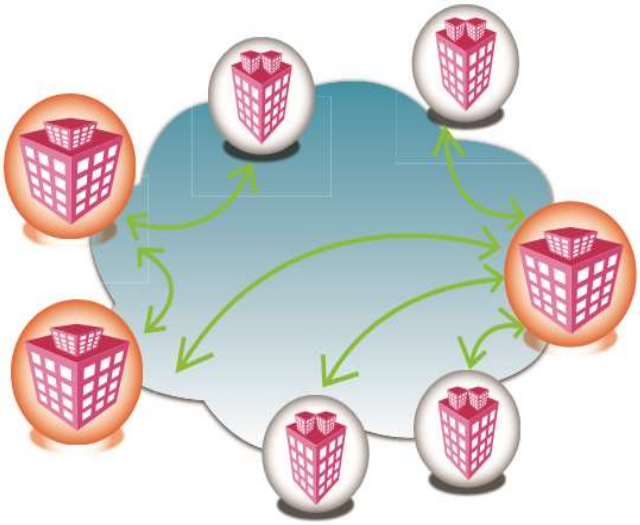
Dok je ovakav način jednostavniji sa strane izvedbe, **kašnjenje** koje se generira u spoke-to-spoke komunikaciji može biti toliko da komunikacija postaje nepouzdana za neke aplikacije.



Primjer organizacije korporativnih VPN veza „hub&spoke" IPSec topologijom

Djelomično "*meshed*" arhitektura

IPSec VPN može biti napravljen u kombinaciji topologija. To može biti uvjetovano potrebama svake pojedine lokacije, ali i postojanja stvarnih fizičkih mogućnosti spajanja.



Neka software rješenja za usmjerivačku opremu nude mogućnost kreiranja dinamičkih IPSec tunela što znatno smanjuje količinu posla za konfiguraciju usmjerivača.

„Dinamički tunel" je posebna implementacija manuelnog tunela koji ima presetirane opcije kako bi se pojednostavnio proces.

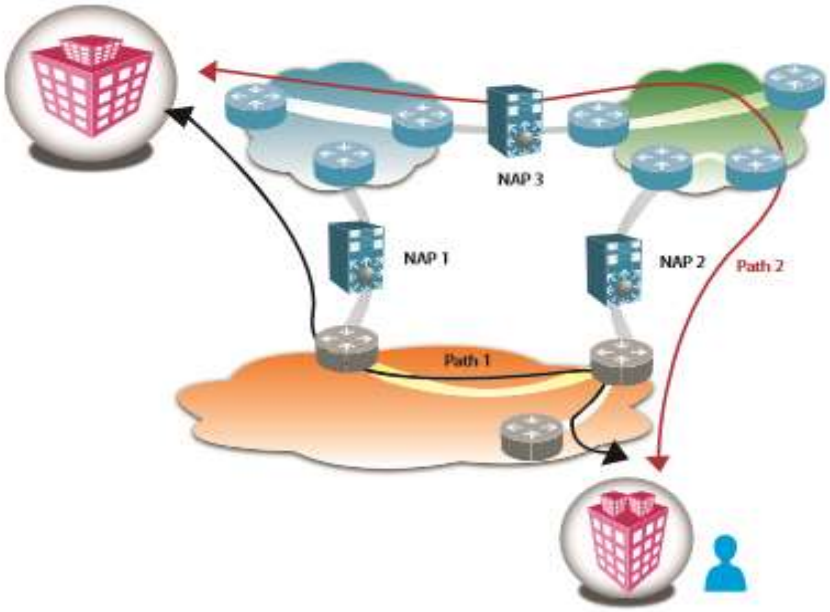
Ova tehnologija može podržati jednoslojnu hub-and-spoke konfiguraciju ali također nudi i mogućnost da dinamički napravi privremene direktne spoke-to-spoke veze.

Dinamičko usmjeravanje nudi znatne prednosti prilikom detekcije ispadanja veza ili opreme iz rada, uz uporabu redundantnih resursa. Također se izbjegava kompleksnost održavanja velikog broja statičkih usmjerivačkih ruta.

Obzirom da IPSec ne podržava IP usmjeravanje, IPSec se prenosi pomoću enkapsulacijskog protokola koji podržava dinamičko usmjeravanje. Npr.standardni IP *Generic Routing Encapsulation* (GRE) tunel.

Quality of Service

Obzirom da će javni pružatelj usluga jednako prioritizirati sve pakete u IPSec tunelu, **klasični QoS nije moguć!**. Postoje i dodatni razlozi za zabrinutost o kojima treba voditi računa, a koji mogu imati utjecaj na kvalitetu usluge IPSec VPN-a.



Pravila usmjeravanja i selekcija izlaza (*peering*) kod svakog operatera javnih usluga striktno slijede Internet pravila — paketi se usmjeravaju prema odredišnoj mreži pomoću najbliže *Network Access Point*, ali međusobni odnosi između različitih mrežnih operatera vrlo rijetko su poznati korisnicima.

Kada se IPSec VPN proteže preko više ISP-ova, najmanje što bi oni trebali napraviti je da imaju predimenzioniranu mrežu u svome jezgrenom (*core*) transportnom dijelu, tj. više nego dovoljnu raspoloživu širinu pojasa.

Ovo ima ogromno značenje iz 2 razloga:

1. U slučaju zagušenja, UDP paketi visokog prioriteta, poput paketa koji prenose govor, mogu jednostavno biti odbačeni jer transportna mreža ne može pružiti klasični QoS jer su paketi kriptirani pa mreža nezna njihov CoS.
2. Greške u sekvencama mogu od strane IPSec procesiranja biti shvaćene kao "*session replay*" pokušaj hakerskog napada (*anti-replay functionality*), pa bi svi primljeni paketi mogli biti pobrisani.

SSL (*Secure Sockets Layer*) VPN

Iako SSL nije mrežna tehnologija, ipak je prihvaćena od brojnih proizvođača kao opcija kojom se pruža **VPN usluga za izdvojene lokacije putem aplikacijskog tunela između korisnika i aplikacijskog servera** (*layer 7* VPN).

SSL i njegov nasljednik TLS su protokoli za upravljanjem sigurnosti prijenosa poruka preko Interneta. Često se svrstavaju u kontekst *e-commerce* poslovanja (npr., veze pomoću HTTPS), jer ovaj protokol provodi vrlo snažnu autentifikaciju između web servera i web preglednika

pomoću digitalnog potpisa (*digital signatures*) i certifikata sa najvećom razinom sigurnosti (*class 3 certifikati*).

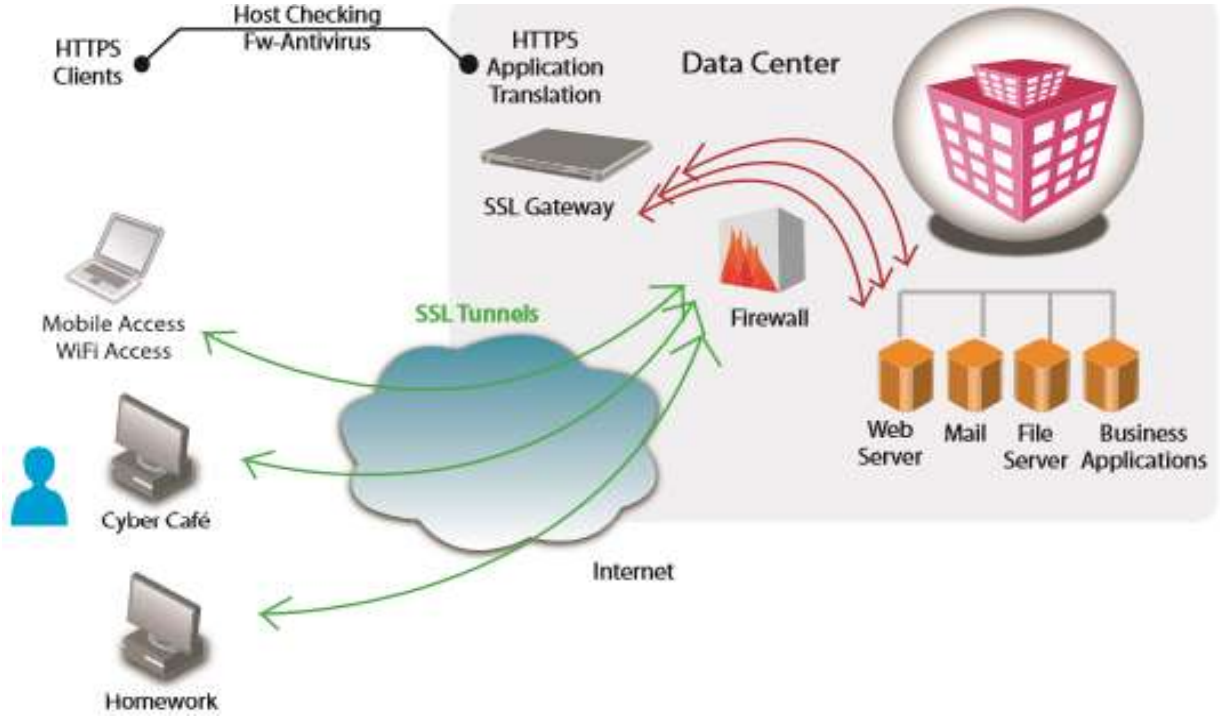
Ovakva solucija postaje prevladavajuća opcija izbora za siguran pristup sa izdvojenih lokacija za osobna računala, tablet, itd. SSL je dobio na popularnosti jer ga često koriste kompanije sa velikim brojem radnika koji rade van ureda.

Obzirom da je SSL prisutan na gotovo svakom računalu, nije potrebna nikakva posebna programska instalacija na računalima, pa je samim time uspostava cijelog VPN sustava brza i jeftina. SSL je postao rastuća konkurencija IPSec-u za siguran izdvojeni (udaljeni) pristup.

SSL VPN generalno ne zahtjeva instalaciju klijentskog software-a obzirom da je SSL integriran u svim web preglednicima, pa je većina današnjih računala su već spremna za korištenje.

Običan web preglednik nam omogućuje stvaranje tunela između udaljenog korisnika i aplikacijskog servera (*client/server*) jer se pri uspostavi vrši autentifikacija na web portal koji je pak tipično SSL VPN Gateway i jednostavno se učita (*download*) mali *plug-in* program koji će voditi promet podataka kroz tunel pomoću SSL-a)

IT infrastruktura za SSL-bazirane VPN-ove mora uključivati aplikacijske proxije (SSL mora znati za svaku vezu ili aplikacijsku sjednicu). Dodatan zahtjev je da server ima dovoljno memorije i snage procesiranja obzirom da je on SSL VPN gateway tj. predstavlja točku ulaza u VPN mrežu pa se na njemu mora vršiti autentifikacija, enkripcija i kontrola integriteta i pristupa.



Glavni tipovi SSL VPN-ova su:

1. SSL portal VPN-ovi i
2. SSL tunnel VPN-ovi.

SSL portal VPN (tzv. *clientless*): Nakon identifikacije, korisnik pristupa web site-u pomoću SSL veze kako bi pristupio različitim mrežnim uslugama putem web stranice. Web stranica je portal prema drugim uslugama (npr.veza prema drugim web serverima, web e-mailu, file sharing-u, aplikacijama koje rade na zaštićenim serverima ili bilo kojom drugom uslugom kojoj se može pristupiti tuneliranjem kroz web stranicu), ali nije veza među aplikacijama.

SSL portal VPN je web site koji korisniku omogućava korištenje raznih usluga.

SSL tunnel VPN: Ovdje SSL veza stvara pravi aplikacijski tunel između izdvojenog korisnika i lokalne mreže. Aplikacija koja je prethodno instalirana na korisničko računalo ("heavy client") ili web-based aplikacija ("light client") uspostavljaju vezu između klijenta i udaljenog servera kroz proxy koristeći „handshake". Također je moguće i stvaranje tunela koji nije aplikacijski specifičan, tj. tunela koji će korisnika spojiti direktno na lokalnu LAN mrežu jednako kao što to radi i IPSec.

SSL VPN-u može se pristupiti sa lokacija koja štite vanjski pristup obzirom da SSL prolazi transparentno kroz NAT, proxy i firewall (većina firewall-ova dopušta SSL promet).

Kod pristupa mobilnih korisnika, **SSL Gateway** će generalno štititi unutarnju mrežu primjenjujući slijedeće sigurnosne postupke:

- Korisnička autentifikacija
- Provjera korisničkog računala
- Provođenje sigurnosne politike (poput firewall-a, ili up-to-date antivirusne zaštite, već kako je to odlučeno od administratora mreže)

SSL Gateway upravlja pravima za korištenje pojedinih aplikacija ili mrežnih resursa. SSL Gateway može razlikovati izdvojene korisnike po korisničkom imenu ili po računalu koje se koristi (može prepoznati računalo koje pripada kompaniji), pa im može dodjeliti različite nivoe pristupa ovisno o tome da li je korisnik zaposlenik ili pak neki poslovni partner.

Mane i ograničenja

SSL nije dizajniran da podržava site-to-site tuneliranje. Obzirom da SSL VPN podržava TCP usluge poput web-a (HTTP) ili e-mail-a (PoP3/IMAP/SMTP), ove konfiguracije je lako implementirati, ali znatno teža je implementacija za neke druge aplikacije.

- Rast kriptiranih transakcija predstavlja jedan od glavnih sigurnosnih problema za korporativne računalne mreže. Veliki količina tog prometa prolazi kroz korporativni gateway, a obzirom da je kriptiran, ne može biti dovoljno provjeren od strane antivirusne zaštite
- U većini slučajeva korisnici sami odlučuju o prihvaćanju sigurnosnih certifikata od „treće strane" iako oni sami nemaju dovoljno znanja da bi donosili takve odluke.

- SSL-bazirani VPN-ovi ranjivi su na „denial-of-service“ napade koji napadaju njihovu TCP vezu i na vanjsku ne-autoriziranu vezu ukoliko je neko pristupao VPN-u sa javnog računala, a nije izbrisao „cookies“ i informacije o sjednici nakon napuštanja računala.

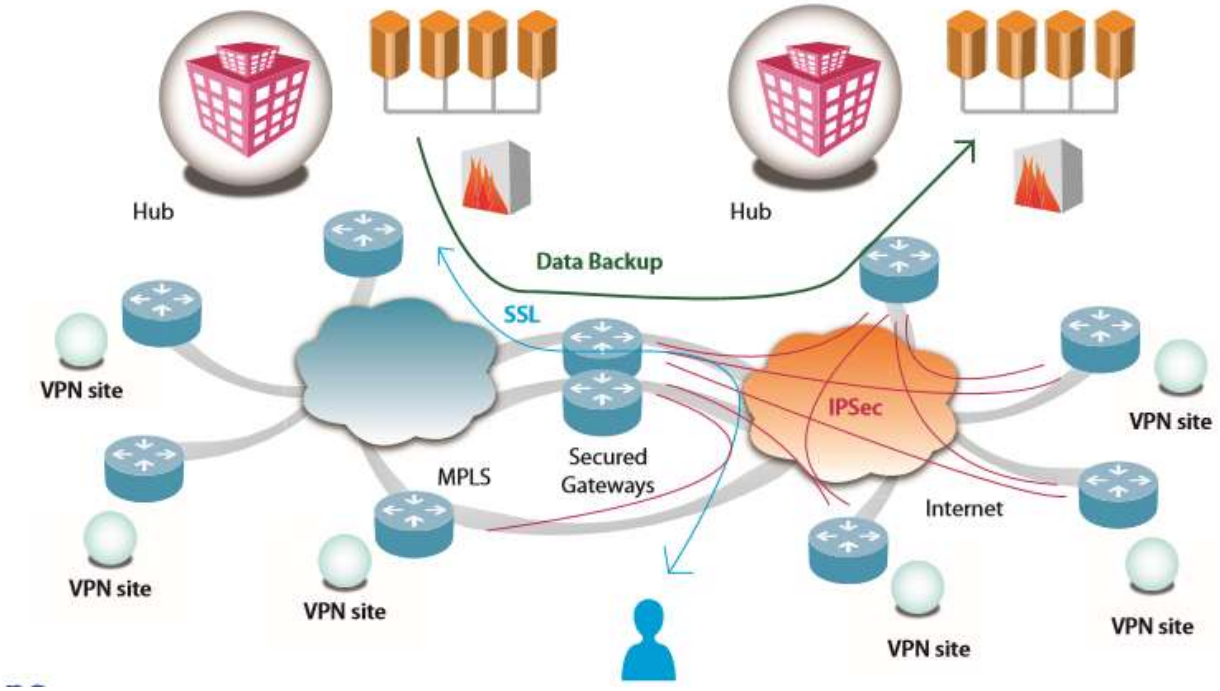
Hibridni VPN

Hibridni VPN pruža mogućnost kombiniranja raznih načina spajanja računalnih mreža kako se bi udovoljilo korisničkim zahtjevima za uspostavom globalne računalne mreže koja je ekonomična (*cost effective*) i može biti centralno administrirana (sa jedne lokacije npr. IT odjel korporacije)

Hibridni VPN omogućuje korisniku da kombinira uporabu MPLS i/ili IPSec tehnologije po želji za svaku mrežnu lokaciju. Ovakve tehničke solucije osiguravaju korisniku brzo i jednostavno širenje (otvaranje novih ureda po svijetu), omogućavaju da se za svaku lokaciju ponaosob izradi analiza i odredi vrsta spajanja na mrežu (MPLS i/ili IPSec, potrebna širina pojasa,..) koja će zadovoljiti njene potrebe, a istovremeno će biti i najekonomičnija

Kako bi se omogućilo spajanje CE baziranih VPN sustava na P usmjerivače, postavlja se jedan ili nekoliko sigurnosnih portala (*secure gateways*) između MPLS jezgrene mreže i IP javne mreže. Ovi portali podržavaju terminiranje IPSec tunela sa autentifikacijom i mapiranjem na korisnikov MPLS VPN, te osiguravaju izolaciju (razdvajanje) između javnog Interneta i VPN mreže.

Obzirom da niti jedan ISP (pružatelj javnih usluga) nije u stanju osigurati spajanje svih lokacija na globalnoj razini, velika pažnja treba se posvetiti da Hibridni VPN na najbolji način uklopi pristup od strane višestrukih ISP davatelja usluga u jednu globalnu VPN mrežu



Kako bi se odabralo najbolje tehničko rješenje, za svaku izdvojenu lokaciju neke korporacije potrebno je izvršiti analizu ponuda svih lokalnih ISP-ova, a ponekad se kompanije odlučuju i za izbor 2 različita ISP-a kako bi osigurale otpornost mreže na ispade iz rada.

Ovdje su nabrojeni najvažniji elementi na koje treba obratiti pažnju kod dizajna **transportne mreže**:

- Tranzitno kašnjenje
- Usporedba korisničkih zahtjeva sa ponudom koju nudi ISP
- Mapa korisničkog prometa – Ovisno o geografiji, lokacijama korporacijskih podatkovnih centara, te tokovima aplikacijskih prometa
- Tranzitna mreža – Analiza ISP transportne mreže, te izlaza (*peering point*) iz nje u svim regijama od interesa
- Broj IPSec krugova – Topologija se određuje nakon analize toka prometa, ograničenja koje postavlja kašnjenje signala i kompleksnost svake pojedine situacije.
- „Hosting“ mogućnost – mogućnost ISP-a da postavi portale kako bi se optimizirala *circuit-based* mreža

Rubni dizajn

Kriteriji za odabir pristupnih veza bi trebale biti:

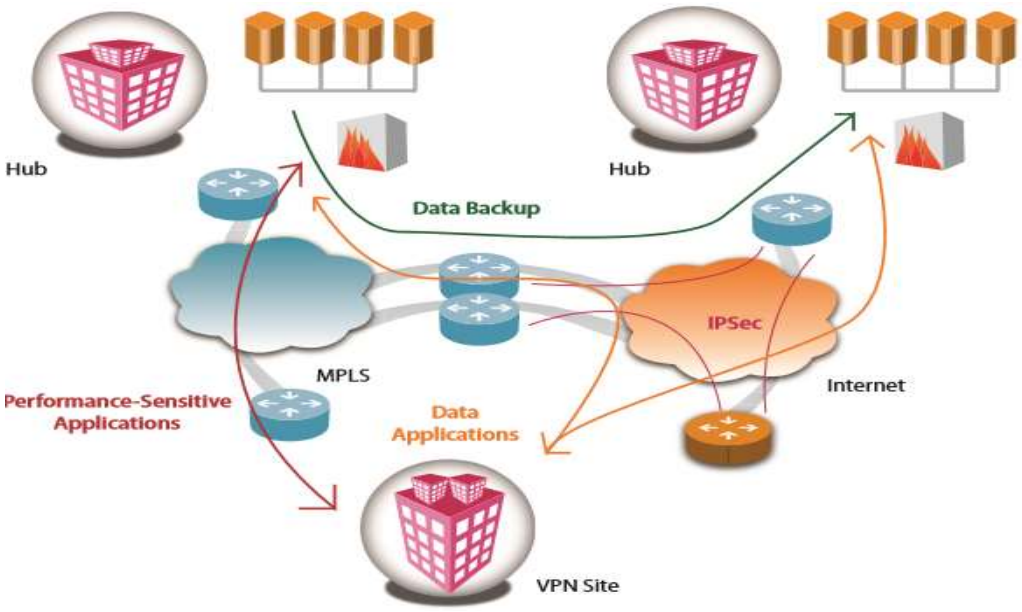
- Pristup usluzi- mogućnost pristupa lokalnoj MPLS ili Internet vezi
- Specifični zahtjevi pojedine korisnikove lokacije – Zahtjevani nivo redundancije
- Volumen prometa – Propusnost mreže u vršnim prometnim satima
- Udaljenost – do najbližeg PoP
- Korisnička pristupna tehnologija – iznajmljeni vod, DSL, koaksijalni kabel, Ethernet, Wimax
- Tranzitno kašnjenje - iz SLA
- Backup and recovery opcije

IPSec VPN može biti korišten kao „backup“ solucija za primarnu MPLS VPN vezu. Ova konfiguracija nudi dvostruki (ili jednostruki) CE, dvostruke pristupne i dvostruke transportne veze do korisnikove lokacije.

Ovakva opcija može se koristiti za aktivni ili „*standby*“ backup, a također se istovremeno može koristiti za rasterećenje tzv. „*best effort*“ prometa (za koji nije potreban QoS) sa glavne veze, kroz jeftini širokopojasni pristup (npr. ADSL).

Balansiranje prometa u ovakvim konfiguracijama može se vršiti primjenom korisnikovih pravila (*policy*) u usmjerivačima ili pak usmjeravanjem koje se bazira na mjerenjima opterećenosti sa oba prijenosna puta.

Ovakve veze mogu nam također ponuditi siguran lokalni pristup Internetu



IPSec kao jeftina opcija za sekundarnu vezu

Kontrola mrežne arhitekture

Adekvatna kontrola mreže nužna je kako bi se osigurao normalan rad osjetljivih aplikacija i kako bi se dugoročno održala visoka razina korisničkog zadovoljstva.

Prve aktivnosti u mrežnom dizajnu trebala bi biti:

- definicija mrežne arhitekture i
- uspostava procesa koji drži tu mrežu pod kontrolom

Upravljanje mrežom mora se vršiti centralizirano!

Jedno tijelo u korporaciji treba vršiti stalan nadzor mrežnih indikatora, biti proaktivno u rješavanju mrežnih problema i stalno optimizirati mrežu kako bi se smanjili troškovi,a povećalo zadovoljstvo korisnika.

Nikako se ne smije dozvoliti da lokalne inicijative uzmu maha tj. da djelatnici koji ne vide širu sliku, krenu na svoju ruku rješavati određene probleme.

Inicijalnoj mrežnoj arhitekturi treba pridružiti **set pravila** koja će kontrolirati sva buduća širenja mreže.

Ova pravila trebala bi jasno predstaviti različite zahtjeve, ograničenja i rješenja koja su korištena kod inicijalnog dizajna, te principe koji su korišteni kako bi se zadovoljili globalni standardi

Potrebno je definirati **mrežne alate** i **procese** kojima se prati uporaba mreže, mrežna i aplikacijska statistička mjerenja, dostupnost usluga, uklanjanje kvarova, upravljanje

promjenama u mreži koje su zahtjevane od novih aplikacija ili pak od povećanja volumena mrežnog prometa.

Nakon toga treba postaviti i stalno osvježavati

mrežnu referencu - točan prikaz trenutne mreže sa zacrtanim planom budućeg razvoja kako bi se osiguralo znanje o svim:

- Elementima arhitekture - Transportnoj topologiji, rubnom dizajnu i kompletnoj listi aplikacijskih karakteristika i tokova prometa
- Administrativna pitanja – Davatelji javnih usluga, ugovori SLA-ovi
- End-to-end statistička izvješća – Vrijeme kašnjenja, pouzdanost mreže (network availability), pouzdanost usluga (service availablity)

Ova lista može biti nadopunjena od strane korisnika, revizora ili pak treće strane

"Trouble-ticket " izvještavanje

Kako bi se pratio rad ISP-ova može se uvesti tzv. „*trouble-ticket*" izvještavanje, kroz koje se mogu pratiti statistike svih kvarova, uočiti koliko često su pojedini elementi u mreži nedostupni, koje je prosječno vrijeme potrebno osoblju ISP-a da popravi kvar, itd.

Statistike mrežnih performansi vrlo su snažan alat kojim se može unaprijediti rad mreže. Npr. preusmjerenje prometa sa elemenata u transportnom sloju koji često ispadaju iz rada, penaliziranje ISP-a ukoliko nije udovoljio uvjetima iz SLA

Zaključak

Za uspostavu velikih korporacijeskih VPN mreža vrlo često morati ćemo kombinirati različite tradicionalne metode, te na taj način stvoriti Hibridni VPN

MPLS VPN je tehnički najbolji, ali i najskuplji način uspostave VPN mreža.

Pruža nam apsolutnu sigurnost i izdvojenost korporacijskog prometa od ostalog prometa javnom mrežom. Pruža nam garantirani QoS što je jako bitno kada to zahtjevaju osjetljive aplikacije koje neka korporacija koristi u svome radu.

Skup je jer moramo na svakoj lokaciji imati skupu opremu (CE usmjerivače), trebamo imati skupe kvalitetne veze od svake lokacije do ulaza u MPLS mrežu (PE usmjerivač), te zbog toga što moramo sklopiti ugovor sa ISP i plaćati naknadu za održavanje VPN mreže.

IPSec VPN je jeftiniji jer ne moramo plaćati naknadu ISP-u za održavanje VPN-a.

Moramo mrežu sami izgraditi i održavati mrežu. Osigurava nam apsolutnu povjeljivost i autentifikaciju, ali ne garantira QoS jer su paketi kriptirani pa transportna mreža ne vidi klasu prometa. Ukoliko imamo više lokacija, umjesto *meshed* topologije moramo koristiti *Hub-and-spoke* topologiju koja pak unosi velika kašnjenja

SSL VPN – najjeftiniji je i najjednostavniji način za uspostavu VPN komunikacije, ali i najranjiviji i najnepraktičniji obzirom da nije dizajniran da povezuje mreže, već je prvenstveno dizajniran da povezuje pojedinačna računala sa web SSL serverom kroz kojeg se na siguran način može pristupiti pojedinim uslugama. U praksi, ovakav način pristupa korporacijskoj mreži koristiti će mobilni djelatnici ali sa ograničenim mogućnostima.

Dizajn VPN mreža velikih korporacija vrlo je kompliciran i zahtjevan posao. Treba analizirati sve aplikacije koje korporacija koristi i za svaku utvrditi koliko je robusna, tj. koliko podnosi kašnjenja ili gubitke paketa. Treba utvrditi koliko prometa i kakvog ide među lokacijama, pa temeljem toga treba dizajnirati mrežu koja će kapacitivno i kvalitativno zadovoljiti sve zahtjeve. Odmah uz dizajn arhitekture mreže treba uspostaviti i procese nadzora i održavanja. Mreža se treba stalno nadgledati i optimizirati. Sve to se treba raditi centralizirano jer treba sagledati cijelu sliku.

PREDAVANJE 14 - Praćenje mrežnih performansi

U ovom odjeljku izvršiti ćemo pregled dostupnih tehnologija za praćenje mrežnih performansi u IP mrežama sa omogućenim QoS uslugama, te udovoljavanje SLA zahtjevima. Postoje dva osnovna pristupa koja se razmatraju u praćenju mrežnih performansi, a to su ***aktivno*** i ***pasivno*** praćenje performansi.

Pasivno praćenje mrežnih performansi- Kod pasivnog praćenja performansi, mrežni elementi snimaju statistike mrežnog prometa koje nam pak prilikom pregleda mogu pružiti uvid u stanje mrežnog prometa na tom elementu. Statistički uzorci sakupljaju se periodički, te se kasnije analiziraju pomoću raznih aplikacija za obradu rezultata mjerenja. Ovakav način mjerenja predstavlja mikro-mjerenja jer se svaki mrežni element posmatra pojedinačno, odvojen od svih ostalih elemenata mreže. Ukoliko želimo dobiti uvid u stanje cijele mreže potrebno je gledati situaciju svih mrežnih elemenata kako bi dobili potpunu sliku mrežnog rada. Pasivno praćenje performansi ne zahtjeva unošenje nikakvog dodatnog prometa u mrežu u svrhu mjerenja.

Aktivno praćenje mrežnih performansi- Za razliku od pasivnog, aktivno praćenje mrežnih performansi uključuje slanje dodatnog prometa kroz mrežu. Kreirani testni tok podataka u sebi sadrži „probne“ pakete čija je jedina svrha otkrivanje mrežnih performansi. Analizom primljenog toka podataka možemo doći do karakteristika mreže. Aktivno praćenje performansi pruža makro-mjerenja mrežnog udovoljavanja SLA zahtjevima jer mjeri performanse mreže kao cjelovitog sustava od izvora do prijemnika podataka.

Sustavi za pasivno i aktivno praćenje mreže mogu biti postavljeni iz brojnih razloga ali najčešće za praćenje i izvještavanje o pruženim mrežnim uslugama te postignutim SLA zahtjevima ili pak kao input ISP operaterima za dalje mrežno širenje i optimizaciju.

Pasivno praćenje mrežnih performansi

Iz QoS perspektive pasivno praćenje mrežnih performansi koristi snimljene prometne statistike pojedinih elemenata mreže koje u sebi sadrže QoS podatke koje element pruža, poput npr. broja propuštenih bita ili duljine reda čekanja paketa. Povlačenje ovih statistika sa elemenata iz njihove MIB (management information base) baze, obično se radi pomoću Simple Network Management Protocol (SNMP) [RFC 1157]. Način prikupljanja uzoraka i njihovo statističko značenje opisuje se u slijedećim odjeljcima.

Koliko često treba uzimati uzorke (frekvencija uzorkovanja)?

U praksi ova odluka se donosi u ovisnosti u veličini spremnika za prikupljanje uzoraka *Sustava za mrežno praćenje* (network management system-NMS), broja mrežnih elemenata sa kojih ćemo skupljati uzorke, opterećenja koje prikupljanje uzoraka nameće mrežnim elementima sa kojih uzorke sakupljamo, te utjecaja samog dodatnog prometa koji je izazvan povlačenjem sakupljakupljenih uzoraka sa elemenata do Sustava za mrežno praćenje. Mnogi od povučenih statističkih uzoraka biti će u formi broja paketa ili bajta – ovakvi podaci mogu nam poslužiti za određivanje prometnih zahtjeva u promatranom intervalu. Dulji intervali sakupljanja imaju veću količinu podataka i mogu poslužiti za pregled trendova prometa. Međutim, dulji periodi sakupljanja će biti statistički obrađeni u samome mrežnom elementu

prije slanja u centar pa ćemo mi vidjeti samo srednju vrijednost što može maskirati probleme koji se javljaju u određenim trenutcima.

U svakom slučaju, za praćenje zadovoljavanja SLA uvijeta porebno je vršitiuzorkovanje sa mrežnih elemenata što je češće moguće (tj. maksimalno koliko namto sam sustav dozvoljava) kako problemi ne bi ostali skriveni.

Statistike svake pojedinačne veze (*per-link statistics*)

Statistike svake veze mogu se koristiti za različite namjene ovisno o tome na kojem dijelu mreže su snimane.

- *Pristupne (access) veze*. Pristupne veze mogu predstavljati granicu DiffServ domene i korisnik/pružatelj usluga domene. Zbog toga se njihove QoS statistike koriste i za otkrivanje problema na vezi kao i za izvještavanje o isporučenom QoS-u prema korisniku.
- *Jezgrene (core) veze*. Na jezgrenim vezama, statistike se koriste za otkrivanje problema na samoj vezi te za procese planiranja samih jezgrenih kapaciteta od strane pružatelja usluga.

Većina proizvođača opreme ima implementiranu MIB bazu u svim mrežnim elementima koja se može koristiti za povlačenje *per-link* statistike.

Praćenje klasifikacije

Usmjerivač može različite tokove prometa klasificirati u jednu prometnu klasu, na koju će se onda primjenjivati jednaka pravila. Praćenje klasifikacije prometa može nam biti značajno kako bi smo odredili koliki je *ponuđeni promet* za svaku pojedinu klasu prometa te koliki je udio te klase u ukupnom prometu. Zanimljive su nam dvije statistike:

Statistika po klasifikacijskom pravilu – Ukoliko se koristi više odvojenih pravila koja nam različite prometne tokove klasificiraju kao jednu jedinstvenu klasu, zanimljivo nam je vidjeti koji je udio upotrebe svakog od tih klasifikacijskih pravila, u ukupnom formiranju toka jedne klase prometa. Nadalje, ukoliko znamo broj paketa i veličinu paketa koji su klasificirani u jednu klasu, moguće je doći do srednje vrijednosti veličine paketa za svaku pojedinu klasu.

Ukupna statistika – Za svaku prometnu klasu također je važno da znamo ukupni broj paketa koji je klasificiran u tu klasu (sumarno, koristeći sva klasifikacijska pravila za tu klasu). Glavna uporaba ove statistike je da se vidi da li je promet pravilno raspodjeljen po klasama.

Monitoriranje primjene politika

ISP pružatelji javnih usluga u svojoj mreži primjenjuju različite „politike“ tj. pravila kako bi zaštitili svoju mrežu i njene performanse. Jedan takav primjer je ograničenje veličine VoIP paketa kojima je dozvoljeno da budu klasificirani kao VoIP te preneseni uz određena QoS jamstva do odredišta. Ukoliko bi se dozvolilo da VoIP paketi jako velike veličine ulaze u sistem, to bi moglo izazvati velika kašnjenja (npr. serijalizacije, čekanja u redu, itd), te narušiti performanse čitave mreže jer bi mreža pokušala osigurati kapacitet za VoIP (jer je najvišeg

prioriteta), pa bi mogla narušiti kvalitetu usluge svih ostalih klasa. Kako bi se to spriječilo operateri postavljaju na razna mjesta (obično na pristupne veze) uređaje koji nadgledaju provođenje njihovih politika i ne dozvoljavaju paketima koji ne slijede njihove politike da uđu u njihov QoS sustav. Praćenje statistika sa „*Policers*“ funkcija omogućava nam da pratimo njihov rad te da vidimo gdje se nalaze glavni problemi.

Praćenje čekanja u redovima (*queing*) i gubljenja paketa (*dropping*)

Za sve klase čekanja u redu, obično se prate slijedeće statistike:

- *Broj paketa i bajta koji su preneseni* - ukupan broj paketa koji su uspješno odaslani iz reda čekanja od strane raspoređivače, te njihov ukupan broj bajta.
- *Broj paketa i bajta koji su izgubljeni* – ukupan broj paketa i njihov zbroj bajta koji su odbačeni od strane funkcije za upravljanje redom čekanja u usmjerivačima.

Statistike nam također pokazuje postotak uporabe svakog od mehanizama odbacivanje paketa u redu čekanja u ukupno odbačenim paketima.

Praćenje odbacivanja paketa za začelja reda (*Tail Drop*)

Ukoliko je uključen mehanizam za odbacivanje paketa kada se desegne maksimalni broj paketa u redu čekanja, tada je potrebno pratiti broj paketa i bajta koji su odbačeni uporabom tog mehanizma.

Obzirom da pri uporabi QoS mehanizama možemo definirati duljinu reda čekanja za svaku klasu prometa ponaosob, trebamo pratiti statistike po svakoj klasi prometa.
Ukoliko imamo veliki postotak odbačenih paketa neke klase to znači da:

- Ili nam red čekanja neke klase radi u značajnom zagušenju, pa toj klasi moramo dati više širine pojasa tj. podići kapacitet ili
- Imamo loše podešeni limit (prenisko postavljen) za broj paketa određene klase koji mogu čekati u redu, potrebno izvršiti novo podešavanje limita

Praćenje statistike prioritizacije odbacivanja paketa sa začelja reda(*Weighted Tail Drop*)

Operateri imaju mogućnost da izvrše označavanje klasa prometa ovisno o tome da li je klasa pokrivena SLA ugovorom ili ne. Ukoliko je takvo označavanje izvršeno, oni mogu definirati da ukoliko dođe do potrebe za odbacivanjem paketa iz reda čekanja, da se odbacuju paketi onih usluga koje nisu zagarantirane SLA ugovorom, kako se ne bi narušila SLA statistika. Prometu paketa koji je označen kao „van SLA ugovora“ smanjuje se granica reda čekanja, dok se povećava granica prometa pokrivenim SLA ugovorom. Statistika bi uvijek trebala pokazivati zanemarivo malo odbacivanje SLA paketa u odnosu na ne-SLA pakete. Ukoliko nije takva situacija nešto nije u redu.

Praćenje RED (*Random Early Detection*)

RED je aktivni mehanizam za upravljanje redom čekanja koji je napravljen da popravi ukupne performanse TCP baziranog prometa. Ukoliko je uključen RED mehanizam, tada bi trebalo pratiti slijedeće statistike:

Broj paketa i bajta koji se nalaze u redu čekanja – broj paketa i njihov broj bajta koji se se uspješno postavili u red čekanja za određeni RED profil. Ukoliko je samo jedan RED profil aktivan, tada bi ovoj broj trebau biti jednak ukupnom broju svih paketa su odaslani iz reda čekanja

Broj paketa i bajta nasumično odbačenih.- „Nasumično odbačeni" su RED odbačeni paketi što se događa kada je izmjerena srednja vrijednost duljine reda čekanja između minimalne i maksimalne vrijednosti za taj određeni RED profil. Ukoliko je RED dobro konfiguriran, tada će većina odbačenih paketa spadati u „Nasumično odbačene". Ukoliko je postotak svih RED odbacivanja relativno velik to nas navodi da je red čekanja relativno velik pa je potrebno razmotriti širenje pojasa (povećanje kapaciteta), ili je potrebno smanjiti prometno opterećenje tog reda ili treba provjeriti konfiguracije minimalnog i maksimalnog praga reda čekanja, ili je prioritizacijska konstanta (*waighting constant*) postavljena previše agresivno ili pak postoji neka aplikacija koja regulira red čekanja koja izaziva probleme.

Broj paketa i bajta koji su prisilno odbačeni. Odbacivanja koja nastaju odbacivanjem paketa kada mjerenje srednje vrijednosti reda čekanja prelazi postavljeni maksimalni prag, nazivaju se prisilna odbacivanja (*forsed drops*). Ukoliko je RED dobro postavljen tada bi nasumična odbacivanja trebala osigurati da je prosječna duljina reda čekanja uvijek ispod konfiguriranog maksimalnog praga. Ukoliko je postotak prisilno odbačenih paketa relativno velik u odnosu na ukupni broj RED odbacivanja, onda treba provjeriti zbog čega se to događa.

Prosječna duljina reda čekanja. Ukoliko je prosječna duljina RED reda čekanja vrlo često blizu postavljenog praga za maksimalnu duljinu reda, ovo nas navodi da ili red ima znatna zagušenja pa treba širiti kapacitete ili pak da smo loše postavili RED pragove.

Praćenje WRED (*Weighted RED*)

WRED se primjenjuje u slučajevima kada operater želi napraviti različita pravila koja će se primjenjivati za pakete prometa koji je obuhvaćen SLA ugovorom i prometa koji nije. Kako bi se to postiglo, primjenjuju se dva RED profila za pakete u istom redu čekanja, a za pakete prometa koji je van SLA ugovora primjenjuje se znatno agresivnije konfiguriran RED profil (npr. niže postavljeni minimalni i maksimalni pragovi za red čekanja), pa će prilikom pojave zagušenja ti paketi bi odbacivani kako bi se zaštitili paketi SLA prometa.

Praćenje sustava (*System monitoring*)

U idealnom slučaju sva odbacivanja paketa na usmjerivaču inteligentno su upravljana od strane QoS funkcija koje smo mi konfigurirali na tom usmjerivaču. Ipak, u praksi se često javlja situacija da imamo odbacivanja paketa zbog nekih ograničenja samog sustava. Ukoliko na tom dijelu sustava nema logike koja razlikuje klase prometa, tada su i gubici paketa neovisni o klasi. Jasno nam je da bi sustavi trebali biti dizajnirani da se izbjegnu ovakve pojave, pa nam je bitno da pratimo ovakve pojave jer mogu ukazivati na ozbiljne probleme samog sustava prijenosa koji mogu ozbiljno poremetiti SLA i to po svim prometnim klasama. Takvo sustavno odbacivanje paketa ovisiti će o implementaciji pojedinog mrežno elementa, ali najčešće se javljaju uslijed:

Odbacivanja uslijed prepunjegog spremnika (no buffer drops) Kada se memorijski spremnik, koji je dijeljen između više redova čekanja, napuni do kraja može doći do situacija da je u

trenutku dolaska nekog paketa, memorija spremnika ne može više smjestiti dolazni paket pa on mora biti odbačen. Ovakve pojave trebale bi zaista biti rijetke iznimke u svakom iole dobro dizajniranom sustavu.

Ulazna odbacivanja (input drops) Događaju se u situacijama kada je ulazni spremnik premalen. Ovakva odbacivanja su simptom u slučajevima kada je dolazna brzina paketa veća od brzine procesiranja samog usmjerivača.

Odbacivanja samog sustavca poput *Odbacivanja uslijed prepunjegog spremnika* ili *Ulaznog odbacivanja,* trebala bi se pratiti pomoću posebnih mjerenja koja bi trebao osigurati proizvođač same opreme pošto se takva mjerenja ne mogu dobiti iz Diffserv MIB baze. Obzirom na utjecaj koji ovakve pojave imaju na cijeli sustav, svako pojavljivanje ovakvih odbacivanja paketa treba odmah pokrenuti opsežne istražne radnje kako bi se uzrok pronašao i što prije otklonio.

Matrica jezgrenog prometa

Ovo je matrica ulaznih (ingress) i izlaznih (egress) prometnih zahtjeva jezgrene mreže. Prometna matrica može biti mjerena ili predviđena pomoću statistika koje se sakupljaju korištenjem tehnika pasivnog nadgledanja mreže. Glavni razlog zašto mjerimo matricu prometa je taj što nam ona služi kao input za dalje planiranje kapaciteta jezgrene mreže. Također nam služi za predviđanje utjecaja rasta prometa, kao i za simulacije „*what-if*" scenarija za slučajeve raznih mrežnih kvarova. Postoje brojne tehnike koje služe za prikupljanje matrice prometa.

Aktivno praćenje mreže

U idealnom slučaju bilo bi moguće mjeriti jitter, kašnjenje, gibitke paketa i propusnost koje aktualni promet osjeća dok prolazi kroz prijenosni sustav. U nekim slučajevima može biti moguće dobiti te infomacije od krajnjih (odredišnih) aplikacija u sustavu. Npr. tamo gdje se koristi real-time protokol RTP, oznaka vremena odašiljanja paketa i broj sekvence iz RTP zaglavlja mogu se koristiti za izračun kašnjenja, jittera i gubitka paketa na odredištu pristiglog toka podataka. Ovakva mjerenja u praksi baš i nisu moguća iz slijedećih razloga: mnoge aplikacije uopće ne koriste RTP protokol, povlačenje ovakvih statistika iz svih aplikacija krajnjih sustava bilo bi nemoguće, krajnji sustav možda nema istog vlasnika kao i prijenosna mreža. Nadalje, kako bi osigurali ove informacije na razini cijele mreže, bilo bi potrebno da svi mrežni elementi jednoznačno identificiraju svaki paket i da mu dodaju vremensku oznaku (*timestamp*) koja bi bila vrlo precizna,....sve to nije moguće u praksi.

Alternativni pristup tom problemu je *Aktivno praćenje mreže* koje je uglavnom provedivo. Aktivno praćenje koristi posebno napravljene (sintetizirane) testne tokove podataka koji sadrže probne pakete, a čiji je cilj da simuliraju pravi mrežni promet između uređaja za aktivno mrežno praćenje kako bismo dobili karakteristike mreže.

U mrežama u kojima je pokrenut Diffserv, aktivno praćenje može se koristiti za mjerenje performansi svih klasa prometa. Ukoliko želimo postaviti sustav za aktivno mrežno praćenje kako bi mjerili zadovoljavanje SLA ugovora, potrebno je postaviti SLA probni sustav koji podržava definirane metrike za IP performance (IPPM) poput onih koje je definirao IETF. U takvom probnom sustavu, testni uređaji (*active monitoring agents*) se postavljeni na postojeće

mrežne elemente, i testni tokovi podataka se šalju između tih uređaja. Ti uređaji mjere primljene tokove i spremaju statistička mjerenja, koja se potom periodički povlače pomoću SNMP protokola u neki nadzorni centar. Pri postavljanju aktivnog sustava praćenja mreže potrebno je unaprijed odrediti:

- Kakvi testni tokovi podataka će se koristiti
- Koliko često će se testovi provoditi i koliko će sami testovi trajati
- Kakva metrika će se mjeriti za primljene tokove
- Na koje mrežne elemente će se postaviti testni uređaji i
- koje će se sve staze mjeriti

Parametri testnog mjernog toka

Karakteristike testnog mjernog toka utjecati će na karakteristike mreže koja se mjeri. Rezultati koje dobijemo ovakvim mjerenjima imaju smisla samo ukoliko naš testni mjerni tok podataka ima iste karakteristike kao i neka klasa stvarnog prometa čije performanse testiramo. Sada se postavlja pitanje, kakvi to parametri testnog toka moraju biti kako bi smo mogli mjeriti karakteristike poput kašnjenja, jittera, gubitka paketa, propusnosti i sl. za neku klasu prometa. To ćemo sada malo dublje razjasniti.

Veličina paketa

Postoje dva pristupa pri određivanju veličine testnih paketa za aktivno mrežno praćenje:

- *Jednake veličine kao i paketi prometa kojeg pratimo*. Na ovaj način točno pratimo kašnjenje serijalizacije koje može biti značajno na vezama niže brzine. Kod zagušenja, veće su šanse da će manji paket biti postavljen u red čekanja jer on možda još i stane u preostali dio slobodne memorije spremnika. Ukoliko koristimo stvarnu veličinu paketa, tada dobivamo bolji uvid u ovu situaciju.
- *Mali paketi*. Ovo je alternativni pristup, a ima dva opravdanja za taj pristup.
  Prvi razlog je ekonomski. Ovakvi paketi koriste se u mrežama gdje imamo vrlo spore pristupne mreže (uski pojas) poput nekih mobilnih mreža. Drugi razlog je ukoliko nam samo mjerenje zahtjeva veliki broj testnih paketa, pa koristimo male pakete kako bi smanjili utjecaj na živu mrežu.

Strategija uzorkovanja

Strategija uzorkovanja testnih paketa određuje distribuciju kašnjenja međusobno odvajajući testne pakete. Postoje tri strategije koje se koriste:

- *Periodičko uzorkovanje*. Vrši se na način da se testni paketi (*probes*) šalju u jednakim vremenskim intervalima, npr. svake sekunde.
- *Nasumično (random) uzorkovanje*. Vrši se tako da se testni paketi šalju u nasumičnim vremenskim intervalima(koji su određeni funkcijom gustoće vjerojatnosti).
- *Grupno uzorkovanje*. Umjesto da se šalju jedan po jedan odvojeni paket unutar nekog vremenskog intervala, kod grupnog uzorkovanja, testni paketi šalju se u grupi

(*burst*) jedan odmah iza drugoga. Vremenski period između odašiljanja dvije grupe testnih paketa može biti periodičan ili nasumičan

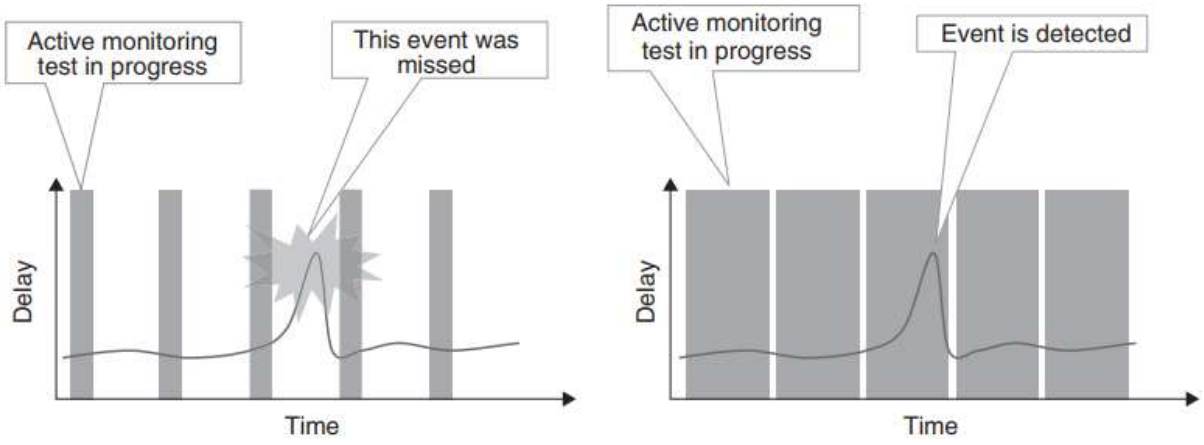
U praksi, najčešće se koriste periodični testni tokovi sa konstantnim vremenskim razmakom između odaslanih test paketa. Ovakve testove najlakše je postaviti, a i rezultate je najlakše interpretirati.

Frekvencija uzorkovanja

Određuje broj poslanih probnih paketa za vrijeme trajanja testa. Utječe direktno i na živu mrežu jer se u standardni promet injektira još i dodatni testni promet koji može imati utjecaj na sveukupne mrežne performanse. Npr. ukoliko injektiramo veliku količinu testnih paketa u neku vezu sa relativno malom širinom pojasa, sami testni paketi mogu uzrokovati degradaciju performansi, pa ni sami mjerni rezultati nisu relevantni. Sa druge strane, ukoliko je frekvencija uzorkovanja premala, mjerne karakteristike testnog toka možda neće odražavati karakteristike pravog toka podataka. Iz tih razloga važno je dobro odrediti frekvenciju uzorkovanja. U praksi nema nekog jedinstvenog odgovora kolika bi frekvencija trebala biti, ali uglavnom se prati karakteristika klase prometa koja se mjeri.

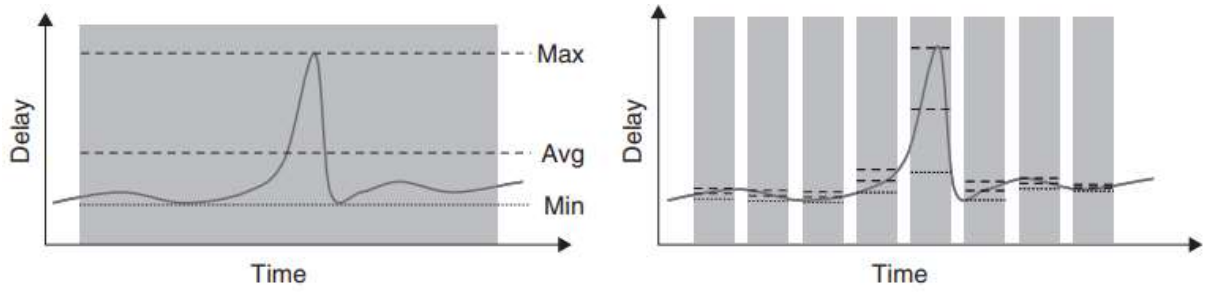
Trajanje i frekvencija izvođenja testa

Trajanje testa definira koliko dugo će se neki aktivni test izvoditi. Frekvencija testiranja određuje koliko često će se pokretati aktivni testovi. Trajanje test i frekvencija testiranja moraju dovoljno dugi i čest kako bi mogli prikazati pravo stanje mjerenog prometa.



Što je niža frekvencija i trajanje testa, to je veća vjerojatnost da će nam problemi promaknuti i ostati nedetektirani, kao što je prikazano na slici iznad.

Obzirom da mjerni agenti uglavnom pohranjuju samo statističke srednje vrijednosti, a ne sirove mjerne rezultate, trajanje mjerenja može imati utjecaj na same izmjerene vrijednosti kako je prikazano na slici ispod.



Slično kao što smo rekli i za pasivno mrežno praćenje, duži testovi koriste se za određivanje trendova, a kraći i češći tamo gdje je potrebna veća granularnost uzoraka.

Za traženje problema kod SLA i za izvještavanje obično se koriste mjerenja sa trajanjem testa od 2 minute, a izvode se konstantno.

Protokoli, sučelja (ports) i aplikacije

Kako bismo osigurali da će nam mjerenja biti relevantna, moramo osigurati da će naš testni tok biti jednako klasificiran kao i tok podataka kojeg mjerimo i to cijelom duljinom mjerne staze. Ukoliko je aktiviran Diffserv mehanizam, aplikacije će osjetiti performanse mreže ovisno o načinu na koji je njihov promet klasificiran.

Tamo gdje se koristi samo jedna klasifikacija, testni paketi moraju imati iste oznake (DSCP, IP precedence or even 802.1p based) kao i mjereni tok, ali ne moraju imati iste IP adrese ili protokole.

Tamo pak gdje se koristi kompleksna klasifikacija, testni paketi moraju u potpunosti biti jednako klasificirani kao i paketi mjerenog toka.

Npr. kod VoIP prometa paketi su određeni brojevima UDP sučelja i IP adresom izvora paketa, pa bi zaglavlje testnog paketa moralo biti takvo da odgovara tim podacima.

Ukoliko je mjereni tok podataka na bazi TCP protokola, IP protokol broj testnog paketa mora biti postavljen na 6 kako bi signalizirao TCP protokol.

Ukoliko je aktiviran Diffserv sa AF klasama koje podržavaju *ugovorni* i promet *van ugovora*, potrebno je da naš testni paket bude označen kao ugovorni od strane sustava.

Mjerne metrike za aktivno praćenje mrežnih performansi

Kašnjenje

Kada govorimo o kašnjenju moramo razlikovati pojmove jednosmjernog kašnjenja i povratnog kašnjenja (*round trip time - RTT*).

Mjerenje RTT kašnjenja zahtjeva da se testni paket pošalje od strane testnog uređaja (*active monitoring agents*) prema odredištu, a po primitku testnog paketa, odredišni uređaj ga pošalje nazad prema testnom uređaju. Obzirom da se u odaslani paket postavlja vremenska oznaka trenutka odašiljanja (*timestamp*), a prilikom dolaska paketa nazad zna se i točno vrijeme povratka, vrlo je jednostavno odrediti vrijeme koje je paketu trebalo da prođe put do odredišta i nazad, tj. povratno vrijeme kašnjenja –RTT.

Mjerenje jednosmjernog kašnjenja pak zahtjeva da se prije samog mjerenja izvrši sinhronizacija lokalnog sata u elementu koji odašilje i elementu koji prima testni paket. Mjerenje vrši prijemnik uspoređujući vrijeme slanja (*timestamp*) iz paketa sa vremenom kada je paket primljen. Najveći izazov kod ovakvih mjerenja je uspostaviti dovoljno preciznu sinhronizaciju lokalnih satova na oba elementa (odašiljaču i prijemniku) jer od toga ovisi preciznost mjerenja.

Znatno je jednostavnije raditi RTT mjerenja jer nije potrebno vršiti precizne sinhronizacije elemenata, a mjerenje samo RTT vrijednosti dovoljno je za veliki broj aplikacija.

Za aplikacije poput VoIP ili interaktivne video konferencije, RTT mjerenja nisu dovoljna. Ipak zbog složenosti mjerenja često se ipak standardno rade samo RTT mjerenja, a tek ukoliko se ustanovi probijanje limita kašnjenja, vrši se jednosmjerno mjerenje za detaljnu analizu i otklanjanje SLA problema.

Većina mjernih sustava predstaviti će nam nekoliko statističkih podataka vezanih za kašnjenja, pa je potrebno znati značenje svake od tih vrijednosti.

Minimalno kašnjenje. – Pruža nam uvid u najmanje moguće kašnjenje koje se može ostvariti na nekoj trasi, a to se događa u trenucima kada je trasa prometno potpuno neopterećena. Minimalno kašnjenje uglavnom će se sastojati od propagacijskog kašnjenja, kašnjenja prospajanja i serijalizacijskog kašnjenja. Čim se pojave kašnjenja veća od minimalnog, znamo da su se počela javljati zagušenja negdje na trasi.

Kašnjenje većine paketa (*High percentile delay*) – Sama informacija o maksimalnom kašnjenju koje je osvareno od bilo kojeg paketa nam nije uopće zanimljiva jer će možda jedan ekscesni paket, u nekoj situaciji imati jako veliko kašnjenje. Takve vrlo rijetke slučajeve ne treba uvrštavati u statistiku. Zato se gleda kašnjenje većine paketa (npr. 99,9% paketa). To su gotovo svi paketi sa izbačenim ekscesnim paketima. Ova mjerenja daju nam maksimalno kašnjenje paketa, ali sa ipak izbačenih npr. 0,01% ekscesnih paketa

Mjerenje prekoračenje praga (*Threshold exceeded count*). Za aplikacije koje imaju stroge kriterije za kašnjenje može biti zanimljivo pratiti broj paketa (od ukupnog broja mjernih paketa) koji su imali kašnjenje veće od dozvoljenog. Kod takvih aplikacija, paket koji stigne sa kanjenjem većim od dozvoljenog je u biti potpuno beskoristan tj. tretira se kao izgubljeni paket.

Prosječno kašnjenje (*Average delay*) – Prosječno kašnjenje zanimljivo nam je sa stajališta određivanja trendova u mreži, ali sa stajališta kratkoročnog promatranjamrežnih performansi nema neko posebno značenje. Ukoliko ga želimo gledati u svjetlu kratkoročnih performansi, trebalo bi uz njega mjeriti i standardu devijaciju uzorka, pa ukoliko je ona veća od normalne, možemo naslutiti da je riječ o nekakvim prijelaznim pojavama, a ne trendu.

Varijacije kašnjenja – Jitter

Kao što smo to već prije spomenuli Jitter se smatra varijacijom jednosmjernog kašnjenja između dva uzastopna paketa. Kod mjerenja jednosmjernog kašnjenja treba izvršiti sinhronizaciju lokalnog sata odašiljačkog i prijemnog mjernog elementa što izaziva brojne poteškoće. Srećom, za mjerenje Jittera ta sinhronizacija nije nam potrebna jer nije potrebno

da znamo individualno vrijeme jednosmjernog kašnjenja paketa. Jitter može izračunati iz podatka o vremenu odašiljanja (timestamp) uzastopnih paketa, pa nam je mjerenje varijacije kašnjenja tj. Jitter-a, jednostavnije od mjerenja jednosmjernog kašnjenja paketa.

Ukoliko je Ts[n] vrijeme slanja paketa n, a Tr[n] je vrijeme kada je primljen.

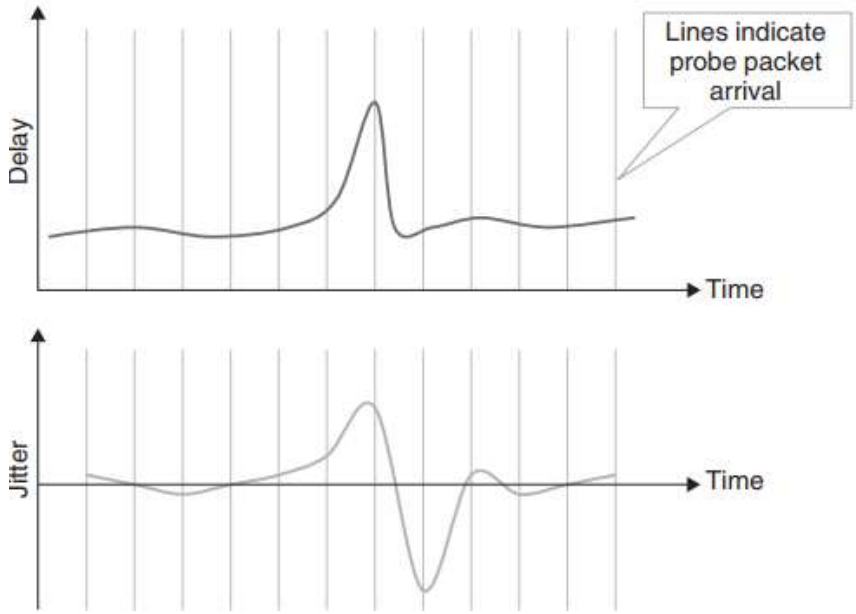
„Jednosmjerno kašnjenje“ (koje nije apsolutno točno jer nismo sinhronizirali satove) ovog paketa označavimo sa D[n].

„Jitter“ tj. varijacija kašnjenja u odnosu na kašnjenje slijedećeg paketa (n+1) može se izračunati na način

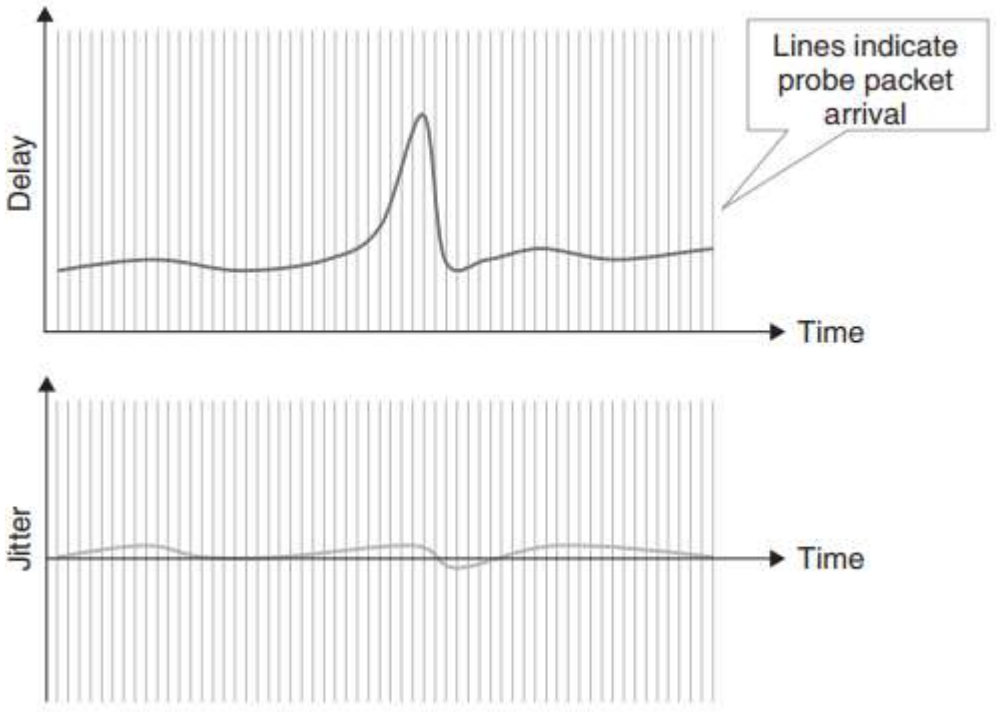
$$\begin{aligned} J[n, n+1] &= D[n+1] - D[n] \\ &= (T_r[n+1] - T_s[n+1]) - (T_r[n] - T_s[n]) \\ &= (T_r[n+1] - T_r[n]) - (T_s[n+1] - T_s[n]) \end{aligned}$$

Osim samog „Jitter-a“, najvažnije statistike koje su nam zanimljive su: varijacije kašnjenja većine paketa (*high percentile jitter*), broj paketa koji prelaze prag varijacije kašnjenja (*threshold exceeded count*), i prosječna varijacija kašnjenja (*average jitter*).

Iz prakse je primjećeno da se za mjerenje Jitter-a treba koristiti veliki broj uzastopnih mjernih uzoraka (*batches*) jer slanje pojedinačnih nasumičnih (*random*) probnih paketa dovodi do velikih vrijednosti izmjerenog jitter-a, što ne daje pravu sliku stanja u mreži kod realnog prometa. Taj fenomen je prikazan na slikama ispod.



Niža frekvencija poslanih probnih paketa – veći izmjereni jitter



Viša frekvencija poslanih probnih paketa – manji izmjereni jitter

Gubitak paketa

Kako bismo bili u mogućnosti pravilno odrediti gubitak paketa, potrebno je da na neki način razlikujemo pakete koji su stvarno potpuno izgubljeni (odbačeni) od onih koji su stigli ali sa velikim kašnjenjem pa su za neku aplikaciju beskorisni. Kod SLA, gubitak paketa se uglavnom definira statistički za neko određeno vrijeme. Mjerenje te statistike može nam biti zanimljivo sa strane određivanja trendova, ali ipak nam ne gorvori ništa o tome kako su ti paketi bili izgubljeni. Zbog toga temeljem samo tog mjerenja ne možemo niti zaključiti kakav će to utjecaj imati na rad neke aplikacije. [RFC 3357] uvodi neka dodatna mjerenja koja opisuju neka „pravila ponašanja" kod pojave gubitaka (*loss patterns*) koja mogu pomoći kod analize mogućeg utjecaja tih gubitaka paketa na rad samih aplikacija:

- **Period gubitka**. Definira frekvenciju pojavljivanja gubitaka paketa i vrijeme trajanja gubitka paketa

- **Udaljenost gubitka**. Vrijeme proteklo između dva uzastopna perioda gubitka.

Predlaže se da se period gubitka i udaljenost gubitka mjere i uspoređuju sa aplikacijskim pragovima tolerancije kako bi se ustanovilo gdje će ti gubici uzrokovati neprihvatljivu degradaciju aplikacijkih performansi.

Širina pojasa i propusnost

Aplikacijska propusnost ovisi o mnogim faktorima koji mogu varirati u širokim rasponima ovisno o dizajnu samog krajnjeg sustava i prometnom profilu. Aktivno praćenje mreže ne pokušava eksplicitno odrediti aplikacijsku propusnost već je izvodi iz nekih drugih mjerenja poput mrežnog RTT i gubitka paketa. Uzmimo za primjer

TCP. Aktivni mjerni sustav može poslati paket koji samo izgleda kao TCP paket, ali uglavnom nema TCP složaj, pa paket nije kontroliran od strane TCP-og sustava kontrole toka i njegovih mehanizama kontrole zagušenja.

Dolazak paketa van redosljeda (Re-ordering)
IP nam ne garantira da će paketi na odredište stizati u istom slijedu kako su i poslani što meže imati velike implikacije na rad nekih aplikacija.

Nepravilan slijed dolazaka paketa sustav za praćenje detektira pomoću broja sekvence koji se dodaje svakom paketu prilikom odašiljanja, a na prijemnom dijelu detektira se da li paketi stižu po redoslijedu. Ukoliko neki primljeni paket ima manji sekvencni broj od paketa koji je zaprimljen prije njega, on se smatra da je stigao „van redosljeda“ (*out of order* ili *re-ordered*). Najjednostavnija metrika za mjerenje ovog fenomena je postotak paketa koji su stigli „van redoslijeda“. (Paketi koji su stigli van redoslijeda /ukupan broj pristiglih paketa)

Raspoloživost
Raspoloživost za IP usluge definira se kao mrežna raspoloživost ili kao raspoloživost usluge, kao što smo to već prije opisali.

- **Mrežna raspoloživost**. Dvosmjerna mrežna raspoloživost između dva aktivna mjerna uređaja može se odrediti slanjem testnih paketa od izvora do prijemnog elementa i nazad. Svaki prispjeli paket definirati će mrežnu raspoloživost, a nepristigli će definirati da mreža nije raspoloživa.

- **Raspoloživost usluge**. Raspoloživost usluge je složena metrika koja nam definira kada je neka usluga moguća između ulazne i izlazne toče u mreži unutar granica SLA definiranih metrika za tu uslugu(npr. kašnjenje, jitter, gubitak,..).

Kvaliteta doživljaja
Aktivni sustavi nadzora uglavnom nemaju mogućnost sagledavanja kako će se izmjerene performanse odraziti na rad pojedine aplikacije. Neki aktivni nadzorni sustavi pokušati će temeljem izmjerenih mrežnih vrijednosti, zaključiti kakve će biti performanse pojedine aplikacije, a samim time i kakva će biti kvaliteta doživljaja rada aplikacije za krajnjeg korisnika tj. "quality of experience" ili QOE. Najčešći način QOE mjerenja je tzv. "mean opinion score" ili MOS, koji nam daje subjektivne vrijednosti QOE za glasovne pozive.

Razmatranja za postavljanje sustava za nadzor mreže

Posebni vanjski mjerni uređaji ili u mrežne elemente ugrađeni mjerni uređaji

Aktivni sustavi nadzora koriste aktivne mjerne elemente za slanje i primanje testnih paketa. Ti aktivni mjerni elementi mogu biti izvedeni kao posebni uređaji ili kao ugrađeni funkcionalni dio nekog pravog mrežnog elementa.

• **Posebni uređaji** (*External agents*). Mogu predstavljati poseban specijalizirani *hardware* ili pak specijalizirano računalo sa mjernim software-om. Ovakvim pristupom odvojili smo mjernu opremu od same prijenosne staze (usmjerivači i switchevi). Mjerna oprema ponaša se kao da je na mrežu spojena od strane korisnika pa ovakav pristup mjerenjima nabliže može

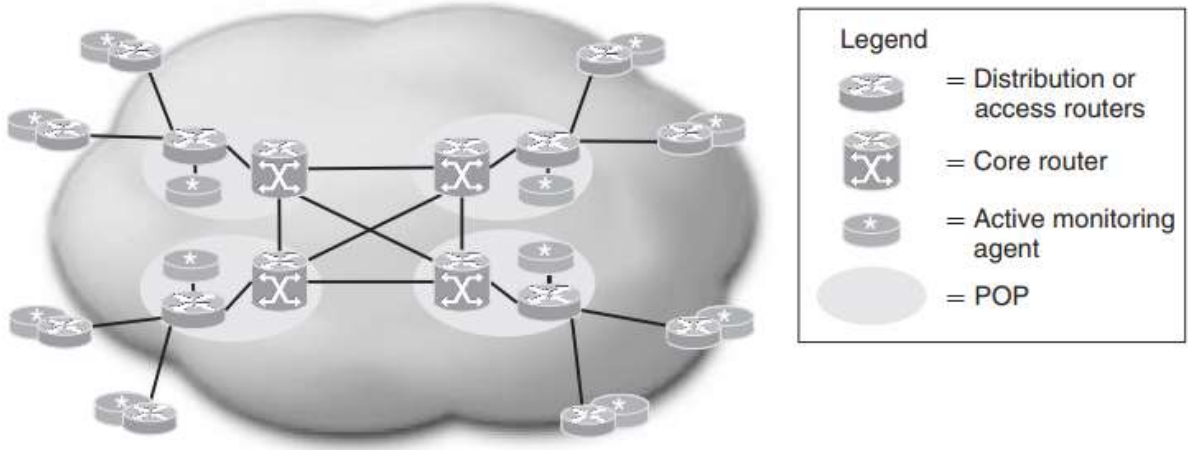
predstaviti korisničko viđenje mreže. Uporaba posebnih uređaja za mjerenja pak zahtjeva kupnju tih samih uređaja, njihov smještaj, napajanje i održavanje – podiže troškove. Za manje urede, korištenje ovakvog načina nadzora nije isplativo

.• **Ugrađeni „agenti“** (*Embedded agents*). Neka mrežna oprema već ima ugrađena programska rješenja za aktivni nadzor mreže. Mrežna oprema sa takvim software-om mogu biti usmjerivači, switchevi ili pak krajnja mrežna oprema poput IP telefona. Uporaba ugrađene funkcionalnosti za aktivna mjerenja na mreži omogućava nam vrlo brz razvoj SLA nadzornog sustava kroz cijelu mrežu, bez potrebe za postavljanjem dodatne opreme.

Topologije sustava za aktivni nadzor mreže

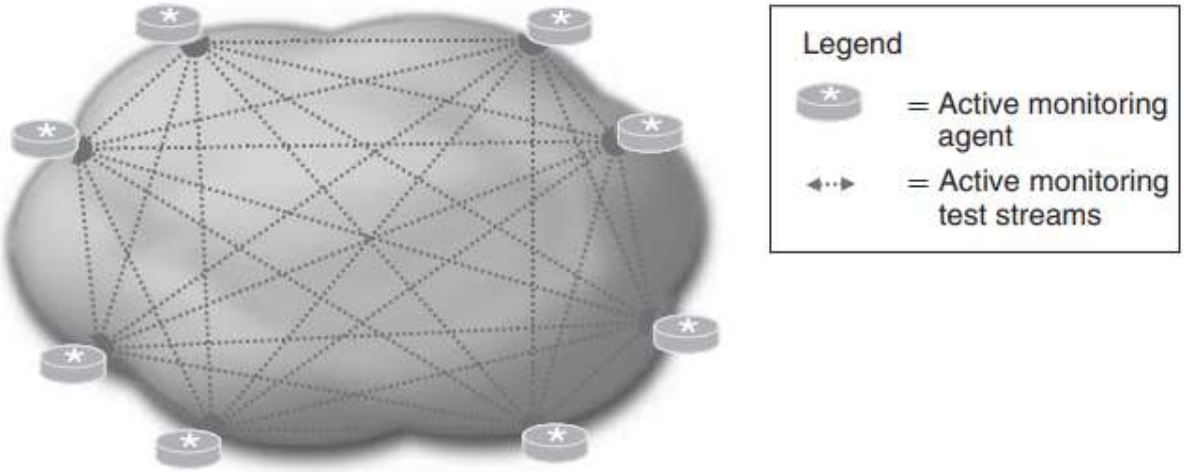
Kod postavljanja aktivnog sustava nadzora glavno pitanje je gdje postaviti aktivne mjerne uređaje(agente). Obzirom da bi kod SLA mjerenja mjerni sustav trebao što bliže opisati kako aplikacije vide mrežne performanse, logično je da bi uređaji trebali biti postavljeni što bliže krajnjim sustavima korisnika. Međutim kod svakog postavljanja uređaja postoje neka ograničenja i odluka o topologiji sustava aktivnog nadzora mreže ovisiti će u tim ograničenjima.

Pogledajmo primjer fizičke mrežne topologije prikazane na slici ispod:



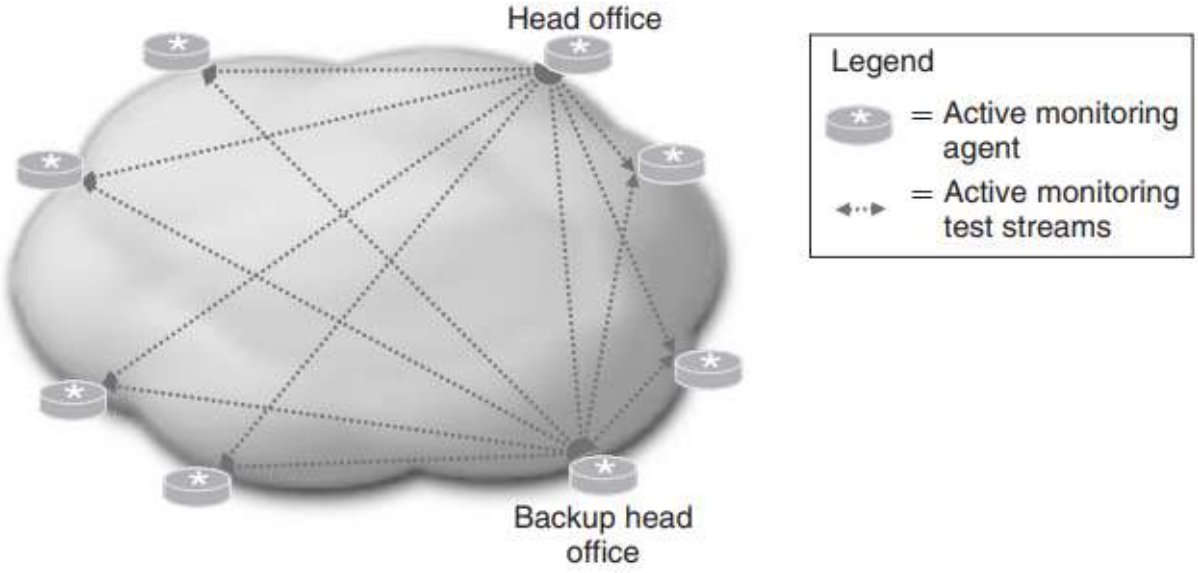
Sve topologije aktivnih SLA nadzornih sustava mogu se svrstati u nekoliko vrsta:

• **Full mesh (svaki sa svakim)**. Mora omogućiti slanje testnih paketa sa svake mjerne točke u svaku drugu mjernu točku, kao što je prikazano na slici ispod.



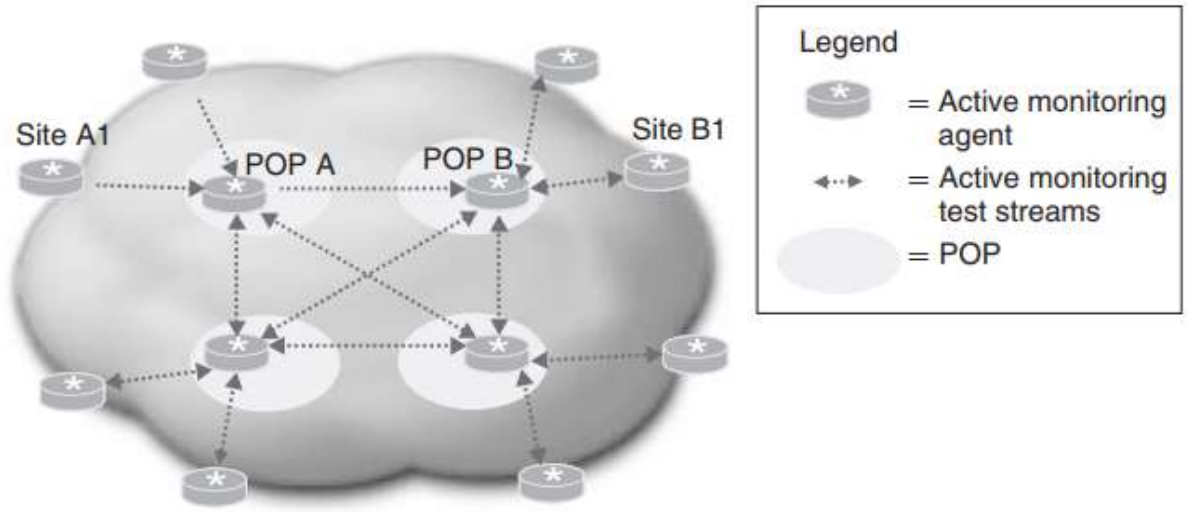
Ovakav pristup je najpreciznij jer mjeri performanse trasa između svih lokacija i pokriva cijelu mrežu. Međutim ovakav način mjerenja ima problem skalabilnosti tj. porastom broja lokacija, naglo nam raste broj trasa koje treba mjeriti n . (n − 1)/2. Za više od samo nekoliko izlaznim mrežnih lokacija, ovakva topologija postaje prekompliciranа za konfiguraciju, a količina prometa testnih paketa postaje tako velika da može izazvati zagušenja pravom mrežnom prometu.

• **Djelomično *mesh* topologija**. Koristi mash testne tokove podataka samo na dijelu topologije. Primjer su Hub & Spoke mreže gdje udaljeni uredi (Spoke) komuniciraju samo sa glavnim uredom (Hub), kao što je prikazano na slici ispod.



Djelomično mash topologija reducira broj testnih tokova. Ukoliko treba aktivno mjeriti RTT, *Hub* lokacije mogu biti konfigurirane kao pošiljatelji aktivnih test paketa dok *Spoke* lokacije djeluju kao primatelji. Na ovaj način sva RTT mjerenja mogu se prikupiti na *Hub* lokaciji.

• **Hijerahijska *mesh* topologija** U mrežana sa komunikacijama svaki-sa-svakim , čisto *mash* tehnologija nije skalabilna, a djelomično *mash* topologija pak ne pokriva nadzorom cijelu mrežu. U ovakvim situacijama može se koristiti takozvana hijerarhijska *mash* topologija. Kod ove topologije, aktivni nadzor mreže je segmentiran. Tipičan način postavljanja je da se uređaji za aktivni nadzor postavljaju centralizirano na svaku lokaciju tzv. point of presence (POP). Aktivni testni tokovi se prema periferiji tj. udaljenim lokacijama organiziraju na *Hub&Spoke* principu, a testni tokovi između POP lokacija rade se po *Mesh* principu. Ovakva topologija prikazana je na slici ispod.



Ovakva topologija najčešće je korištena u praksi jer predstavlja kompromis između skaliranja i vjerodostojnosti mjerenja. POP lokacije konfiguriraju se kao odašiljačke za sve RTT mjerenja, pa za prikupljanje mjerenja nije potrebno obilaziti udaljene lokacije. Nedostatak ovakve topologije je što nam ne omogućava nadzor sa-kraja-nakraj sustava. Ukoliko nam trebaju mjerenja između lokacija A1 i B1, ona moraju biti statistički procjenjena kobinacijom svih segmenata mjerenja na toj trasi (od lokacije A1 do POP A, od POP A do POP B, i od POP B do lokacije B1). Na primjer, moguće je procjeniti prosječno kašnjenje sa-kraja-na-kraj sumiranjem svih kašnjenja po segmentima trase. Za procjenu vjerojatnosti gubitka paketa, ako je vjerojatnost gubitka na segmentu x dana sa Px, onda nam je vjerojatnost gubitka sa-kraja-na-kraj:

$$P = 1 - [(1 - P_1) \times (1 - P_2) \times \ldots \times (1 - P_n)]$$

Međutim, nikako nije moguće procjeniti varijaciju kašnjenja (jitter) sa-kraja-na-kraj pomoću kombinacije mjerenja po segmentima. Ukoliko su nam potrebna jitter mjerenja sa-kraja-na-kraj, potrebno ih je selektivno zasebno napraviti.

Mjerenja *Equal Cost Multiple Paths*

Mnoge mreže imaju višestruke pravce između različitih djelova mreže i to iz razloga otpornosti, ali i iz razloga kapaciteta. IGP protokoli poput OSPF i ISIS određuju koje će se staze koristiti između dvije točke u mreži izračunom staze sa najmanjim *costom.* Ukupni *Cost*

neke staze izračunat je sumiranjem individualnih metrika svake veze na stazi. Ukoliko postoji više staza koje udovoljavaju kriterijima *najmanjeg costa* između dvije točke, tada će IGP protokol moguće distribuirati promet kroz sve staze. Algoritmi za balansiranje prometnog opterećenja uglavnom se nazivaju equal cost multi-path (ECMP) algoritmi i vlasništvo su svakog proizvođača opreme. Različiti proizvođači koristiti će različite kriterije za odluku koja staza će biti korištena za transport određenog paketa iako svi oni kao inpute koriste informacije iz zaglavlja paketa poput IP adrese odredišta, adrese izvora, broja protokola, izvornog i odredišnog UDP/TCP porta. ECMP algoritmi predstavljaju značajan problem za aktivni nadzor mrežnih performansi jer za taj problem nije lako naći rješenje. Za neko mjerenje treba moći koristiti samo jednu stazu, a ne mnogo njih jer inače nam mjerenja nemaju smisla. Postoje razne solucije za rješenje ovog problema, ali niti jedna ne daje rješenje za sve moguće situacije. Npr. naš aktivni mjerni sustav može testnom paketu mjenjati dodjeljenu IP adresu izvora ili IP adresu odredišta, te UDP/TCP brojeve portova, kako bi pokušali poslati pakete svim mogućim stazama. Međutim, ECMP algoritam kao jednu od varijabli za odabir staze koristi i neke nasumične (random) unose, pa nikad nismo sigurni da li su sve moguće staze izmjerene.

Sinhronizacija takta (*Clock Synchronization*)

Kako bi postigli vrlo precizna jednosmjerna mjerenja kašnjenja, staovi (vremenski takt) na svim mrežnim elementima mora biti sinhroniziran. Svaka sinhronizacijska greška direktno unosi tu grešku u mjerenja jednosmjernog kašnjenja. Mrežni elementi održavaju svoju informaciju o točnom vremenu pomoću svoje interne *clock* kartice (*clock board*) koja pruža vremensku informaciju cijelom uređaju. Postoje razni načini za sinhronizaciju takta između razlićitih mrežnih elemenata.

Najprecizniji način sinhronizacije takta na mrežnim uređajima je pomoću vanjskog izvora takta sa „stratum 1“ klase preciznosti poput GPS sata ili radio sata. Ovakav način sinhronizacije je skup, pa može biti prihvatljiv za jezgrene elemente mreže, ali sigurno nije prihvatljiv za sinhronizaciju opreme u perifernim udaljenim uredima.

Alternativni pristup je da se kroz mrežu distribuira „stratum 1“ vrijeme pomoću network time protocol (NTP) [RFC 1305]. NTP sinhronizira satove među uređajima na mreži razmjenim vremenskih poruka (timestamped messages). NTP pokušava postići dugotrajnu preciznost na uštrb kratkotrajne točnosti vremena. Na primjer, on će progresivno ubrzati ili usporiti svoj sat kako bi ga što bliže približio onome što on smatra „točnim vremenom“. Ukoliko se naša aktivna mjerenja performasi obavljaju u tom periodu, mogu se pojaviti vrlo čudni rezultati poput negativnog vremena kašnjenja!

NTP uglavnom održava preciznost točnosti vremena unutar 10ms u WAN mrežama, što generalno nije dovoljna preciznost takta za neka precizna mjerenja poput jednosmjernog vremena kašnjenja za VoIP usluge ili video streaming.

U LAN mrežama, u dobrim uvjetima, NTP može održavati točnost vremena unutar greške od 1ms ili čak i manje, što je dovoljno precizno za sva aktivna mjerenja performansi mreže.

Uzevši u obzir ograničenja i cijene vremenske sinhronizacije, uobičajeni pristup mrežnoj sinhronizaciji vremena je distribucija „stratum 1“ vremenske informacije do svih POP lokacija i to uz pomoć posebne mreže (management network), kako bi se osigurala preciznost od 1ms (ili bolja) korištenjem NTP sinhronizacijskog protokola.
To nam omogućava mjerenja jednosmjernog kašnjenja između POP lokacija. Sinhronizacija pristupnih usmjerivača u udaljenim uredima pomoću NTP protokola nije dovoljno precizna, a dovođenje „stratum 1“ informacije je nemoguće, pa se SLA izvještavanje za pristupne veze vrši pomoću RTT mjerenja, a ne pomoću jednosmjernog kašnjenja.

Zaključak

Telekomunikacijske mreže nisu statične.

Stalno se šire, mjenja se mrežna oprema, promet oscilira, događaju se kvarovi...a samim time mjenjaju se i mrežne performanse. Kako bismo znali kakve performanse pruža neka mreža potrebno je kontinuirano vršiti mjerenja performansi.

Mjerenja na mreži mogu biti aktivna i pasivna.

- Pasivna se sakupljaju na svakom pojedinom mrežnom elementu i u biti mogu nam samo reći kakve performanse ima taj element. Praćenjem performansi svih elemenata mi možemo samo naslutiti mrežne performanse.

- Za pravo mjerenje performansi, pogotovo u svjetlu ispunjavanja SLA zahtjeva, koriste se aktivna mjerenja. Obzirom da ona injektiraju testne pakete u živu mrežu, treba biti vrlo oprezan sa konfiguracijom takvih mjerenja.

- Testni paketi moraju što je više moguće nalikovati na pakete pravog prometa kako bi ih mreža mogla usmjeravati i tretirati na isti način jer jedino tako će nam mjerenja biti vjerodostojna.

- Osobe zadužene za aktivna mjerenja moraju jako dobro vladati znanjem o kreiranju samih mjerenja kao i o tumačenju samih mjernih rezultata.

BIBLIOGRAFIJA

John Evans, Clarence Filsfils: „*Deploying IP and MPLS QOS for Multiservice Networks*“ – Morgan Kaufman Publishers, 2007.

Mirjana D. Stojanović, Vladanka S. Aćimović-Raspopović: “Savremene IP mreže: Arhitekture, tehnologije i protokoli” – Akademska misao, 2012.