Ograničavanje veličine ulaznog toka u čvor paketne mreže ovisno o granicama QoS parametara

Manolić, Kristian

Undergraduate thesis / Završni rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:642252

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-24**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Kristian Manolić

OGRANIČAVANJE VELIČINE ULAZNOG TOKA U ČVOR PAKETNE MREŽE OVISNO O GRANICAMA QOS PARAMETARA

ZAVRŠNI RAD

Zagreb, 2018.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 3. travnja 2018.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Tehnologija telekomunikacijskog prometa I**

ZAVRŠNI ZADATAK br. 4654

Pristupnik: **Kristian Manolić (0135236955)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Ograničavanje veličine ulaznog toka u čvor paketne mreže ovisno o granicama QoS parametara**

Opis zadatka:

Opisati ulogu mrežnih čvorišta u paketnim mrežama kao i osnovne značajke različitih vrsta aplikacija. Analizirati karakteristiöne duljine paketa pojedinih aplikacija i granice parametara za pojedinu vrstu usluge (poput veličine gubitka paketa i kašnjenja). Primijeniti stečeno znanje iz podvorbenih sustava u analizi veličine ulaznog toka u čvorovima paketne mreže i na proizvoljnim problemskim zadacima prezentirati i komentirati dobivene rezultate.

Mentor:

Predsjednik povjerenstva za završni ispit:

dr. sc. Marko Matulin

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

OGRANIČAVANJE VELIČINE ULAZNOG TOKA U ČVOR PAKETNE MREŽE OVISNO O GRANICAMA QOS PARAMETARA

LIMITING PACKET NODE INPUT TRAFFIC FLOWS BASED ON QOS PARAMETERS

Mentor: doc. dr. sc. Marko Matulin

Student: Kristian Manolić

JMBAG:0135236955

Zagreb, rujan 2018.

OGRANIČAVANJE VELIČINE ULAZNOG TOKA U ČVOR PAKETNE MREŽE OVISNO O GRANICAMA QOS PARAMETARA

SAŽETAK

Danas postoji veliki broj različitih tipova aplikacija, te svaka od njih ima specifične zahtjeve za resursima mreže. Da bi se korisniku pružila zadovoljavajuća kvaliteta usluge razvijeni su mnogobrojni mehanizmi i tehnike upravljanja mrežnim resursima, i definirani su parametri kvalitete usluge (*Quality of Service* - QoS) a to su: kašnjenje, varijacija kašnjenja, gubitak paketa i širina propusnog pojasa. Ideja ovog završnog rada je definirati karakteristične duljine paketa i zahtjeve za parametrima QoS-a različitih tipova aplikacija, kako bi mogli ograničiti ulazni tok u čvor paketne mreže. Tipovi aplikacija su govorne, video i aplikacije za prijenos podataka.

KLJUČNE RIJEČI: aplikacija, kvaliteta usluge, kašnjenje, varijacija kašnjenja, gubitak paketa, širina propusnog pojasa, duljina paketa, paketni čvor

SUMMARY

Today there are a large number of different types of applications, each of which has specific network resource requirements. To provide the customer with satisfactory service quality, numerous mechanisms and techniques of network resource management have been developed, and QoS parameters are defined, such as delay, jitter, packet loss and bandwidth. The idea of this paper is to define the characteristic packet lengths and QoS parameter requirements of different types of applications in order to limit the input stream in packet node. Types of applications are voice, video, and data transfer applications.

KEY WORDS: application, Quality of Service (QoS), delay, jitter, packet loss, bandwith, packet size, packet node

Sadržaj

1. Uvod ... 1

2. Uloga paketnih čvorišta ... 3

2.1 Kontrola zagušenja ... 3

2.1.1Mehanizmi kontrole zagušenja ... 4

2.1.2 Tehnike kontrole zagušenja ... 7

2.2 Upravljanje usmjeravanjem ... 8

2.2.1 Fiksno usmjeravanje ... 9

2.2.2 Adaptivno usmjeravanje ... 9

2.3 Kontrola pogreškama ... 10

2.3.1 Detekcija pogreška ... 10

2.3.2 Ispravak pogreške ... 12

3. Značajke aplikacija ... 14

3.1 Govorne Aplikacije ... 14

3.1.1 SIP ... 15

3.1.2 RTP ... 16

3.1.3 Kodeci i Komponente VoIP-a ... 18

3.2 Video aplikacije ... 19

3.2.1 Prijenos videa strujanjem ... 20

3.2.2 Video konferencije ... 22

3.3 Aplikacije za prijenos podataka ... 24

3.3.1 Elektronička pošta ... 24

3.3.2 Usluge pretraživanja informacija ... 24

3.3.3 Dijeljene datoteka ... 25

4. Karakteristične duljine paketa pojedinih aplikacija i granice QoS parametara ... 26

4.1 Kvaliteta usluge (QoS) 26

4.1.1 Kašnjenje 26

4.1.2 Varijacija kašnjenja 27

4.1.3 Šiina pojasa ili propusnost 28

4.1.4 Gubitak paketa 28

4.2 Karakteristične duljine paketa i granice QoS parametra 28

4.2.1 Govorne aplikacije 28

4.2.2 Video aplikacije 30

5. Podvorbeni modeli i matematički izračuna performansi paketne mreže 31

6. Ograničavanje veličine ulaznog toka u čvor paketne mreže uz određeno prometno opterećenje 34

7. Zaključak 37

Popis literature 39

Popis slika 42

Popis tablica 43

1. Uvod

Paketne mreže su prvobitno bile namijenjen samo za prijenos podataka, no njihov ubrzan razvoj i široka primjena ih je učinila pogodnim za distribuciju različitih multimedijskih sadržaja. Iako paketne mreže nisu namijenjene za prijenos u stvarnom vremenu, različiti protokoli kao što je RTP (eng. *Real Time Transfer Protocol*) omogućuju prijenos multimedijskog sadržaja u stvarnom vremenu. Ti protokoli su omogućili razvoj različitih govornih i video aplikacija. Takve aplikacije imaju specifične zahtjeve za parametrima QoS-a (eng. *Quality of Service*) i kapaciteta prijenosnog medija. Govorne i video aplikacije koje se prenose u stvarnom vremenu generiraju veliku količinu prometa. Iz tog razloga potrebno je implementirati različite tehnike i mehanizme kontrole pogreška, usmjeravanja i kontrole zagušenja u čvorovima paketne mreže, kako mreža ne bi došla u stanje zastoja gdje nema isporuke paketa.

Različite vrste multimedijskih aplikacije imaju različite zahtjeve za parametrima QoS-a, a ti parametri su: kašnjenje (eng. *delay*), varijacija kašnjenja (eng. *jitter*), širina pojasa (eng. *bandwith*) i gubitak paketa (eng. *packet loss*). Cilj ovog završnog rada je okarakterizirati različite vrste aplikacija i njihove potrebe za parametrima QoS-a. Rad je strukturiran u sedam poglavalja.

1. Uvod
2. Uloga paketnih čvorišta
3. Značajke aplikacija
4. Karakteristične duljine paketa pojedinih aplikacija i granice QoS parametara
5. Podvorbeni modeli i matematički izračuna performansi paketne mreže
6. Ograničavanje veličine ulaznog toka u čvor paketne mreže uz određeno prometno opterećenje
7. Zaključak.

U drugom poglavlju se opisuje uloga paketnih čvorišta. Njihova uloga je kontrola zagušenja, upravljanje usmjeravanjem i kontrola pogreška. U ovom poglavlju se opisuju razni mehanizmi i tehnike uloga paketnih čvorišta.

U trećem poglavlju se opisuju glavne značajke različitih tipova aplikacija. Te aplikacije su govorne aplikacije, video aplikacije i aplikacije za prijenos podatka. Osim samih

značajki ovih tipova aplikacija bit će još i objašnjeni ključni protokoli i standardi za njihov rad.

U četvrtom poglavlju se opisuju parametri QoS-a. Osim samih parametara također su i prikazane karakteristične duljine paketa različitih aplikacija i njihovih granica parametara QoS-a.

U petom poglavlju se opisuju karakteristike podvorbenih modela. Osim samih karakteristika još su objašnjene formule Markovljevog M/D/1 modela koje su potrebne u šestom poglavlju.

U šestom poglavlju je provedena analiza maksimalne veličine ulaznog toka u čvor koja je napravljena u ovisnosti prosječne duljine paketa i kapacitetu poslužitelja, za definirani parametar maksimalnog prosječnog vremena čekanja u redu. Prosječne duljine paketa definirane su u skladu sa četvrtim poglavljem i analizama provedenim u relevantnim studijama. U analizi svi rezultati su dobiveni primjenom

Zadnje poglavlje je zaključak u kojem su ukratko opisane tehnologije koje se koriste u ograničavanju prometnog toka u čvor paketne prema granicama QoS parametara i rezultati dobiveni u analizi ograničavanja maksimalnog prometnog toka.

2. Uloga paketnih čvorišta

2.1 Kontrola zagušenja

Zagušenje mreže može nastati kada je broj poslanih paketa prema mreži veći od sposobnosti mreže da ih obradi, ili pojavom velikog broja paketa u čvoru ili poveznici što uzrokuje znatan pad kvalitete usluge (eng. *Quality of Service*). Tipične posljedice zagušenja mreže su povećanje broja izgubljenih paketa, dulje vrijeme čekanja i blokiranje stvaranja novih konekcija. Glavni zadatak kontrole zagušenja je održavanje konstantnog broja paketa koji ulaze u mrežu kako bi se zadržala određena kvaliteta usluge i da bi se spriječio kolaps mreže.

Zagušenje utječe na dva parametra performansi mreže, a to su propusnost (eng. *throughput*) i kašnjenje (eng. *delay*). Propusnost se opisuje kao postotak iskorištenosti mrežnih resursa, te se mijenja zavisno o broju paketa i raste linearno. To znači da propusnost raste kada i broj paketa u mreži raste, međutim, ako broj paketa pređe određenu granicu na primjer 60% od ponuđenih mrežnih resursa, tada propusnost počinje padati. Ukoliko broj paketa u mreži nastavi rasti tada dolazi do zastoja (eng. *deadlock*), to je stanje mreže u kojem niti jedan paket nije isporučen na niti jedno odredište. Da bi se spriječio zastoj i kolaps mreže uvedene su tehnike kontrole zagušenja. Međutim, te tehnike smanjuju propusnost u idealnim slučajevima jer se dio resursa mreže koristi za kontrolu zagušenja, [1].

Postoje dvije vrste kontrole zagušenja reaktivna i prediktivna. Reaktivna kontrola zagušenja ublažava zagušenje nakon što ono nastane. To znači da domaćin prati razne parametre koji upućuju na zagušenje mreže (kao što su kašnjenje i gubitak paketa) te kad uoči pad u kvaliteti određenih parametra, počinje primjenjivati tehnike kontrole zagušenja. Protokoli transportnog sloja koji u sebi imaju implementirane algoritme za izbjegavanje zagušenja glavni su primjer reaktivne kontrole zagušenja. Primjer takvog protokola je TCP (eng. *Transmision Control Protocol*) koji je zadužen za kontrolu zagušenja na Internetu jer je IP (*Internet Protocol*) prejednostavan u dizajnu da bi mogao obavljati kontrolu zagušenja. Treba naglasiti da TCP nema mogućnost izbjegavanja zagušenja, već on polagano dovodi mrežu u zagušenja te tada počinje ublaživati nastalo zagušenje. To je posljedica toga što TCP ne zna primjerene brzine prijenosa pa ih mora potražiti negdje drugdje, [1], [2].

Kod prediktivne kontrole zagušenja nužna je takozvana metoda rane detekcije, koja omogućava ruteru i usmjerivaču da saznaju izvor zagušenja prije nego dođe do njega. Ovakva

vrsta upozorenja omogućava da svi izvori prometa prilagode svoje brzine prijenosa prije nego dođe do zagušenja. Ova vrsta kontrole se pokazala efikasnija od reaktivne jer poboljšava performanse TCP-a koji koristi aktivno upravljanje redovima ili skraćeno AQM (eng. *Active Queue Management*), [2].

2.1.1 Mehanizmi kontrole zagušenja

2.1.1.1 Spori početak

Kada pošiljatelj počinje slati pakete u mrežu on inicijalno ne zna koliko paketa može poslati. Da bi pošiljatelj otkrio koliko paketa može poslati koristi takozvani spori početak (eng. *slow start*), kako bi ispitao kapacitet mreže. Spori početak onemogućuje pošiljatelju ili poslužitelju da dovede mrežu u zastoj neposredno nakon što je pošiljatelj/poslužitelj počeo slati pakete u mrežu, te je jedan od ključnih mehanizama koji sprječavaju mrežu da dođe u stanje zagušenja.

Ovaj mehanizam omogućuje da pošiljatelj polagano povećava broj paketa koji šalje u mrežu. Kada pošiljatelj počinje slati pakete inicijalno šalje samo dva paketa prema odredištu. Kada odredište zaprimi pakete, tada ono šalje potvrdnu poruku pošiljatelju da su paketi stigli na odredište. U svakom ciklusu se broj paketa koji pošiljatelj šalje poveća za dva puta, te se taj ciklus nastavlja sve dok pošiljatelj više neće dobiti povratnu poruku. To znači da mreža ili primatelj/odredište nema više raspoloživih resursa da zaprimi nadolazeće pakete, [1].

Negativni efekt ovog mehanizma je povećanje kašnjenja, koje znatno utječe na QoS pojedinih aplikacija. Jedna od najosjetljivijih aplikacija na kašnjenje je prijenos govora koristeći IP (eng. *Voice over Internet Protocol*). Kod takvih aplikacija se najčešće isključuje spori početak kako bi se smanjilo kašnjenje, što bi u budućnosti moglo dovesti do velikih problema jer VoIP aplikacije postaju sve popularnije, [1].

2.1.1.2 Brza retransmisija i brzi oporavak

Brza retransmisija i oporavak su zapravo algoritmi kojima je glavna zadaća smanjiti količinu izgubljenih paketa i posljedično negativan utjecaj na propusnost mreže, te otkloniti greške prije nego istekne retransmisijski tajmer. Kod brze retransmisije se koriste povratne poruke (ACK) prema kojima algoritam prepoznaje je li primatelj primio pakete u pogrešnom redoslijedu, odnosno da nije zaprimio određeni paket. Algoritmi brze retransmisije i brzog

oporavka poboljšavaju performanse TCP-a, zbog toga što nema smanjenja protoka paketa i što su gubici rano detektirani, [1].

Ovi algoritmi koriste dvije metode prema kojima detektiraju zagušenje. Jedna je zaprimanje tri duplikata ACK, a druga se temelji na odstupanju u vremenu odaziva RTT (eng. *Round Trip Time*). Kada izvorište zaprimi tri duplikata ACK-a tada se pokreću algoritmi brze retransmisije i brzog oporavka. Na primjer, pošiljatelj je zaprimio tri ACK-a za peti paket i jedan ACK za sedmi paket, tada pošiljatelj šalje paket broj šest prije nego je istekao tajmer za retransmisiju jer je zaključio da je taj paket izgubljen. Potom se pokreće mehanizam brzog oporavka koji postavlja prag sporog početka na polovicu trenutnog okvira sporog početka. U sljedećem koraku se okvir zagušenja postavlja na prag sporog početka uz još dodatna tri paketa. Ako pošiljatelj nastavi zaprimati duplikate ACK-a svaki put se okvir zagušenja poveća za jedan te se taj određeni paket šalje ponovno. Kada pošiljatelj prestane zaprimati duplikate tada se okvir zagušenja postavlja na prag sporog početka, [3].

Ako nema dovoljno preostalih paketa da se detektiraju duplikati pojedinih paketa odnosno ACK-a tada tajmer prepoznaje zastoj te postavlja prag okvira sporog početka na polovicu trenutnog okvira zagušenja i zatim se širina okvira zagušenja smanjuju na jedan. Na kraju se ponovno pokreće mehanizam sporog početka, [3].

Ovi algoritmi omogućuju konekciji da se brzo oporavi od gubitka pojedinih paketa u prijenosu. Problemi nastaju kada dođe do gubitka više paketa iz određenog niza podataka, što može uzrokovati veliku degradaciju performansi. Uzrok tomu je što algoritmi mogu maksimalno poslati jedan paket za vrijeme pojedinog RTT-a, a širina okvira zagušenja se može smanjiti čak nekoliko puta tokom jednog RTT-a jer se u prijenosu može izgubiti veći broj paketa. To može uzrokovati znatan pad u propusnosti mreže, [3].

2.1.1.3 Nasumična rana detekcija

Nasumična rana detekcija (eng. *Random Early Detection* - RED) je strategija upravljanja redovima koja služi kao podloga za mehanizam izbjegavanja zagušenja. RED je nastao kao zamjena za prijašnju strategiju upravljanja redovima koja je prouzročila neželjeni fenomen globalne sinkronizacije tokova. Kada se međuspremnik popuni, pošiljatelju je potrebno određeno vrijeme da detektira gubitak paketa, a u međuvremenu se međuspremnici i dalje popunjavaju, što uzrokuje gubitak paketa u više tokova. Budući da više izvora detektira gubitak paketa, svi izvori će usporiti istovremeno. To uzrokuje globalnu sinkronizaciju koja

smanjuje iskorištenost mrežnih resursa, jer su svi izvori usporili istovremeno zbog sporog početka što kasnije uzrokuje preplavljivanje redova čekanja zbog toga što su svi tokovi ubrzali istovremeno, [2].

Prednost RED-a je u tome da se može implementirati kao strategija upravljanja međuspremnicima bez ikakvih potrebnih promjena u TCP protokolu. RED, umjesto da čeka preplavljivanje međuspremnika, nasumično odbacuje paket s ciljem odbacivanja paketa iz više tokova u različitim trenucima. To je omogućilo konstantnije brzine prijenosa, što je dovelo do kraćih redova i bolje iskorištenosti mreže.

RED prati prosječnu duljinu reda, zatim se prosječna duljina uspoređuje s pragovima T_{min} i T_{max}. Vjerojatnost odbacivanja se računa pomoću prosječne vjerojatnosti ispuštanja q koja je prikazana. Kod T_{min} nema odbacivanja paketa jer kratki redovi ukazuju da nema zagušenja. Ako prosječna duljina reda prelazi prag T_{max} svi paketi se odbacuju jer to upućuje na ozbiljno zagušenje u mreži. Između granica T_{min} i T_{max} prosječna vjerojatnost ispuštanja q raste linearno do njenog maksimuma p. Realna vjerojatnost ispuštanja računa se prema formuli iz [4]:

$$p_{drop} = \frac{q}{1 - q \cdot broj\ paketa} \tag{1}$$

Broj paketa predstavlja broj paketa koji nisu odbačeni od zadnjeg odbacivanja paketa. Ovim pristupom RED pokušava odbacivati pakete proporcijalno broju konekcija.

RED je doživio komercijalni uspjeh širom svijeta, što je dovelo do razvitka novih inačica RED-a. Jedna od tih inačica je FRED (eng. *Flow Random Early Detection*). FRED je u suštini RED s nekolicinom novih dodatnih mogućnosti. U FRED-u su uvedena dva nova parametra *min* i *max*, te je njihova zadaća odrediti minimalni i maksimalni broj paketa koji se može nalaziti u međuspremniku za svaki pojedini tok. Također FRED prati broj paketa u međuspremnicima za svaki tok u kojem ima paketa u međuspremniku. FRED također penalizira tokove s velikim brojem grešaka na takav način da šalje pakete na tokove koji imaju manji broj grešaka, [2], [4].

Blue je jedna od metoda AQM-a u kojoj je jedna od fundamentalnih promjena ta da se upravljanje redovima obavlja prema gubitku paketa i iskorištenosti pojedine poveznice, a ne prema prosječnim duljinama redova. Blue koristi samo jednu vjerojatnost, a to je *Pm* koja služi za obilježavanje ili odbacivanje paketa iz reda. Ako red konstanto odbacuje pakete zato

što je došlo do preplavljivanja međuspremnika onda Blue povećava vjerojatnost *Pm* te na taj način povećava učestalost slanja poruka o stanju poveznice. Na ovaj način Blue saznaje primjerene brzine slanja. Jedna od najboljih posljedica korištenja Blue-a je omogućavanje kontrole toka s minimalnim veličinama međuspremnika, što u konačnici smanjuje kašnjenje od kraja do kraja i povećava efikasnost iskorištenosti resursa mreže [4]. Prednosti i nedostaci pojedinog AQM-a prikazane su tablicom 1.

Tablica 1: Prednosti i nedostaci AQM-a

AQM	Prednost	Nedostatak
RED	Rana detekcija zagušenja. Ne pravi razlike između tokova. Nema globalne sinkronizacije.	Problem u postavkama parametara. Nedovoljna osjetljivost na povećanje prometa,
FRED	Dobra mjera zaštite kod nepredvidivih tokova.	Problem u postavkama parametara. Nedovoljna osjetljivost na povećanje prometa.
Blue	Pravi razliku između tokova (preferira tokove s manjim brojem grešaka). Smanjuje gubitak paketa i kašnjenje.	Dolazi do problema pri velikom opterećenju.

Izvor: [4]

2.1.2 Tehnike kontrole zagušenja

Tehnike kontrole se mogu svrstati u dvije skupine: otvorene petlje i zatvorene petlje. Otvorene petlje su zapravo protokoli koji služe za izbjegavanje ili prevenciju ulaska mreže ili sustava u stanje zagušenja. Ova kategorija rješenja ili protokola nastoji riješiti problem dobrim dizajnom, kako bi bila sigurna da se zagušenje uopće ne pojavljuje. Jednom kada se sustav ili mreža pusti u rad, nema dodatnih korekcija. Razna pravila ili politike sustava ili mreže odlučuju o tome kada će prihvatiti ili odbaciti promet i odlučuju o raspoređivanju resursa. Glavna karakteristika je da donose odluku bez uzimanja u obzir trenutačno stanje mreže, [1], [2].

Zatvorene petlje su protokoli koji dopuštaju sustavu ili mreži da uđu u stanje zagušenja, potom detektiraju zagušenje, te tek na kraju otklanjaju zagušenje. Tijekom rada mjere se određeni parametri mreže i vraćaju se na dijelove podmreže koja može poduzeti mjere za smanjenje zagušenja. Prema [1] i [2] taj se pristup može podijeliti u tri koraka:,

- Mreža se nadzire kako bi se otkrilo je li zagušena ili ne i na kojim se lokacijama i uređajima pojavljuje zagušenje.
- Potom se te informacije šalju na dio mreže gdje se mogu poduzeti određene mjere.

- Mreža poduzima mjere za otklanjanje zagušenja.

2.2 Upravljanje usmjeravanjem

Upravljane usmjeravanjem (eng. *Routing control*) općenito predstavlja problem pretraživanja mogućih rješenja i izbor rute (smjera) u komutacijskim čvorištima kako bi se zadovoljile potražnje krajnjih korisnika.

Osnovni zadatak je uspostavljanje puteva (fizičkih ili virtualnih) između izvorišta i odredišta, angažirajući raspoložive mrežne resurse na efektivan i efikasan način. To podrazumijeva da komutacijska čvorišta trebaju biti osposobljenja za obavljanje umjeravanja prometa, te imajući na brizi koordinirano upravljanje usmjeravanjem na razini mreže, [5].

Cilj upravljanja usmjeravanjem prometa je optimizirati performanse mreže u danim ograničenjima, pri čemu su ciljevi optimizacije najčešće brzina prijenosa, smanjenje čekanja i pouzdanost. Treba naglasiti da je upravljanje usmjeravanjem implementirano u svakom čvoru paketne mreže i odnosi se na svaki paket koji putuje kroz mrežu, [5].

Iako postoji više shema za klasificiranje, u praksi se najčešće upravljanje usmjeravanjem dijeli na sljedeće tri klase:

- slučajni izbor,
- fiksno usmjeravanje,
- adaptivno usmjeravanje.

Metodom slučajnog izbora selektiraju se smjerovi prema probabilističkim zakonitostima, pri čemu svi smjerovi mogu biti jednako vjerojatni ili se pojedine rute mogu preferirati. Treba naglasiti da ova metoda ne ovisi o informacijama o stanju mreže, već usmjeravanje obavlja samo putem paketnih adresa. Metoda slučajnog izbora nije naišla na široku primjenu u komercijalnim mrežama, već se ona koristi samo u specifičnim paketnim mrežama kao što su vojna, policijska i druge slične mreže, [5].

Fiksno (eng. *Static*) i adaptivno (eng. *Dynamic*) usmjeravanje podrazumijeva da postoje jasno definirane tablice usmjeravanja prema kojima se biraju rute u mreži. Kod fiksnog usmjeravanja tablice usmjeravanja se ne mijenjaju, odnosno korisnik (administrator)

sam definira tablice usmjeravanja, a kod adaptivnog se mogu mijenjati zavisno o vremenu, stanju poveznice ili o stanju mreže, [5].

2.2.1 Fiksno usmjeravanje

Kao što je ranije spomenuto tablice usmjeravanja kod fiksnog usmjeravanja se ne mijenjaju automatski, već korisnik (administrator) mora sam promijeniti tablice usmjeravanja ako dođe do promjene na mreži.

Za svaki par usmjerivača (eng. *router*) postoji definirana ruta prema kojoj se paketi šalju. Usmjerivač prema tim tablicama određuje gdje treba proslijediti paket, odnosno prosljeđuje paket sljedećem čvor na putu. Budući da su tablice usmjeravanja definirane, nema potrebe za korištenjem procesorskih resursa čvora. Što u konačnici smanjuje zahtjeve za širinom propusnog pojasa (eng. *bandwith*), [6].

Metoda fiksnog usmjeravanja se koristi u okruženjima gdje je promet mreže predvidljiv te nema učestalih promjena u topologiji mreže. Ova metoda se ne koristiti u mrežama koje su sklone učestalim promjena i velikim količinama prometa. Prednosti i nedostaci fiksnog usmjeravanja prikazane su tablicom 2. Danas većina mreža u suštini koristi dinamičko usmjeravanje za komunikaciju između usmjerivača, jedino se u specifičnim slučajevima koriste jedan ili dva statička usmjerivača za neželjeni promet koji dolazi na mrežu, [6], [7].

Tablica 2: Prednosti i nedostaci fiksnog usmjeravanja

Prednosti	Nedostaci
Malo korištenje procesorskih i memorijskih resursa. Mali zahtjevi za *bandwithom*. Jedinstvena kontrola prometa kroz mrežu.	Kod svake promjena infrastrukture, promjene se moraju ručno uvesti u tablice. Nema tolerancije na pogreške ako dođe do kvara na mreži ili poveznici. Nepraktično za velike mreže.

Izvor: [7]

2.2.2 Adaptivno usmjeravanje

Kod adaptivnog usmjeravanja tablice usmjeravanja su definirane protokolima usmjeravanja kao što su RIP (eng. *Routing Information Protocol*), EIGRP (eng. *Enhanced Interior Gateway Routing Protocol*), i OSPF (eng. *Open Shortest Path First*). Ovim protokolima omogućeno je raspoređivanje prometa na alternativne puteve zavisno o stanju mreže. Prema [7] glavni parametri prema kojima se bira najbolji put su:

- kašnjenje,
- propusnost ili raspoloživost,
- troškovi, i
- posebni zahtjevi.

Budući da usmjerivači dijele tablice usmjeravanja među sobom, kao posljedicu toga uzrokuju povećanje korištenja procesorskih i memorijskih resursa kao i širine propusnog pojasa. Zbog toga čitava mreža može postati upravljački osjetljiva i nestabilna kod većih opterećenja. Prednosti i nedostaci adaptivnog usmjeravanja prikazane su tablicom 3. Koncept adaptivnog usmjeravanja je primijenjen u Internetu jer omogućuje usmjeravanje uzimajući u obzir promjenu u topologiji mreže i promjene u prometnom opterećenju, [5], [7].

Tablica 3: Prednosti i nedostaci adaptivnog usmjeravanja

Prednosti	Nedostaci
Bolja implementacija u većim mrežama. Automatski bira zamjensku rutu u slučaju ispadanja poveznice.	Povećanje korištenja *bandwitha* zbog razmjene tablica usmjeravanja među čvorovima. Povećanje korištenja procesorskih i memorijskih resursa mreže. Protokoli usmjeravanja biraju najbolji put, a ne mreža.

Izvor: [7]

2.3 Kontrola pogrešaka

Prilikom slanja svakog paketa može doći do pogreške u prijenosu zbog nastalih smetnji u prijenosu, što uzrokuje da neki bitovi promjene svoje vrijednosti. Kontrola pogrešaka omogućuje primatelju da javi pošiljatelju da je došlo do pogreške u prijenosu te da pošalje zahtjev za retransmisiju određenog paketa. Kontrola pogrešaka se može podijeliti u dvije kategorije:

- detekcija pogreške, i
- ispravak pogreške.

2.3.1 Detekcija pogreška

Detekcija pogreška omogućuje primatelju da ustanovi da li je došlo do pogreške u prijenosu. Postoje tri osnovna načina detekcije pogreška:

- provjera pariteta,
- ciklička provjera redundantnosti (eng. *Cyclic Redundancy Check*-CRC), i

- provjera sume (eng. *Checksum*)

Provjera pariteta je najjednostavniji način detekcije pogreška. Njezina karakteristika je da se dodaje bit pariteta na kraju niza podataka. Bit pariteta poprima vrijednost zavisno o tome radi li se o parnom paritetu (paran broj jedinica u nizu) ili neparnom paritetu (neparan broj jedinica u nizu). Primjer parnog pariteta i neparnog pariteta prikazan je tablicom 4, [8].

Tablica 4: Primjer provjere pariteta

Niz od sedam bitova	Niz sa parnim paritetom	Niz sa neparnim paritetom
0100100	01001000	01001001
0100000	01000001	01000000

Ako pošiljatelj koristi paran paritet za slanje niza na primjer kao što je 0101100 onda će na kraju niza dodati bit pariteta vrijednosti 1 i poslat će niz 01011001. Primatelj zaprima i obrađuje niz, te ako je broj jedinica u nizu paran on zaključuje da nije došlo do pogreške u prijenosu. Ako dođe do greške u prijenosu i broj jedinica više nije paran, onda primatelj detektira pogrešku. Treba naglasiti da ako dođe do pogreška u prijenosu na dva (ili bilo kojem parnom broju) mjesta odnosno bitova neće se detektirati pogreška. Parni paritet se najčešće koristi u sinkronom prijenosu, a neparni u asinkronom prijenosu.

Kodovi cikličke provjere redundantnosti se dijele na bitove koje pošiljatelj želi prijenos i obično se označavaju s D. Prvo se pošiljatelj i prijemnik moraju dogovoriti o r + 1 bitnom uzorku, poznatijem kao generator, koji se obično označava s G. Za određeni dio podataka D, pošiljatelj će odabrati dodatne bitove R i dodati ih u D tako da se dobiveni d + r bitni uzorak (tumači kao binarni broj) bude točno djeljiv s G. Proces provjere pogrešaka s CRC-om je vrlo jednostavan i odvija se na sljedeći način: prijamnik dijeli d + r primljene bitove s G, ako ostatak nije nula prijemnik zna da je došlo do pogreške, inače se podaci prihvaćaju kao ispravni, [8].

Provjera sume se koristi za provjeru integriteta podataka odnosno je li došlo do pogreške u prijenosu ili je li netko promijenio podatke. Provjera sume se može izvesti na više drugačijih načina i algoritama. Najjednostavnija metoda *Checksuma* je slanje brojeva i njihove sume na odredište kako bi se otkrilo je li došlo do pogreške u prijenosu. Budući da je ova metoda vrlo jednostavna i nepouzdana ona se u praksi ne koristi, već se koriste razne kriptografske *hash* funkcije i već ranije spomenuti CRC, [8], [9].

U Internet mreži se koristi 16 bitna provjera sume, te se na strani pošiljatelja poduzimaju sljedeći koraci:

1. Poruka se dijeli na 16 bitne riječi.
2. Vrijednost *checksuma* se postavlja u nulu.
3. Sve riječi se komplimentiraju uključujući *i checksum*.
4. Kada se komplementacija izvrši ta vrijednost postaje *checksum*.
5. *Checksum* se šalje s podacima.

Na strani primaoca se poduzimaju sljedeći koraci kako bi se ustanovila pogreška u prijenosu:

1. Poruka se dijeli na 16 bitne riječi (uključujući i *checksum*).
2. Sve riječi se zbrajaju korištenjem jednog komplementa.
3. Kada se komplementacija izvrši ta vrijednost postaje *checksum*.
4. Ako je vrijednost *checksuma* nula, poruka se prihvaća, u suprotnom slučaju se poruka odbacuje.

2.3.2 Ispravak pogreške

Ispravak pogreške omogućuje primatelju da otkloni grešku koja je nastala u prijenosu. Dva osnovna načina otklanjanja pogreške su:

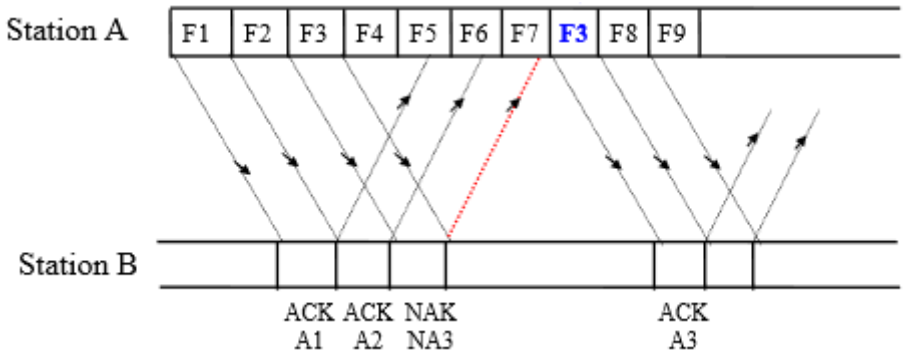
- retransmisija, i
- FEC (eng. *Forward Error Correction*).

Za ispravak pogreške pomoću retransmisije najčešće se koriste ARQ (eng. *Automatic Repeat Request*) protokoli. ARQ radi na sljedećem principu: prvo primatelj detektira pogrešku u poruci te zatim šalje ARQ poruku. Kada pošiljatelj zaprimi ARQ poruku, on počine ponovno slati poruku. Taj proces se ponavlja sve dok poruka nije pravilno isporučena ili dok broj ponovno poslanih poruka ne pređe broj predodređenih retransmisija. Postoji više tipova ARQ protokola a neki od njih su: stani-i-čekaj (eng. *Stop-and-wait*) ARQ i selektivna retransmisija (eng. *Selective Repeat*), [8], [10].

Stani-i-čekaj ARQ protokol je u suštini vrlo sličan brzoj retransmisiji. Razlika je u tome što se u ovom protokolu ne čekaju tri duplikata ACK, već je uvedena nova vrsta ACK-a koja zamjenjuje duplikate, a to je NACK (negativni ACK). Princip rada je u suštini isti, samo pošiljatelj šalje svaki paket pojedinačno, a zatim čeka odgovor primaoca. Kada pošiljatelj zaprimi ACK od primaoca, tek tada se šalje sljedeći paket, u suprotnom slučaju (zaprimljeni

NACK) ponovno se šalje isti paket. U slučaju gubitka paketa, paket se ponovno šalje kada istekne tajmer za retransmisiju. Prednost ovog protokola je njegova jednostavnost i mogućnost implementacije s minimalnim veličinama međuspremnika, no kao posljedicu uzrokuje neefikasno korištenje resursa mreže, [10].

Selektivna retransmisija je najefektivniji protokol ARQ-a. Ona šalje pakete samo u slučajevima kada zaprimi NACK ili istekne tajmer za retransmisiju. Treba naglasiti da ovaj protokol zahtijeva kompleksniju izvedbu pošiljatelja, jer mora imati mogućnost slanja paketa van predviđenog niza, kako je prikazano slikom 1. Također primalac mora imati dovoljno slobodnih memorijskih kapaciteta međuspremnika da pohrani sve pakete koji su zaprimljeni nakon paketa za koji je poslan NACK, kao i dovoljno procesorske snage da ponovno posloži pakete u odgovarajući redoslijed, [10].



Slika 1: Primjer ponovnog slanja paketa, [10]

FEC je metoda koja služi za ispravak pogreške nastale slanjem paketa kroz mrežu. Glavna značajka FEC je da dodaje redundantnost podacima koristeći specifične algoritme. Redundantni bitovi su kompleksne funkcije originalnih informacijskih bitova. Svaki bit se šalje više puta jer do pogreške može doći na bilo kojem uzorku slanja. Izvorni podaci mogu se pojaviti u kodiranom obliku na izlazu. Kodovi koji uključuju neizmijenjeni ulazni niz u izlaznom kodu nazivaju se sistemski, a oni koji ne uključuju nazivaju se nesistemski, [8].

3. Značajke aplikacija

Prvobitno su paketne mreže bile namijenjene samo za prijenos podataka i tekstualnih poruka, što je dovelo do razvoja aplikacija za prijenos podatka. Kako su se razvijale razne nove tehnologije prijenosa, paketne mreže su polagano postojale sve prilagodljivije za prijenos različitih multimedijskih sadržaja. Razvojem novih protokola kao što su SIP (eng. *Session Iniciation Protocol*) i RTP (eng. *Real Time Transfer Protocol*), omogućio je razvoj govornih i video aplikacija.

3.1 Govorne aplikacije

Govorne aplikacije mogu se definirati kao prijenos govora korištenjem IP protokola, koji je poznatiji kao VoIP. Za razliku od tradicionalnog prijenosa govora u telefonskim mrežama, koje za vrijeme komunikacije zahtijevaju cijeli resurs kanala, VoIP za prijenos govora koristi pakete. U paketnim mrežama se informacija (govor) dijeli u više paketa koji se šalju prema odredištu koristeći više puteva. Prema [11] glavne funkcije VoIP su:

- Signalizacija - to je način na koji uređaji komuniciraju unutar mreže, aktivirajući i koordinirajući različite komponente potrebne za uspostavljanje poziva.
- Usluge baza podataka - način su za pronalaženje krajnjih točaka i prevođenje adresa koje koriste dvije mreže.
- Uspostavljanje i raskidanje razgovora - poziva se uspostavlja između dvije krajnje točke koje započinju sesiju jedna između druge.
- Operacije utemeljene na kodecima – ove operacije omogućuju da glas iz analognog oblika pretvore u digitalni oblik kako bi prijenos putem IP mreže bio moguć.

VoIP aplikacije definirane su nizom protokola koji su zaduženi za razne zadaće kao što su signalizaciju i uspostavu poziva i prijenos podatak u stvarnom vremenu.

Glavna zadaća protokola za signalizaciju i uspostavu poziva, je da strankama omogući uspostavu poziva na njihov zahtjev. Postoji više protokola ove kategorije no glavni predstavnici i najčešće korišteni su H.323 i SIP. Oba protokola su namjena za komunikaciju od kraja-do-kraja. H.323 sam po sebi nije protokol već on daje upute kako koristiti ostale protokole i razvijen je primarno za klasični prijenos govora i video konferencije na lokalnim mrežama (eng. *Local Area Network* - LAN). SIP je razvijen isključivo za IP mreže i koristi se u nizu različitih aplikacija kao što su prijenos videa na zahtjev, prijenos govora, audio sadržaja i online video igre, [11].

Protokol zadužen za prijenos podataka u stvarnom vremenu je RTP. RTP sesije za prijenos videokonferencija i multimedijskog sadržaja, u pravilu koriste SIP za uspostavljanje sesije. Za prijenos RTP koristi UDP (eng. *User Datagram Protocol*) protokol, osim u slučajevima prijenosa putem strujanja kada se koristi TCP protokol.

3.1.1 SIP

SIP je signalizacijski protokol koji se koristi za uspostavljanje, prijenos i raskidanje multimedijskih sesije na IP mrežama. SIP je dizajniran na temelju HTTP (eng. *Hyper Text Transport Protocol*), od kojeg je preuzeo sintaksu i metodu tekstualnog kodiranja. SIP je protokol koji zahtjeva odgovor, što znači da zahtjeva poslužitelja, i čeka odgovor klijenta. Nakon što se uspostavi sesija, drugi protokoli obavljaju pregovaranje o vrsti medija (audio, video, itd.) koji će se razmjenjivati i način na koji će ga slati između krajnjih točaka. SIP korištenjem postojećih protokola i njihovih funkcija omogućuje manje korištenje resursa mreže i smanjuje složenost SIP-a, [12].

SIP je standardiziran za niz protokola transportnog sloja kao što su TCP i UDP. U slučaju kada se koristi prijenos preko nepouzdanog transportnog protokola kao što je UDP, SIP ima svoje ugrađene mehanizme i tajmere za retransmisiju kako bi povećao pouzdanost. Kada se koristi prijenos preko pouzdanog transportnog protokola kao što je TCP, onda se ti ugrađeni mehanizmi ne koriste.

Prvotno je SIP razvijen kako bi podržao pet specifičnih zahtijeva za uspostavljanje i raskidanje multimedijskih sesija. Tih pet zahtjeva su:

- Lokacija korisnika, gdje se može identificirati krajnja točka sesije, kako bi se uspostavila sesija.
- Dostupnost korisnika, gdje sudionik koji se zove ima sposobnost odlučiti želi li on sudjelovati u komunikaciji.
- Korisničke mogućnosti, dogovor između korisnika oko vrste i parametara medija koji će se koristiti u komunikaciji.
- Uspostavljanje sesije, dogovor između korisnika oko parametara sesije.
- Upravljanje sesijom, brine o: mijenjanju parametra sesije, prijenosu podataka, pozivanju određenih usluga i raskidanju sesija.

SIP ne bi mogao funkcionirati na mreži bez uporabe raznih uređaja i protokola. Glavni uređaji su oni koji omogućuju sudionicima da međusobno komuniciraju. U nekim slučajevima može biti potreban niz različitih poslužitelja, koji su potrebni da korisnici uspostave sesiju među sobom. Kako bi se omogućila komunikacija između korisnika potrebne su dvije ključne komponente SIP-a, korisnički agenti i SIP poslužitelj, [12], [13].

Korisnički agenti su u stvari oba računala koja su potrebna za uspostavljane poziva i zaprimanje poziva. Oni čine dvije krajnje točke komunikacije u sesiji. U korisničkim agentima postoje dvije komponente: klijent i poslužitelj. Kada korisnički agent podnese zahtjev (kao što je pokretanje sesije), to je korisnički agent klijenta (eng. *User Agent Client*) ili skraćeno UAC, a korisnički agent koji reagira na zahtjev je korisnički agent poslužitelja (eng. *User Agent Server*) ili skraćeno UAS. Budući da će korisnički agent prvo poslati poruku, a zatim će odgovoriti na povratnu poruku, onda će se korisnički agent izmjenjivati uloge tijekom cijele sesije, [13].

SIP poslužitelj se koristi za pridjeljivanje korisničkih imena odgovarajućim IP adresama, tako da zahtjevi poslan od jednog korisničkog agenta prema drugom može biti pravilno usmjeren. Korisnički agent registrira se na SIP poslužitelja, pružajući mu svoje korisničko ime i trenutnu IP adresu, čime se utvrđuju njegova trenutna lokacija na mreži. To također potvrđuje da su prisutni na mreži, tako da drugi korisnički agenti mogu vidjeti da su prisutni i slobodni za razgovor, što im omogućuje da ih na taj način pozovu u sesiju. Budući da vjerojatno korisnički agent ne zna IP adresu drugog korisničkog agenta, zahtjev je upućen SIP poslužitelju za pozivanje drugog korisnika u sesiju. SIP poslužitelj zatim identificira je li osoba trenutno na mreži, te ako je, uspoređuje korisničko ime s njegovom IP adresom kako bi se odredila njegova lokacija. Ako korisnik nije dio iste domene, što znači da koristi drugog SIP poslužitelja, onda će također prosljeđivati zahtjeve ostalim poslužiteljima, [13].

3.1.2 RTP

Cilj RTP-a je osigurati jedinstven način prijenosa podataka različitih medija (audio, video, itd.) u stvarnom vremenu na IP mrežama. Glavna uloga RTP-a je implementacija slijednih brojeva IP paketa za glasovne ili video informacije, da omogući odredištu da posloži IP pakete u odgovarajući redoslijed, ako je došlo do pogreške u prijenosu. Prema [12] RTP omogućuje:

- identifikaciju tipa informacije koja se prijenosi,

- dodavanje slijednog broja informaciji koju prenosi, i
- praćenje paketa koji putuje prema odredištu.

RTP tokovi su jednosmjerni i sadrže samo jedan tip medija. Svaki RTP tok se obično prima na drugom kanalu. Na primjer, dvosmjerna audio i video sesija zapravo su četiri različite RTP sesije. RTP također definira kontrolni protokol, RTP kontrolni protokol ili skraćeno RTCP (eng. RTP *Control Protocol*).

RTCP je dizajniran da efikasno koristi širinu propusnog pojasa, i da se na pravilan i odgovarajući način prilagođava različitim tipovima sesija (*unicast* i *multicast*). Otkrivanjem broja sudionika u jednoj sesiji, RTCP osigurava da promet ne prelazi 5% ukupne širine propusnog pojasa RTP medija, te da je ta širina propusnog pojasa jednako podijeljena među sudionicima u sesiji, [11].

RTP koristi 32 bitno zaglavlje za povećanje učinkovitost u prijenosu i služi kao spremnik za različite tipove medija. RTP zaglavlje prikazano je slikom 2. Zaglavlje u sebi sadržava informacije o sinkronizaciji i slijednim brojevima, kao i sve ostale informacije koje su potrebe da primatelj može reproducirati poslani medij. Osim toga, RTP zaglavlje dopušta primatelju RTP-a da postane svjestan mogućih pogreška uzrokovanih prijenosom preko IP mreže, kao što su, [14]:

- gubitak paketa,
- jitter ili varijacija kašnjenja, i
- Nepravilan dolazak paketa na odredište (slijedni broj).

V=2	P	X	CC	M	Sequence number
Timestamp					
Identification of the synchronization source (SSRC)					
Identification of the contribution source (CSRC)					

Slika 2: Prikaz RTP zaglavlja, [14]

Značenje sljedećih polja je ovdje objašnjeno:

- V - Oznaka verzije protokola duljine 2 bita
- P – Polje za ispune duljine 1 bita, u slučaju da je P=1 to znači da paket sadrži dodatne informacije od prethodnog paketa

- X – Polje dodatak duljine 1 bita, ako je X=1 onda je iza zaglavlja paket dodatka
- CC- brojač CSRC-a duljine 4 bita – označava broj CSRC-a koji slijede iza zaglavlja
- M- Polje oznake duljine 1 bita - definirano je profilom aplikacije
- PT- Oznaka vrste medija duljine 7 bita – definira vrstu medija koja se prenosi (audio, video, itd.)
- *Sequence number* (slijedni broj) duljine 16 bita- polje u kojem je zapisani slijedni broj (prvi broj je dodijeljen nasumično, a za svaki sljedeći paket se vrijednost polja poveća za jedan)
- *Timestamp* (oznaka vremena) duljine 32 bita- Označava trenutak kada je prvi bajt RTP paketa zapisan. Ovaj trenutak mora biti preuzet iz sata koji se povećava na monoton i linearan način ovisno o vremenu kako bi omogućio usklađivanje i izračunavanje jittera na odredištu.
- SSRC polje duljine 32 bita – jednoznačno označava izvor i nasumično je dodijeljeno od strane aplikacije. SSRC identificira sinkronizirani izvor. Ovaj identifikator odabire se nasumično s namjerom da je jedinstven među svim izvorima iste sesije. Popis CSRC identificira izvore SSRC-a koji su pridonijeli dobivanju podataka sadržanih u paketu koji sadrže taj identifikatora. Broj identifikatora je dan u polju CC.
- CSRC polje duljine 32 bita – identificira izvore koji su pridonijeli dobivanju podataka sadržanih u paket.

3.1.3 Kodeci i komponente VoIP-a

Glavan zadaća kodeka je izvršiti paketizaciju glasa u pakete. Proces pretvaranja analognih valova u digitalnu informaciju obavlja se pomoću kodera i dekoderom (CODEC). Postoji mnogo standarda koji opisuju procese transformacije analognog glasovnog signal u digitalni oblik. Proces pretvorbe je vrlo složen, te se većina pretvorbi temelji na pulsno kodiranoj modulaciji PCM (eng. *Pulse-code modulation*) ili nekim drugim vrstama modulacije. Treba naglasiti da za svaki standard ima propisane zahtjeve za širinom propusnog pojasa. Lista CODEC-a je prikazana tablicom 5, [15].

Tablica 5: Karakteristike CODEC-a

ITU standard	Modulacijska tehnika	Bandwith (kb/s)	Kašnjenje (ms)
G.711	PCM	64	<1.00
G.721	ADPCM	16,24,32,40	<1.00
G.728	LD-CELP	16	~2.50
G.729	CS-ACELP	8	~15.00
G.723.1	CELP	6.3,5.3	~30.00

Izvor:[15]

Izlaz iz CODEC-a je tok podataka koji se stavlja u IP pakete i prenosi se preko IP mreže na krajnju točku. Te krajnje točke moraju koristiti identične standarde, kao i skup parametara CODEC-a. Ako dvije krajnje točke koriste različite standarde ili parametre onda će komunikacija u tom slučaju biti nerazumljiva.

Iako su VoIP komponente po svojim funkcionalnostima vrlo su slične komponentama u klasičnoj telefoniji, samo što koriste drugačiji pristup. Jedina bitna razlika je u tome što VoIP zahtjeva postojanje *gateway*-a, a četiri glavne komponente VoIP-a su, [11]:

- Poslužitelj za obradu poziva – poznatiji kao IP PBX je poslužitelj koji se bavi kontrolom svih VoIP konekcija koje su uspostavljene. Ova komponenta je obično softwareski implementirana, no može biti razvijen kao dio neke platforme ili specifičnog uređaja.
- Korisnički terminali odnosno uređaji – svi VoIP telefoni ili sva korisnička oprema koja može podržati VoIP aplikacije.
- Medijski ili VoIP *gateway* – glavna uloga ovih *gateway*-a je pretvorba signala iz analognog u digitalni oblik (kao i iz digitalnog u analogni) i stvaranje VoIP paketa. Također mogu imati niz dodatnih mogućnosti kao što su: otklanjanje jeke, kompresija glasa, pri gušenje buke, i druge slične funkcije.
- IP mreža – bez koje prijenos paketa od kraja do kraja ne bi bio moguć.

3.2 Video aplikacije

Video aplikacije su aplikacije koje koriste paketnu mrežu kako bi pružile korisniku usluge video prijenosa. Usluge se korisniku mogu pružiti na njegov zahtjev, ili mogu biti prenesene u stvarnom vremenu. Glavni transportni protokoli u ovim aplikacijama su TCP i UDP, dok aplikacije koje prenose sadržaj u stvarnom vremenu koriste RTP.

Budući da su video signali dosta veliki koriste se razni standardi kompresije, to jest razni video kodeki koji pretvaraju video signal u digitalni oblik, te potom te podatke enkapsuliraju u niz IP paketa različitih veličina. Prema [16] pet glavnih karakteristika video aplikacija su:

- Prijenos video signala odvija se pomoću različitih aplikacija, što omogućuje lakše dohvaćanje resursa mreže.
- Aplikacije nisu ograničene duljinom prijenosa, odnosno udaljenošću između izvorišta i odredišta.
- Smanjenje troškova jer se za prijenos koristi već izgrađena infrastruktura (bakrene parice, optički kablovi) pa nema potrebe za ulaganjem u infrastrukturu.
- Smanjenje troška električne energije jer postoje sustavi koji pružaju energiju preko Etherneta (*Power-over-Ethernet*).
- Koristi manji *bandwith* za kompresiju, slanje i pohranjivanje.

Dva tipa video aplikacija su prijenos videa strujanjem (eng. *streaming video)* i video konferencije.

3.2.1 Prijenos videa strujanjem

Prijenos videa strujanjem je proces isporuke video sadržaja korisniku koji se potom odmah reproducira na njegovom uređaju. Ovo je često prvi tip aplikacija na koju ljudi pomisle kada se govori o prijenosu videozapisa preko IP mreža. Osim vrlo popularnih aplikacija za zabavu, ovaj tip aplikacija može se koristiti u niz različitih svrha, kao što su: poslovne svrhe, komunikacijske svrhe, u svrhu obuke i obrazovanja, itd. U prijenosu videozapisa putem strujanja postoji veliki broj tehnologija, a prema [16] najčešće korištene tehnologije su:

- Čisto strujanje (eng. *True streaming*) - gdje se videozapis prenosi i reproducira u stvarnom vremenu.
- Preuzimanje i reprodukcija – gdje se kompresirani videozapis prvo cijeli preuzme na odredište te se tek onda reproducira.
- Progresivno preuzimanje i reprodukcija – ova tehnologija se može opisati kao kombinacija prethodne dviju metoda.

3.2.1.1 Čisto strujanje

Čisto strujanje preko IP mreže započinje uzimanjem digitalnog videozapisa signala, te ga potom dijeli u IP pakete koje šalje na IP mrežu. Video signal može biti nekomprimiran, ali općenito kada se govori o prijenosu putem strujanja, video sadržaj je komprimiran pomoću nekog video kodeka, jer nekomprimirani video signal zauzima velike količine *bandwitha*.

Da bi strujanje ispravno funkcioniralo, video sadržaj treba stići na odredište točno kada je to potrebno, što u praksi nije jednostavno postići, jer mnogi čimbenici mogu utjecati na pravodobnu isporuku videozapisa. Zbog toga mreža mora biti sposoban isporučiti sadržaj korisniku bez gubitka paketa i bez drastičnih promjena u vremenima kašnjenja, jer to znatno utječe na korisnički doživljaj i kvalitetu usluge. Prednosti i nedostaci čistog strujanja su prikazane tablicom 6, [16].

Tablica 6: Prednosti i nedostaci čistog strujanja

Prednosti	Nedostaci
Sadržaj se prenosi na korisnički zahtjev. Nema pohrane videozapisa na korisnički uređaj. Pogodan za prijenos uživo.	Razlika u kvaliteti mreže između više izvora strujanja može znatno degradirati kvalitetu video signala. Nema retransmisije paketa.

Izvor:[16]

Strujanje je uspješno implementirano na različitim mrežnim tehnologijama, od *dial-up* tehnologija do širokopojasnih tehnologija pristupnih mreža. Jedini uvjet je da je dostupna propusnost mreže bude veća ili jednaka brzini slanja podataka, [16].

3.2.1.2 Preuzimanje i reprodukcija

Preuzimanje i reprodukcija preuzima datoteku video sadržaja na korisnički uređaj, gdje se video sadržaj dekodira i reproducira. Ovaj tehnologija je vrlo slična procesu koji koriste web stranice. Preuzimanje i reprodukcija upotrebljavaju iste protokole kao i normalan web, a ti protokoli su: HTTP, FTP (eng. *File Transfer Protocol*) i TCP. Video i audio sadržaji mogu biti pohranjeni na standardnim web poslužiteljima kada se koristi preuzimanje i reprodukcija. Protokoli i postupci potrebni za slanje sadržaja gledatelju isti su kao i za jednostavne stranice HTML (eng. *Hypertext Markup Language*) teksta, [16].

Jedna od glavnih prednosti preuzimanja i reprodukcije je da to može raditi preko bilo koje brzinske mrežne veze. To je moguće jer ne postoje ograničenje na kašnjenje paketa i paketi ne moraju dolaziti na odredište u određenom nizu, jer se prvo sav sadržaj preuzme te se

tek onda reproducira. Prednosti i nedostaci preuzimanja i reproduciranja prikazane su tablicom 7.

Tablica 7: prednosti i nedostaci preuzimanja i reprodukcije

Prednosti	Nedostaci
Moguće korištenje FTP i HTTP protokola za preuzimanje video sadržaja. Ako dođe do gubitka paketa aktivira se TCP-ov mehanizam za retransmisiju.	Svaka promjena u vremenu kašnjenja može aktivirati TCP-ov mehanizam za kontrolu toka što može znatno smanjiti brzine prijenosa. Da bi preuzimanje bilo uspješno potrebni su zadovoljavajući kapaciteti memorije za pohranu podataka.

Izvor: [16]

3.2.1.3 Progresivno preuzimanje i reprodukcija

Progresivno preuzimanje i reprodukcija je inačica preuzimanja i reprodukcija. Koristi se za oponašanje strujanja za aplikacije u kojima prijenos strujanjem neće ispravno funkcionirati. Progresivno preuzimanje i reprodukcija preuzima video sadržaj i dijeli ga u manje segmente, te se svaki šalje prema odredištu. Čim se segment potpuno preuzme, odgovarajući software za reprodukciju može početi obrađivati i reproducirati video sadržaj, dok se sljedeći segmenti preuzimaju. Sve dok svaki novi segment stigne prije njegova vremena za reprodukciju, software za reprodukciju bit će u mogućnosti stvoriti glatku neprekinutu sliku videozapisa. Prednosti i nedostaci progresivnog preuzimanja i reprodukcije prikazani su tablicom 8, [16].

Tablica 8: Prednosti i nedostaci progresivnog preuzimanja i reprodukcije

Prednosti	Nedostaci
Nema trajne pohrane video sadržaja na korisnički uređaj. Brža reprodukcija video sadržaja nego u preuzimanju i reprodukciji.	Zahtjeva specijalne tehnike segmentiranja video sadržaja, koji ne podržavaju svi software-i za reprodukciju. Povećana kompleksnost i troškovi.

Izvor: [16]

3.2.2 Video konferencije

Video konferencije koriste sinkronizirane audio i video signale kako bi omogućile dvosmjernu komunikaciju između dvije udaljene točke. Da bi prijenos video signala bio moguć nužno je prvo napraviti kodiranje. Jedan od glavnih standarda koji se koristi u video konferencijama za kodiranje je H.264. U video konferencijama razmjenjuje se više tipova sadržaja ,a za pravilno postupanje s različitim tipovima sadržaja implementiran je H.323 standard. Video konferencije mogu biti uspostavljanje između dva ili više korisnika na taj

način da audio i video signali reagiraju na aktivnosti korisnika. Video konferencije za uspostavljanje sesije koriste SIP protokol. Osim uspostavljanja video konferencije moguće je i uspostavljanje podatkovne konferencije, što omogućuje T.120 protokol.

3.2.2.1 H.323

H.323 je međunarodni standard za paketne multimedijske komunikacije, koji je definiran od strane Međunarodne Telekomunikacijske Unije (eng. *International Telecommunication Union* - ITU). H.323 standardiziran je da radi na nizu tehnologija koje se koriste u paketnim mrežama bile one pouzdane ili nepouzdane (TCP i UDP). H.323 sam po sebi nije standard već je on definiran nizom drugih standarda koje koristi. Njegova glavna zadaća je da određenim protokolima objasni kako da postupaju s pojedinim tipom multimedijskog sadržaja. Postoji niz uređaja koji su propisani H.323 standardom, koji su zaduženi za uspješno uspostavljanje video konferencija. Prema [16] četiri najvažnija uređaja propisana H.323 standardom su:

- Terminali – krajnje točke komunikacije u H.323 standardu.
- *Gateway* – služi kao prevoditelj između različitih protokola koji se koriste za uspostavljanje i raskidanje poziva, kao i za konvertiranje video i audio signala u odgovarajući oblik za komunikaciju.
- *Gatekeeper* – njegova implementacija u mreži nije obavezna ali može korisnicima pružiti usluge pretrage baze podataka.
- Upravljačka jedinica – uređaji koji se koriste kada se komunikacija odvija na više od dva terminala.

3.2.2.2 H.264

H.264 je poznatiji pod nazivom MPEG 4 i to je standard za kodiranje i dekodiranje video signala. Njegova glavna prednost je u tome što se može primijeniti u video konferencijama koje koriste male brzine slanja, kao i u video konferencijama koje koriste veće brzine slanja.

Ovaj standard je našao široku primjenu u video konferencijama jer omogućuje slanje slika visoke kvalitete koristeći vrlo male brzine prijenosa. Također ovim standardom paketi dolaze na odredište u odgovarajućem redoslijedu što smanjuje kašnjenje uzrokovano kodiranjem i dekodiranjem, [16].

3.2.2.3 T.120

Osnovna funkcija T.120 protokola je omogućavanje podatkovne konferencije, koje su vrlo slične glasovnim i video konferencijama. To znači da više korisnika može dijeliti iste podatke među sobom u stvarnom vremenu. Prema [16] postoji niz funkcija koje se mogu izvesti koristeći T.120 protokol, a neke od njih:

- *Chat* – omogućuje korisnicima da razmjenjuju kratke tekstualne poruke među sobom.
- Prijenos datoteka – omogućuje slanje datoteka sa jednog računala na drugo.
- Dijeljene aplikacije – Omogućuje korisniku koji je pokrenu aplikaciju da neki drugi udaljeni korisnik preuzme kontrolu nad tom aplikacijom.

Najveći problem T.120 protokola je u sigurnosti, jer omogućuje niz funkcija koje zlonamjerni korisnici mogu iskoristi kako bi postavili razne *maleware* aplikacije na računalo. Ili u slučaju da je pokrenuta aplikacija koja omogućuje preuzimanje kontrole nad računalom, omogućilo bi korisniku da pregledava korisnikove datoteke bez odobrenja. Zbog tih razloga mnoge od funkcija koje T.120 omogućuje nisu korištene u većem broju, [16].

3.3 Aplikacije za prijenos podataka

3.3.1 Elektronička pošta

Elektronička pošta je prvotno bila namijenjena samo za slanje i primanje tekstualnih poruka kroz mrežu između dva korisnika. Danas korisnici osim slanja tekstualnih poruka imaju i mogućnost slanja slika i datoteka različitih tipova. Elektronička pošta je definirana protokolima POP (eng. *Post Offfice Protocol*) koji služi za preuzimanje poruka s poslužitelja i SMTP (eng. *Simple Mail Transfer Protocol*) koji služi za slanje poruka. Svaka poruka se sastoji od zaglavlja i tijela poruke. U zaglavlje elektroničke pošte spada adresa pošiljatelja, adresa primatelja i naslov poruke, a tijelo sadrži tekst poruke, [17].

3.3.2 Usluge pretraživanja informacija

Usluge pretraživanja informacija ili poznatije kao WWW (eng. *World Wide Web*) su u osnovi način prijenosa podataka između stranaka putem Interneta, utemeljenja na modelu klijent-poslužitelj. Glavne tehnologije na kojima je WWW baziran su: HTTP i HTML. HTTP

je protokol aplikacijskog sloja koji je zadužen za razmjenu informacija između klijenta i poslužitelja u Internet mreži. HTML je jezik koji je razvijen za stvaranje hipertekstualnih dokumenata koji se objavljuju na Internetu. Informacije se nalaze na poslužiteljima koji su spojeni na Internet mrežu i koji su uspostavljeni od strane raznih tvrtki, sveučilišta, organizacija ili privatnih korisnika. Poslužitelji su uglavnom uspostavljeni na običnim radnim jedinicama koji pokreću specijalizirani poslužiteljski softwear-a. Klijenti pristupaju informacijama na poslužiteljima pomoću raznih Web preglednika koji mogu prikazivati više tipova informacija (slika, audio, govor, itd.), [18].

3.3.3 Dijeljene datoteka

Dijeljenje datoteka je metoda distribucije digitalnog sadržaja između korisnika koji imaju različite administratorske povlastice, koristeći podatkovnu mrežu. Dijeljenje datoteka omogućuje velikom broju korisnika da pristupe istoj datoteci te im pruža mogućnost da pročitaju, uređuju, preuzmu ili isprintaju datoteku. Karakteristika ovih aplikacija je u tome da kada korisnik jednom preuzme datoteku sa tog tipa mreže, njihovo računalo postaje dijelom te mreže što omogućuje ostalim korisnicima da preuzmu datoteku s korisničkog računala. [19], [20].

Dijeljene datoteka se može izvršiti na nizu metoda od kojih su najpopularnije: dijeljenje datoteka pomoću prijenosnog medija (USB, CD, DVD, itd.), distribuiranje datoteka preko centralnog poslužitelja na mreži, WWW hiperlinkovi i distribucijske P2P (eng. *Peer-to-peer*) mreže. Danas se dijeljene datoteka izvršava preko paketnih mreža koje koriste razne protokole za prijenos datoteka ka što je FTP, dok se nekoć uglavnom koristila metoda distribucije prenosim medijem, [19], [20].

Dijeljene datoteka je u pravilu nezakonito ako korisnik nema autorska prava ili prava za distribuciju sadržaja. Dijeljene datoteka je također vrlo rizično jer stranice i programi poput BitTorenta postavljaju razne zlonamjerne software u datoteke kako bi dohvatile informacije o korisniku, [19], [20].

4. Karakteristične duljine paketa pojedinih aplikacija i granice QoS parametara

4.1 Kvaliteta usluge (QoS)

Osnovni način pružanja QoS-a je pružiti uslugu za određenu razinu, na razini paketa ili na razini sesije, što se može izvesti na dva načina. Prvi način je da se određenim korisnicima dodjeljuju prioriteti, a drugi je da se određenim korisnicama pruži veća širina propusnog pojasa, kako bi se pružila odgovarajuća razina QoS-a. Prema [21] dva glavna pristupa u pružanju razine usluga su:

- Rezervacijom resursa - U ovom se modelu identificiraju mrežni resursi i rezerviraju. Mrežni čvorovi klasificiraju dolazne pakete i koristite rezervacije za pružanje QoS-a. Model integriranih usluga (*IntServ*) se temelji na ovom pristupu.
- Bez rezervacije resursa - U ovom modelu resursi nisu rezervirani, već umjesto toga, promet se klasificira u različite skupove klasa, na temelju kojih mrežni čvorovi pružaju prioritet pri posluživanju. Model diferencijalne usluge (*DiffServ*) se temelji na ovom pristupu.

Modelom integriranih usluga klasificiraju se tri skupine usluga koje mogu biti ponuđene korisniku, a to su:

- *Best effort* usluge – u ovom tipu usluga ne postoje zahtjevi za QoS, već mreža pruža najbolju kvalitetu usluge koju može pružiti korisniku u tom trenutku.
- Usluge garantirane isporuke – ove usluge korisnicima pružaju dovoljne širine propusnog pojasa, prihvatljivo vrijeme kašnjenja i osiguravaju da nema gubitka paketa u tokovima.
- Usluge ograničenih mogućnosti – garantiraju korisniku da će dobiti kvalitetu usluge koja je što bliža kvaliteti usluge u *Best effort* prijenosu.

4.1.1 Kašnjenje

Kašnjenje ili latencija je vrijeme koje je potrebno paketu da prođe kroz mrežu od kraja do kraja. Kašnjenje je jedan od glavnih parametra QoS-a na koji treba obratiti pozornost kod aplikacija koje koriste komunikaciju u stvarnom vremenu kao što su VoIP, i druge slične.

Velike vrijednosti kašnjenja ne moraju nužno degradirati kvalitetu takvih aplikacija, ali rezultat može biti nedostatak sinkronizacije između korisnika, što može uzrokovati nerazumljivost u komunikaciji. U pravilu se preporuča da vrijednost kašnjenja za takve aplikacije bude manja od 150 milisekundi. Prilikom planiranja višeuslužnih mreža treba obratiti pažnju na sve elemente koji utječu na kašnjenje, prema [11], [22] to su:

- Kašnjenje koje nastaje u čvorovima zbog paketizacije. To je vrijeme koje je potrebno čvorištu da pohrani podatke u pakete, u suštini što je paket veći to je kašnjenje zbog paketizacije veće. Vrijeme paketizacije ovisi i o vremenu koje je potrebno odredišnom čvoru da obradi zaprimljene podatke. Vrijeme paketizacije u idealnim slučajevima ne bi trebalo prelaziti 30 ms.
- Kašnjenje koje je potrebno za serializiranje digitalnih podataka na fizičke veze. Ovo kašnjenje je obrnuto proporcionalno brzini veze. Drugim riječima, što je brži medij, to je manje kašnjenje. Ova vrijednost je ovisna o tehnologiji poveznice (*link*) koja se koristi i njezinoj pristupnoj metodi. Iako je to kašnjenje neizbježno (bez obzira na propusnu širinu koja se koristi), korištenjem velikih širina propusnih pojasa i korištenjem malih broja veza, moguće je smanjiti vrijeme kašnjenja.
- Propagacijsko kašnjenje je vrijeme koje je potrebno električnom (ili svjetlosnom) signalu da prođe dužinu vodiča. Brzina ovih signala je uvijek manja od brzine svjetlosti. Uvijek postoji propagacijsko kašnjenje; međutim, to postaje problem samo u slučajevima kada signali prelaze velike udaljenosti.
- Kašnjenje uzrokovano čekanjem u redovima, je vrijeme koje paket provede u međuspremniku u mrežnom elementu dok čeka prijenos. Zbog promjena u količini mrežnog prometa dolazi do varijabilnih kašnjenja u redu čekanja. Ovo kašnjenje također se temelji na količini prometa koja pokušava proći kroz element, to jest pokušava pristupiti određenoj poveznici.
- Kašnjenje uzrokovano prosljeđivanjem paketa, je vrijeme koje je potrebno mrežnom uređaju (usmjerivač, komutator, vatrozid i sl.) da pohrani paket u međuspremnik dok odlučuje kojem čvoru treba proslijediti paket. Ovo kašnjenje je varijabilno i ovisi o arhitekturi i funkcijama pojedinih mrežnih uređaja.

4.1.2 Varijacija kašnjenja

Varijacija kašnjenja (eng. *jitter*) je razlika u kašnjenju paketa iste sesije. Najveći krivac *jittera* je varijacija u redu čekanja zbog dinamičkih promjena u mrežnom opterećenju.

Drugi uzrok su paketi koji ponekad mogu imati drugačiju vezu koja nije fizički iste duljine ili parametara kao i ostale veze.

U praksi se uvijek očekuje neko vrijeme varijacije kašnjenja. Velike vrijednosti varijacije kašnjenja mogu prouzročiti probleme u kvaliteti aplikacija koje su vremenski dosta osjetljive, jer paketi mogu doći na odredište nepravilnim redoslijedom, što bi za *gateway* značilo da te pakete treba odbaciti. Problem nastaje kada *gateway* pretjerano počne odbacivati pakete iz međuspremnika jer su došli nepravilnim redoslijedom, posljedica toga je veliki razmak u reprodukciji medija, za aplikacije koje su osjetljive na *jitter*, [11].

4.1.3 Šiina pojasa ili propusnost

Širina prijenosnog pojasa (eng. *bandwith*) zapravo predstavlja maksimalni dostupan kapacitet kanala koji se može koristiti u svrhu prijenosa podataka na nekoj vezi. Širina propusnog pojasa definirana je kao broj prenesenih bitova u nekoj vremenskoj jedinici npr. MB/s. Različite aplikacije imaju različite potrebe za širinom propusnog pojasa, a nedovoljne širine propusnog pojasa mogu uzrokovati povećanje kašnjenja i zagušenje mreže.

4.1.4 Gubitak paketa

Gubitak paketa je jedan od parametara koji znatno utječe na kvalitetu usluge, svih vrsta aplikacija. Gubitak paketa u prijenosu je neizbježan, te može nastati iz niza razloga. Do gubitka paketa obično dolazi prilikom zagušenja u mreži, kada su usmjerivači i komutatori prisiljeni odbaciti paketa iz reda čekanja kako bi spriječili preplavljivanje međuspremnika. Još jedan od razloga može biti greška u prijenosu jer paketi mogu doći na pogrešno odredište koje ga u tom slučaju odbacuje. Aplikacije koje ne koriste prijenos u stvarnom vremenu mogu tolerirati određeni gubitak paketa, jer koriste TCP koji u sebi ima ugrađeni tajmer za retransmisiju. Kod aplikacija koje su vremenski osjetljive retransmisija paketa nema smisla jer kada paket dođe na odredište već je prošao njegov trenutak kada se treba reproducirati, pa ti paketi samo mogu izazvati još veće degradiranje kvalitete usluge, [22].

4.2 Karakteristične duljine paketa i granice QoS parametra

4.2.1 Govorne aplikacije

Kod govornih aplikacija karakteristična duljina paketa ovisi o duljini zaglavlja i o sadržaju koji se prenosi koji je definiran raznim kodecima. Duljina zaglavlja u govornim aplikacijama sastoji se od:

- IP zaglavlja duljine 20 bajta,

- UDP zaglavlja duljine 8 bajta,
- RTP zaglava koje duljine 12 bajta,
- Ethernet L2 zaglavlja duljine 18 bajta, koje u sebi sadržava 4 bajta za CRC.

Duljina sadržaja paketa ovisi o kodeku koji koristi. Duljine glasovnog sadržaja paketa ovisno o kodecima prikazane su tablicom 9. Stupac duljina glasovnog sadržaja iz tablice 9 predstavlja koliki dio glasovnog sadržaja će se prenositi svakim paketom, [23].

Tablica 9: Duljina sadržaja u VoIP paketima

Kodek	Duljina glasovnog sadržaja (bajt)	Duljina glasovnog sadržaja (ms)
G.711	160	20
G.728	60	30
G.729	20	20
G.723.1	20	30

Izvor:[23]

Budući da duljina paketa ovisi o kodeku tako ne postoji prosječna duljina paketa za sve govorne aplikacije već postoji prosječna duljina paketa za pojedini kodek. Na primjer ako se koristi G.711 standard za prijenos govora onda će prosječna duljina paketa iznositi 218 bajtova. Duljina paketa ovisi o duljini zaglavlja i duljini sadržaja. Duljina zaglavlja je uvijek ista i iznosi 58 bajta (zbroj svih zaglavlja), a duljina sadržaja je u ovom slučaju 160 bajtova, [23].

Govorne aplikacije su vrlo osjetljive na kašnjenje, varijaciju kašnjenja i gubitak paketa. Veliko kašnjenje uzrokuje dugo vrijeme odgovora, što znači da kada korisnik počne govoriti prođe dugi vremenski period prije nego ga drugi korisnik čuje, što korisnici smatraju ne prihvatljivim te iz tog razloga prekidaju razgovor. Velika odstupanja u varijaciji kašnjenja i gubitak velikog broja paketa uzrokuju nerazumljivost u komunikaciji. Prihvatljive i preporučene granice QoS parametara za glasovne aplikacije prikazane su tablicom 10.

Budući da su različite aplikacije osjetljive na kašnjenje, varijaciju kašnjenja i gubitak paketa, te imaju specifične zahtjeve za širinom propusnog pojasa, korisno je provesti analizu maksimalnog ulaznog toka u čvor za definirano maksimalno prosječno vrijeme čekanja paketa u redu. Vrijeme koje paket provede u redu čekanja jedan je od glavnih uzročnika varijacije kašnjenja i ima veliki utjecaj na vrijeme kašnjenja i gubitak paketa. Analiza maksimalnog ulaznog toka u čvor provedena je u 6. poglavlju ovog rada.

Tablica 10: Granice QoS parametara za glasovne aplikacije

Parametar	Prihvatljivo	Preporučeno
Kašnjenje	Do 300 ms	150 ms
Varijacija kašnjenja	Do 50 ms	20 ms
Gubitak paketa	Do 5%	<1%
Bandwith	Minimalno 64 kbit/s	1 Mbit/s

Izvor:[23]

4.2.2 Video aplikacije

Postoji nekoliko atributa koji se mogu koristiti za opisivanje videozapisa. Na primjer, videozapis se može prenositi pomoću strujanja ili može biti unaprijed postavljen, te visoke razlučivosti ili niske razlučivosti. Veličina paketa ovisi o vrsti video kodeka koji se koristi za kodiranje i dekodiranje kao što su H.264, MPEG4 i napredno video kodiranje (eng. *Andvanced Video Coding*) ili skraćeno AVC. Nakon što se obavi kodiranje dobivaju se paketi duljine 188 bajta koji se zovu PES (eng. *Packetized Elementary Stream*), te se potom ti paketi pakiraju u IP pakete. IP paket može sadržavati maksimalno 7 PES paketa, što bi značilo da je maksimalna duljina paketa 1316 bajta ne uključujući zaglavlja, [24].

Razlučivost videa ima velike potražnje za propusnom širinom. Video manjih razlučivosti kao što su 704 x 576 piksela zahtijevaju minimalni propusni pojas od 1 Mbit/s, a video većih razlučivosti 1920 x 1080 piksela zahtijevaju od 5 do 8 Mbit/s zavisno o tehnici kodiranja, [24].

Video aplikacije koje se prenose u stvarnom vremenu su osjetljive na kašnjenje, varijaciju kašnjenja i gubitak paketa. Prihvatljive i preporučene granice QoS parametara za video aplikacije prikazane su tablicom 11.

Tablica 11: Granice QoS parametara za video aplikacije

Parametar	Prihvatljivo	Preporučeno
Kašnjenje	Do 300 ms	150 ms
Varijacija kašnjenja	Do 50 ms	10 ms
Gubitak paketa	Do 1%	<0.5%
Bandwith	1-8 Mbit/s za video niske i srednje razlučivosti	Minimalno 8 Mbit/s za video visoke razlučivosti

Izvor: [24]

5. Podvorbeni modeli i matematički izračuna performansi paketne mreže

Za uspješno dizajniranje podatkovne mreže nužan je odabir odgovarajućeg prometnog modela. Kriteriji prema kojima se odabire prometni model su:

- uzorci dolazaka poziva/paketa,
- vrijeme zauzimanja resursa,
- blokirani pozivi/ gubici paketa,
- broj izvora (ograničeni i neograničeni).

Ako je primjerice jedan izvor prometa i jedan poslužitelj, vjerojatnost blokiranja jednaka je nuli, no međutim kako broj izvora raste vjerojatnost blokiranja postaje sve veća. Broj izvora je važan kada je sustav posluživanja (npr. broj kanala) mali i još se zahtijeva određena razina posluživanja. Primjer ograničenog izvora je slučaj kada je npr. broj izvora ponuđenog prometa mali u odnosu na broj poslužitelja, [25].

Nakon što se odredi uzorak dolaznih poziva i definira način posluživanja u smislu blokiranja, broj izvora poziva/paketa, odnosno vrsta izvora (ograničen i neograničen izvor) i distribucija vremena zauzimanja resursa, ispunjene su pretpostavke za odabir prometnog modela koji opisuje određeno okruženje. Premda ne postoji model koji može egzaktno opisati realne situacije, tim modelima se pretpostavljaju prosjeci u svim situacijama. Prema [25] najčešće korišteni prometni modeli su:

- Erlangov B model,
- prošireni Erlang B model, i
- Erlang C model.

Također je potrebno odabrati prikladnu disciplinu posluživanja paketa u paketnim mrežama. Disciplinom posluživanja određena su pravila prema kojim se poslužuju paketi. Najjednostavnija disciplina i najčešće susretana u praksi je disciplina "prvi došao prvi poslužen" (eng. *First Came First Served*) ili skraćeno FCFS, [26].

Pojedini mrežni sustavi i podsustavi mogu se prometno opisivati nekim od Markovljevih modela posluživanja. U slučaju da dolasci paketa imaju značajke Poissonova toka i veličine paketa su determinirane, može se primijeniti model M/D/1, [5], [26], gdje su:

- M/D/1 – oznaka distribucije dolazaka odnosno međudolaznih vremena, što je u ovom slučaju M, što označava eksponencijalnu distribuciju.
- M/D/1 – oznaka distribucije vremena posluživanja, u ovom slučaju D, što označava determinističku distribuciju posluživanja.
- M/D/1 – Oznaka broja kanala.

Markovljevim modelom posluživanja mogu se razmatrati osnovne komponente kašnjenja u sustavima, a to su: $T_q = T_s + T_W + T_{pr}$ (2)

gdje su:

- T_q – kašnjenje ili vrijeme zadržavanja paketa u sustavu,
- T_s – prosječno vrijeme posluživanja,
- T_w – prosječno vrijeme čekanja u redu, i
- T_{pr} – vrijeme propagacije koje za ne satelitski prijenos zanemarujemo.

Markovljev M/D/1 model ima značajke Poissonova toka i determinirane veličine paketa, onda u tom slučaju vrijede sljedeći izrazi za izračunavanje kašnjenja (sva vremena kašnjenja izražavaju se vremenskom jedinicom), [5]:

$$T_q = \frac{T_s}{1-\rho} \cdot (1 - \frac{\rho}{2}) \tag{3}$$

$$T_s = \frac{D}{C} \tag{4}$$

$$T_W = \frac{T_s \cdot \rho}{2 \cdot (1-\rho)} \tag{5}$$

U izrazu (4) oznaka D predstavlja prosječnu duljinu paketa.

Prometno opterećenje ρ jediničnog poslužitelja može biti u rasponu od 0 od 1 Erlanga, ovisno o tomu koliki dio kapaciteta je iskorišten tijekom promatranog vremena. Prema [5] izraz za prometno opterećenje glasi:

$$\rho = \emptyset \cdot \frac{D}{C} \tag{6}$$

$$\emptyset = \frac{\rho}{T_s} \tag{7}$$

gdje je:

- $\emptyset$ - intenzitet nailazaka paketa u jedinici vremena
- $C-$ kapacitet poslužitelja

Prosječni broj paketa koji čeka u redu na posluživanje (Lw) računa se prema sljedećim izrazima:

$$L_w = \frac{\rho^2}{2 * (1 - \rho)} \tag{8}$$

$$L_w = \emptyset * T_w \tag{9}$$

6. Ograničavanje veličine ulaznog toka u čvor paketne mreže uz određeno prometno opterećenje

Analiza veličine ulaznog toka u čvor paketne mreže napravljena je o ovisnosti prosječne duljine paketa i kapaciteta poslužitelja. Maksimalno vrijeme čekanja paketa u redu u ovoj analizi iznosi 10 ms. Prosječne duljine paketa definirane su u skladu s poglavljem 4. i analizom duljina paketa provedenom u [27].

Uvrštavanjem vrijednosti u izraz (4) određene su vrijednosti prosječnog vremena posluživanja za prosječnu duljinu paketa 1744, 3200, 5600, 9040, 9600, 10400 bita i kapacitet poslužitelja 1 Mbit/s.

Tablica 12: Vrijednosti prosječnog vremena posluživanja za kapacitet poslužitelja 1 Mbit/s

Prosječna duljina paketa *D* (bit)	Prosječno vrijeme posluživanja *Ts* (ms)
1744	1,74
3200	3,2
5600	5,6
9040	9,04
9600	9,6
10400	10,4

Iz rezultata prikazanih u tablice 12 može se zaključiti da na prosječno vrijeme posluživanja utječe prosječna duljina paketa, odnosno da veća prosječna duljina paketa povećava prosječno vrijeme posluživanja.

Maksimalno prometno opterećenje ρ izlučuje se iz izraza (5), te uvrštavanjem vrijednosti u izraz dobivaju se vrijednosti prikazane u tablici 13. Iz rezultata prikazanih u tablici 13 može se zaključiti da veće vrijednosti prosječnog vremena posluživanja i prosječne duljine paketa smanjuju maksimalno prometno opterećenje, koje poslužitelj može obraditi da prosječno vrijeme čekanja u redu ne prelazi 10 ms.

Tablica 13: Vrijednost maksimalnog prometnog opterećenja ρ za kapacitet poslužitelja 1 Mbit/s

Prosječna duljina paketa (bit)	Prosječno vrijeme posluživanja *Ts* (ms)	Maksimalno prosječno vrijeme čekanja u redu *Tw* (ms)	Maksimalno prometno opterećenje ρ (Erl)
1744	1,74	10	0,9198
3200	3,2	10	0,8621
5600	5,6	10	0,78125
9040	9,04	10	0,6887
9600	9,6	10	0,6757
10400	10,4	10	0,6579

Uvrštavanjem vrijednosti maksimalnog prometnog opterećenja iz tablice 13 u izraz (7) dobivaju se vrijednosti maksimalnog prometnog toka prikazane u tablici 14. Iz rezultata prikazanih u tablici 14 može se zaključiti da manje prosječne duljine paketa imaju veću vrijednost maksimalnog ulaznog toka, zbog kraćeg prosječnog vremena posluživanja i većeg maksimalnog prometnog opterećenja.

Tablica 14:Maksimalni prometni tok za kapacitet poslužitelja 1 Mbit/s

Prosječna duljina paketa D (bit)	Prosječno vrijeme posluživanja Ts (ms)	Maksimalno prometno opterećenje ρ (Erl)	Maksimalna veličina ulaznog toka Ø (paket/s)
1744	1,74	0,9198	527
3200	3,2	0,8621	269
5600	5,6	0,78125	139
9040	9,04	0,6887	76
9600	9,6	0,6757	70
10400	10,4	0,6579	63

Uvrštavanjem vrijednosti u izraz (4), (5) i (7) određene su vrijednosti prosječnog vremena posluživanja, maksimalnog prometnog opterećenja i maksimalne veličine ulaznog toka, za prosječnu duljinu paketa 1744, 3200, 5600, 9040, 9600, 10400 bita i kapacitet poslužitelja 5 i 10 Mbit/s (tablice 15 i 16).

Tablica 15: Vrijednost Ts, ρ i Ø za kapacitet poslužitelja 5 Mbit/s

Prosječna duljina paketa (bit)	Prosječno vrijeme posluživanja *Ts* (ms)	Maksimalno prosječno vrijeme čekanja *Tw* (ms)	Maksimalno prometno opterećenje ρ (Erl)	Maksimalna veličina ulaznog toka Ø (paket/s)
1744	0,349	10	0,9829	2817
3200	0,64	10	0,969	1514
5600	1,12	10	0,947	845
9040	1,1808	10	0,9171	507
9600	1,92	10	0,9124	475
10400	2,08	10	0,9058	435

Tablica 16: Vrijednost Ts, ρ i Ø za kapacitet linka 10 Mbit/s

Prosječna duljina paketa (bit)	Prosječno vrijeme posluživanja *Ts* (ms)	Maksimalno prosječno vrijeme čekanja *Tw* (ms)	Maksimalno prometno opterećenje ρ (Erl)	Maksimalna veličina ulaznog toka Ø (paket/s)
1744	0,174	10	0,9914	5684
3200	0,32	10	0,9843	3075
5600	0,56	10	0,9728	1737
9040	0,904	10	0,9568	1058
9600	0,96	10	0,9542	993
10400	1,04	10	0,9506	914

Iz tablica 15 i 16 se može zaključiti da povećanjem kapaciteta poslužitelja može se znatno smanjiti prosječno vrijeme posluživanja. Nadalje se može zaključiti da zbog smanjenja prosječnog vremena posluživanja, prosječno vrijeme čekanja u redu za velike prosječne duljine paketa ostaje u definiranim granicama pri velikim prometnim opterećenjima, što uzrokuje veću veličinu ulaznog toka.

7. Zaključak

Jedna od osnovnih ljudskih potreba je komunikacija, a današnje komunikacijske tehnologije su omogućile komunikaciju s ljudima diljem svijeta u stvarnom vremenu koristeći različite multimedijske aplikacije. Iz tog razloga korisnici žele koristi multimedijske aplikacije na svojim računalima.

Korisnici danas ne žele više koristiti paketne mreže samo za prijenos poruka i datoteka, nego žele imati i mogućnost pristupa različitim audio i video sadržajima u stvarnom vremenu. Takve potrebe korisnika dovele su do ubrzanog razvoja paketnih mreža, i većeg broja korisnika. S porastom korisnika su se pojavila i veća prometna opterećenja, ta povećanja su dovele do potrebe za implementiranjem različitih dodatnih mehanizama i tehnika u čvor paketne mreže, kako se mreža ne bi dovela u stanje zastoja. Te vrste mehanizama su kontrola zagušenja, upravljanje usmjeravanjem i detekcija i ispravak pogreška.

Ti mehanizmi su omogućili da se ograniči ulazni tok u čvor paketne prema različitim parametrima QoS kako bi se korisnicima garantirala određena razina usluge. QoS parametri su: kašnjenje, varijacija kašnjenja, gubici paketa i propusna širina. Da se može pružiti određena kvaliteta usluge razvijena su dva modela QoS-a , a to su *IntServ* i *DifServ*. Ovi modeli su pružili da se kvaliteta usluge može pružiti na razini paketa, sesije ili mreže.

Aplikacije koje se danas najviše koriste su govorne i video aplikacije, a pogotovo one koje zahtijevaju prijenos u stvarnom vremenu. Privatni korisnici većinom te aplikacije koriste kako bi pristupile raznim zabavnim sadržajima kao što su: online video igre, gledanje video strujanjem, preslušavanje glazbe itd. Osim u zabavne svrhe veliku primjenu su našle i u poslovnom svijetu, a najpopularniji tip aplikacija je video konferencija. Različite organizacije, sveučilišta, i medicinske ustanove koriste video konferencije kako bi pružile različite online tečajeve, strukovna usavršavanja i imali poslovne sastanke, između više lokacija kako bi smanjile svoje troškove.

Prema analizi koja je provedena u poglavlju 6, može se zaključiti da ograničavanjem prosječnog vremena koji paket provede u redu čekanja može znatno smanjiti veličinu ulaznog toka pri manjim kapacitetima poslužitelja i većim prosječnim duljinama paketa. Nadalje se može zaključiti da granice prosječnog vremena čekanja u redu pri većim kapacitetima poslužitelja mogu uzrokovati velika maksimalna prometna opterećenja. Kako bi se smanjila maksimalna prometna opterećenja nužno je smanjiti granice prosječnog vremena čekanja u redu pri većim kapacitetima poslužitelja.

Različite studije ukazuju na trend rast broja korisnika govornih i video aplikacija, a pogotovo video aplikacija koje prenose video strujanjem. Taj tip video aplikacija koristi velike širine propusnog pojasa i zahtijevaju mala vremena kašnjenja. Uvođenjem novih tehnologija i medija za prijenos podataka poput optičkih vlakana omogući će se korisnicima da koriste ove tipove aplikacija bez ikakvih problema i sa garantiranom određenom kvalitetom usluge.

Popis literature

[1] Socrates, C., Sridharan, R.: Congestion Control for Packet Switched Networks: A Survey, International Journal of Scientific and Research Publications, 2014.

[2] Chen, T.: Network Traffic Management, The Handbook of Computer Networks, Dallas, Southern Methodist University, 2007.

[3], Cheng-Yuan, H., Chen, Y., Yi-Cheng, C., Cheng-Yun, H.: Fast retransmit and fast recovery schemes of transport protocols: A survey and Taxonomy, Computer Networks, 2008.

[4] Thiruchelvi, J.: A Survey On Active Queue Management Mechanisms, International Journal of Computer Science and Network Security, 2008.

[5] Bošnjak, I.: Telekomunikacijski promet II, Zagreb: Fakultet prometnih znanosti, 2001.

[6]https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/unicast/503_u1_2/nexus3000_unicast_config_gd_503_u1_2/l3_route.html?referring_site=RE&pos=2&page=https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configur (pristupljeno: kolovoz 2018)

[7] Balchunas, A.: Static vs. Dynamic Routing, raspoloživo na: https://www.routeralley.com/guides/static_dynamic_routing.pdf, (pristupljeno: kolovoz 2018.)

[8] Budhathok, D.: Error control and Detection, raspoloživo na: http://www.idc-online.com/technical_references/pdfs/data_communications/Error_Control_and_Detection.pdf. (pristupljeno kolovoz 2018.)

[9] https://techterms.com/definition/checksum (pristupljeno: kolovoz 2018.).

[10]: https://nptel.ac.in/courses/106105080/pdf/M3L3.pdf, (pristupljeno kolovoz 2018).

[11] Juniper Networks: Voice Over IP 101, raspoloživo na: https://cours.etsmtl.ca/mgr816/VoIP101.pdf, (pristupljeno: kolovoz 2018.)

[12] Baset, S., Gurbani, V., Johnston, A.: The Session Initiation Protocol (SIP): An Evolutionary Study, Journal of communications, 2012.

[13]https://cdn.ttgtmedia.com/searchVoIP/downloads/Building_a_VoIP_Network_Ch[1]._8.pdf, 2006, pp. 345-386. (pristupljeno: kolovoz 2018.)

[14] https://ccm.net/contents/288-rtp-rtcp-protocols, pristupljeno (Kolovoz 2018) .

[15] Veličković, Z., Jocić, J.: Measurement QoS Parameters of VoIP Codecs as a Function of the Network Traffic Level, 5th International Conference on Information Society and Technology, 2015.

[16] Simpson, W.: Video over IP, Elsevier, 2008.

[17] https://techterms.com/definition/email (pristupljeno kolovoz 2018.)

[18] Arvidsson A., Karlsson P.: The Characteristics of WWW Traffic and the Relevance to ATM raspoloživo na: https://www.diva-portal.org/smash/get/diva2:837823/FULLTEXT01.pdf (pristupljeno: kolovoz 2018.)

[19] https://searchmobilecomputing.techtarget.com/definition/file-sharing

(pristupljeno kolovoz 2018.)

[20]:https://www.techopedia.com/definition/16256/file-sharing (pristupljeno: kolovoz 2018.)

[21] Sivalingam, K., Mahadevan, I.: Quality of Service Architectures for Wireless Networks: IntServ and DiffServ Models, Lipanj 1999.

[22] SANS Institute: Latency and QoS for Voice over IP, 2004, raspoloživo na:https://www.sans.org/reading-room/whitepapers/voip/latency-qos-voice-ip-1349 (pristupljeno: kolovoz 2018.)

[23]https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html (pristupljeno: kolovoz 2018.)

[24]https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/pktvideoaag.html, (pristupljeno: kolovoz 2018.)

[25]https://moodle.srce.hr/2017-

2018/pluginfile.php/1210641/mod_resource/content/5/Odabir%20prometnog%20modela%20za%20objavu.pdf (pristupljeno: kolovoz 2018.)

[26]https://moodle.srce.hr/20172018/pluginfile.php/1210661/mod_resource/content/3/Sustavi%20poslu%C5%BEivanja%20s%20%C4%8Dekanjem.pdf (pristupljeno: kolovoz 2018.)

[27] Xiao-Long, W., Wei-Min, L., Fang, L. , Hua, Y.: Packet size distribution of typical Internet applications, Beijing University of Posts and Telecommunications, Beijing, China

Popis slika

Slika 1: Primjer ponovnog slanja paketa 13
Slika 2: Prikaz RTP zaglavlja 17

Popis tablica

Tablica 1: Prednosti i nedostaci AQM-a 7
Tablica 2: Prednosti i nedostaci fiksnog usmjeravanja 9
Tablica 3: Prednosti i nedostaci adaptivnog usmjeravanja 10
Tablica 4: Primjer provjere pariteta 11
Tablica 5: Karakteristike CODEC-a 19
Tablica 6: Prednosti i nedostaci čistog strujanja 21
Tablica 7: prednosti i nedostaci preuzimanja i reprodukcije 22
Tablica 8: Prednosti i nedostaci progresivnog preuzimanja i reprodukcije 22
Tablica 9: Duljina sadržaja u VoIP paketima 29
Tablica 10: Granice QoS parametara za glasovne aplikacije 30
Tablica 11: Granice QoS parametara za video aplikacije 30
Tablica 12: Vrijednosti prosječnog vremena posluživanja za kapacitet poslužitelja 1 Mbit/s 34
Tablica 13: Vrijednost maksimalnog prometnog opterećenja ρ za kapacitet poslužitelja 1 Mbit/s 34
Tablica 14:Maksimalni prometni tok za kapacitet poslužitelja 1 Mbit/s 35
Tablica 15: Vrijednost Ts, ρ i Ø za kapacitet poslužitelja 5 Mbit/s 35
Tablica 16: Vrijednost Ts, ρ i Ø za kapacitet linka 10 Mbit/s 35