

## 2. ARHITEKTURA RAČUNALNIH MREŽA

### 2.1 OPĆA SVOJSTVA RAČUNALNIH MREŽA

#### 2.1.1 SISTEMATIZACIJA MREŽA

Računalne mreže možemo podijeliti prema elementima, topologiji, načinu korištenja usluge, vlasništvu i obuhvatu područja.

##### 2.1.1.1 Podjela mreža prema elementima

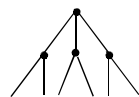
- **MREŽE TERMINALA** - osiguravaju vezu centralnog računala i njegovih terminala. Ovaj koncept je vezan za tzv. velika računala. Sva obrada se obavlja na računalu, a terminal služi za interakciju s operaterom.
- **MREŽE RAČUNALA** - čvorovi ove mreže su računala koja primaju poruke, usmjeravaju ih na odredište, skupljaju i izdaju podatke o stanju i uporabi mreže, itd. Svako računalo uz sebe može imati mrežu terminala.

U novije vrijeme razlika među mrežama računala i terminala postaje sve manja. Naime, osobna se računala sve češće koriste kao terminali, pa se uvođenjem novih funkcija podjela polako gubi.

##### 2.1.1.2 Podjela mreža prema topologiji



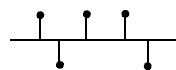
**zvjezdasta mreža** - karakterizirana je prolazom cjelokupnog prometa kroz jedan čvor, koji može biti glavno računalo sustava. Razmjena podataka među terminalima moguća je samo kroz glavno računalo. Upravljanje prometom je jednostavno, ali kvar glavnog računala znači prekid komunikacije.



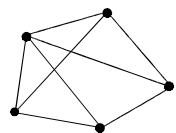
**stablasta mreža** - može se smatrati hijerarhijskom vezom više zvjezdastih mreža, koje zovemo podmrežama. Terminal može komunicirati unutar vlastite podmreže, a tražiti vezu s drugim podmrežama preko nadređene razine.



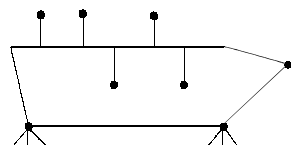
**prstenasta mreža** - svako računalo je spojeno na dva susjedna. U slučaju prekida jednog kanala, postoji mogućnost prijenosa podataka obilaznim putem.



**sabirnička mreža** - ostvarena je višespojnim povezivanjem. Nema središnjeg čvora, pa upravljanje može biti distribuirano. Zbog toga postoji mogućnost sudara poruka. U tom slučaju čvor čeka neko slučajno odabrano vrijeme i zatim ponovo šalje poruku.



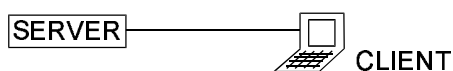
**isprepletena mreža** - ostvaruje se povezivanjem svakoga sa svakim. Neekonomična je za terminalske i druge mreže s malim iskorištenjem, ali može biti interesantna za mreže računala.



mreža općenite topologije, nastaje kombinacijom elementarnih topologija prema potrebama korisnika.

### 2.1.1.3 Podjela mreža prema načinu korištenja usluga

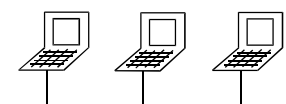
- Mreža **korisnik-poslužnik** (client-server), slika 2.1 je mreža s poslužiteljima.



Slika 2.1. - Mreža korisnik-poslužnik

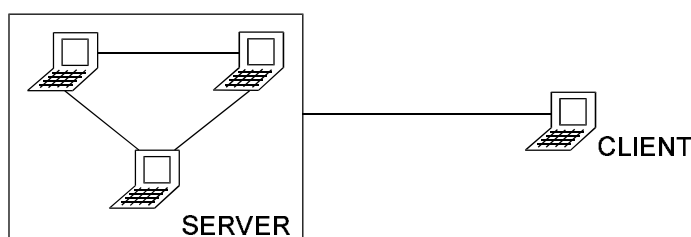
Poslužnik daje uslugu računalu korisnika, najčešće kroz korištenje nekog resursa. Dio se poslova obavlja na korisničkom računalu, na kojem se odvija korisnički program. Za razliku od mreža s neinteligentnim terminalima, na ovaj se način smanjuje opterećenje centralnog računala.

- Mreže s **ravnopravnim učesnicima** (peer-to-peer), slika 2.2, razvile su se zbog bolje kooperacije suradnika u timu. Svako računalo na mreži istovremeno je i korisnik i poslužnik, tj. izvršava i korisnički i poslužnički dio programske podrške.



Slika 2.2. - Mreža ravnopravnih učesnika

- Mreže s **distribuiranom obradom** razvijaju se umjesto velikih centralnih računala. Mogu biti dio mreže korisnik-poslužnik ili mreže s ravnopravnim učesnicima. Npr. kod mreže korisnik-poslužnik, mreža računala obavlja funkcije poslužnika, slika 2.3.



Slika 2.3. - Distribuirana baza podataka kod mreže korisnik-poslužnik

### 2.1.1.4 Podjela mreža prema vlasništvu

- Kod **privatnih mreža** - vlasnik (korisnik) samostalno upravlja mrežom prema vlastitim potrebama, tj. elementi mreže su u najmu ili vlasništvu pravne osobe, koja ujedno upravlja tom mrežom.
- Kod **javnih mreža** - vlasnik na komercijalnoj osnovi pruža uslugu prijenosa podataka drugima, te upravlja mrežom kako bi optimalno iskoristio instalirane kapacitete, a pri tome korisnicima pružio maksimalnu kakvoću usluge. Navedimo nekoliko primjera javnih mreža:
  - \* **Sustavi za prijenos poruka** (BBS, Bulletin Board System) su računala kojima korisnici pristupaju terminalski posredstvom telefonske mreže i modema. Na korisničko-poslužničkom konceptu omogućavaju prenošenje poruka organizirano kroz elektronsku poštu i debatne (news) grupe, te prijenos datoteka. Pojavom Interneta gube na popularnosti.
  - \* **Javne terminalske mreže** (npr. AOL, America On Line, CompuServe) su u početku radile kao veliki BBS sustavi, a danas su to mreže koje osiguravaju pristup Internetu (Internet Provider). Osnovno im je pružanje usluge elektronske pošte i WWW stranica, te telefonskog pristupa Internetu svojim korisnicima. U posljednje vrijeme, nude se i posebni pretplatnički priključci velikih kapaciteta (ADSL, Asymmetrical Digital Subscriber Loop) za stalnu vezu s Internetom.
  - \* **Interaktivne baze podataka**, npr. videotekst (modemski) i teletekst (preko TV prijemnika). Korisniku se omogućava pristup podacima u bazi, te ponekad slanje vlastitih podataka. Videotekst sustav gubi važnost razvojem Interneta, dok teletekst postaje standardni sustav jednosmjernih informacija odašiljanih za vrijeme sinkro impulsa TV slike.

- \* **Javne paketske preže**, npr. X.25 (HT CroPac), izgrađene su s namjerom pružanja usluge prijenosa podataka. Nedostatak korisničkih usluga ograničio je njihovo širenje, a pojavom Interneta polako gube na značenju.
- \* **Internet** - danas je jedina globalna mreža za prijenos podataka, koja umrežava milijune računala i pokriva cijeli svijet. Organizirana je kao mreža svih mreža. Nema vlasnika ni centralizirano upravljanje, osim velikih dobrovoljnih organizacija za poslove administracije. Svojom tehnologijom zadovoljava korisnike i dovoljno je jeftina za masovnu upotrebu. Prednost joj je u dobro definiranim mrežnim uslugama, kao što su WWW, elektronska pošta, prijenos datoteka (FTP) i terminalski pristup računalima (TELNET).

#### 2.1.1.5 Podjela mreža prema obuhvatu područja

- **Lokalne mreže** (LAN, Local Area Network) povezuju računala unutar jedne prostorije ili zgrade, te tvorničkog kruga ili sveučilišnog kampusa. Karakterizira ih velika brzina prijenosa i malo kašnjenje. Koriste se sabirničke (Ethernet), prstenaste (Token Ring) i kombinirane (Token Bus) mreže, od kojih je najrašireniji Ethernet. Mreže lokalno povezanih terminala mogu se smatrati lokalnim mrežama.
- **Gradske mreže** (MAN, Metropolitan Area Network) povezuju računala na jednom manjem teritoriju, npr. na području većeg grada. To su uglavnom javne mreže koje velikom broju korisnika omogućavaju pristup Internetu. Imaju manji kapacitet nego lokalne mreže, a kašnjenje im je osrednje. Grade se korištenjem tehnologija korisničkih i globalnih mreža.
- **Globalne mreže** (WAN, Wide Area Network). Povezuju računala razmještena na velikim udaljenostima, reda veličine 100 i više km, i na velikom teritoriju, jedne ili više država, koje ne moraju biti na istom kontinentu. To su javne mreže izgrađene telekomunikacijskom tehnologijom, ranije koristeći PCM sustave telefonske mreže, a danas optičke kanale i ATM tehnologiju. Karakterizira ih manja do velika (ATM) brzina prijenosa i veliko kašnjenje.

#### 2.1.2 OSNOVNA SVOJSTVA MREŽE

Javne i veliki dio privatnih mreža trebale bi imati sljedeća svojstva:

- **Otvorenost** - dostupnost svim potencijalnim korisnicima, pod pojmom otvorenosti podrazumijeva se danas javnost specifikacija, koja omogućuje raznim proizvođačima ponudu kompatibilne opreme;
- **Generalnost** - u smislu povezivanja raznorodnih sustava, kako bi zadovoljile sve zahtjeve na određenom području;
- **Ekonomičnost** - ekonomičnost se mjeri za dva parametra: koliko je mreža ekonomična sa stanovišta korisnika, a koliko sa stanovišta same mreže (da bi funkcionirala i financirala vlastiti razvoj).
- **Modularnost** - mogućnost naknadnog uključivanja nekih sustava. Modularnost je povezana s ekonomičnošću, jer omogućava etapnu izgradnju.
- **Fleksibilnost** - mogućnost promjene načina povezivanja (strukture) u toku rada same mreže.
- **Elastičnost** - mogućnost povezivanja s drugim mrežama;
- **Adaptivnost** - takav način upravljanja samom mrežom da se postigne maksimalna kakvoća prema korisniku. Prije se smatralo da je to mogućnost povezivanja opreme raznih proizvođača.
- **Transparentnost** - mora postojati jedinstvena tehnologija, koja povezuje korisnike na mreži;
- **Integralnost** - prije se tražila, a danas se podrazumijeva mogućnost integracije različitih informacijskih struktura, odnosno mogućnost da se u mrežu uključe različiti korisnici.

Od svih mreža danas, ove zahtjeve zadovoljava samo Internet.

#### 2.1.3 VRSTE KOMUTACIJE (PROSPAJANJA)

Komutacija ili prospajanje je postupak kojim se informacija korisnika prenosi s kraja na kraj mreže. Razlikujemo prospajanje kanala, poruka i paketa.

- **Komutacija kanala.** Najviše se koristi u telefonskim mrežama. U komutacijskom centru (telefonska centrala) vodovi se povezuju tako da se uspostavi cjelovit komunikacijski kanal s kraja na kraj mreže. Korisnicima je tada na raspolaganju čitav kapacitet kanala, bez obzira da li ga oni u tom času koriste

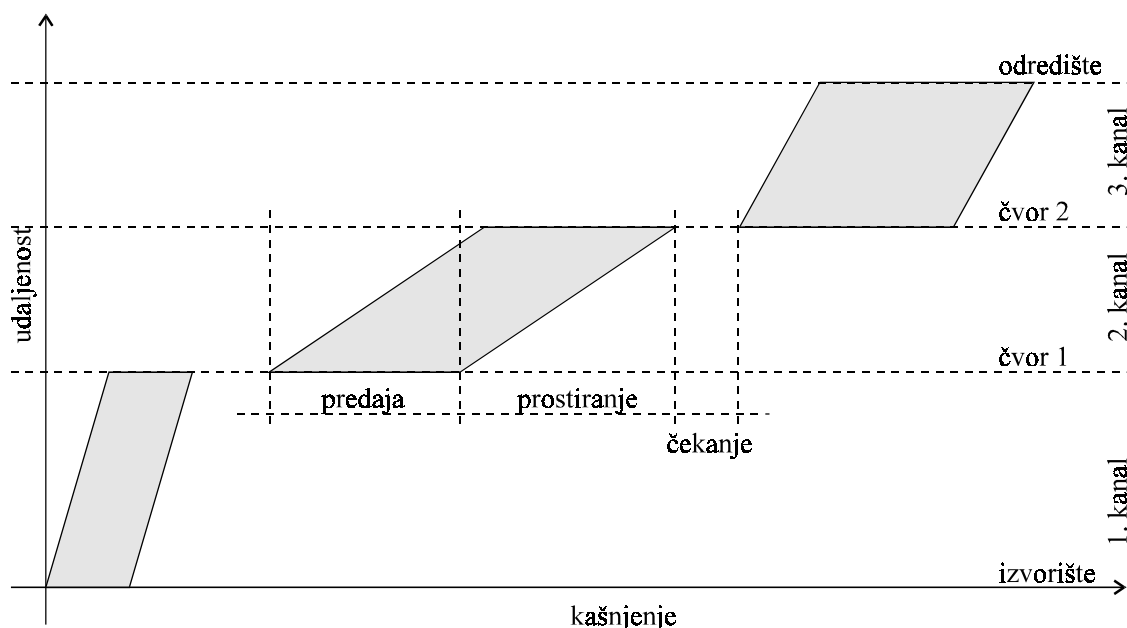
ili ne. Drugi korisnici ne mogu raspolagati tim kapacitetom. Kada korisnici to odluče, veza se raskida, spojni putovi se oslobađaju, a nove veze mogu koristiti oslobođene kapacitete. Ako je pozvani učesnik zauzet, ili ako je zauzet neki od spojnih putova do njega, učesnik koji poziva mora ponavljati poziv tako dugo, dok se ne oslobodi spojni put, čime se gubi vrijeme na uspostavljanje veze. Česti ponovljeni pozivi opterećuju telefonsku centralu.

Kada se veza jednom uspostavi, vrijeme kašnjenja načelno je jednako vremenu prostiranja (propagacije) na kanalima, jer je veza direktna. Ipak, kod složenih telefonskih mreža koje koriste izvedene digitalne kanale, postoji i dodatno kašnjenje potrebno za analogno-digitalnu i digitalno-analognu pretvorbu, te za sinkronizaciju među dijelovima mreže. Ukupno malo kašnjenje, osim kod satelitskih veza, pogodno je za govorne komunikacije.

Komutacija kanala nije pogodna za prijenos podataka zbog nedovoljne iskorištenosti kapaciteta kanala (kanal je na raspolaganju samo izvornim učesnicima), te zbog dugačke i neizvjesne procedure prospajanja. Pojedini korisnik na jednom priključku može ostvariti samo jednu vezu. Masovno se, međutim, koristi telefonska mreža s komutacijom kanala za pristup mrežama za prijenos podataka.

- **Komutacija poruka.** Mreže s komutacijom poruka primaju poruke (koje mogu sadržavati tekst ili računalne podatke) u komutacijskim čvorištima. Tu se poruke privremeno pohrane, a zatim šalju dalje do odredišta na osnovu podataka o poruci, koji se nalaze u njenom zaglavlju. Između pošiljaoca i primatelja ne uspostavlja se neposredna veza. Čvorište usmjerava poruke prema odredištu, provjerava ispravnost prenesenog sadržaja, te obavještava pošiljaoca o sudbini poruke.

Kašnjenje na mrežama s komutacijom poruka je veliko, pa nisu pogodne za prijenos govora. Ono se sastoji od vremena prijenosa i vremena prostiranja na svim spojnim putovima do odredišta, uvećano za vrijeme čekanja poruke u čvorovima, slika 2.4. Pri tome je u primjeru prvi kanal velike brzine i malog kašnjenja (lokalna mreža), drugi srednje brzine i velikog kašnjenja (globalna mreža), a treći je male brzine i kašnjenja (lokalna modemska veza).



*Slika 2.4. - Kašnjenje kod komutacije poruka*

Prijenos podataka komutacijom poruka ima prednost pred komutacijom kanala, jer ne postoji potreba za uspostavljanjem fizičkog puta između pošiljaoca i primatelja. Poruke se primaju u centru bez obzira da li su spojni vodovi do primatelja slobodni ili nisu. Danas se mreže s komutacijom poruka ne grade kao samostalne mreže, već se komutacija poruka pruža kao jedna od usluga u mrežama s komutacijom paketa (npr. elektronička pošta).

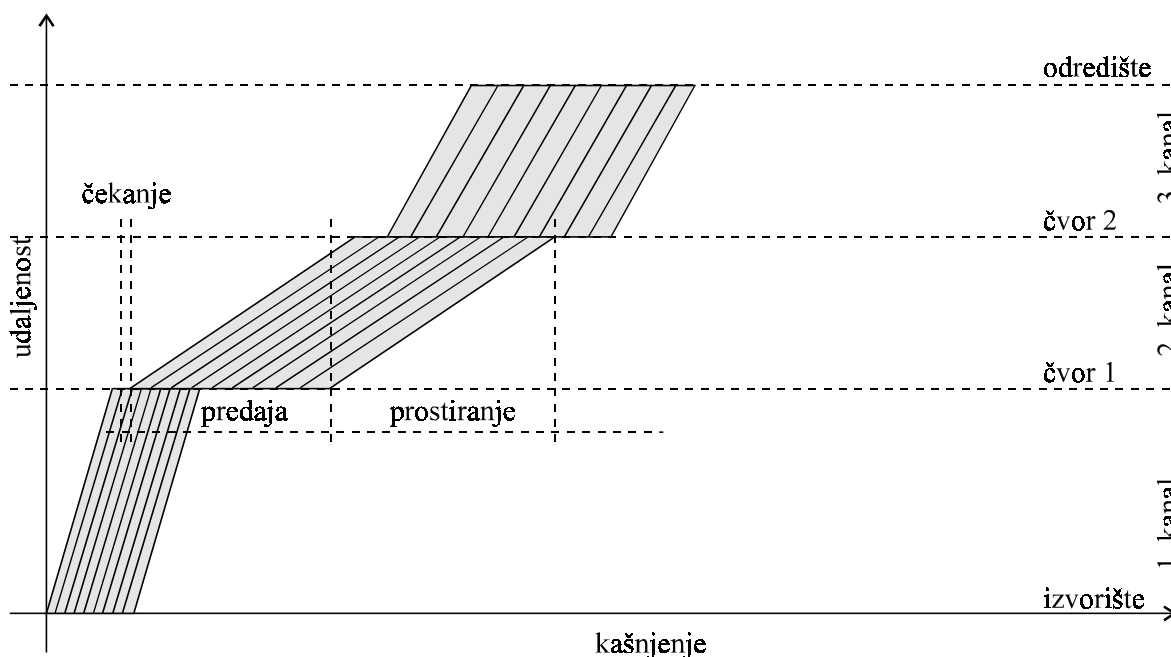
- **Komutacija paketa.** Poruke korisnika dijele se na pakete, koji se prenose kroz mrežu. Kad paket dođe u čvor, šalje se što je moguće prije prema odredištu, kako bi kašnjenje bilo minimalno. Razlikujemo usmjeravanje i prosljeđivanje paketa, a prosljeđivanje je moguće organizirati na dva načina, prosljeđivanjem pojedinačnih paketa ili korištenjem virtualnog kanala.

Algoritmima usmjeravanja određuje se optimalni put paketa prema odredištu. Nažalost, ovi algoritmi zahtijevaju veliku količinu obrade, pa ih nije moguće primijeniti na svaki pojedinačni paket. Stoga se, korištenjem algoritama usmjeravanja, periodički proračunavaju tablice usmjeravanja, a pojedinačni paketi se prosljeđuju na osnovu tih tablica.

Kod prosljeđivanja svakog paketa zasebno, on u svome zaglavlju mora nositi globalnu adresu odredišta. Teoretski svaki paket se može slati zasebnim putem, dok u praksi većina paketa neke veze ide istim putem, prema relativno stabilnim tablicama usmjeravanja. Mogućnost biranja alternativnih putova osigurava visoku sigurnost dolaska paketa na odredište.

Kod prosljeđivanja korištenjem virtualnog kanala, samo prvi paket veze nosi globalnu adresu odredišta. Prolaskom tog paketa i njegove potvrde kroz mrežu uspostavlja se virtualni kanal, kao put kojim se prosljeđuju svi ostali paketi te veze. Prosljeđivanje je vrlo jednostavno, a štedi se i na veličini zaglavlja, jer ostali paketi nose u zaglavlju samo kratke indikatore virtualnog kanala. Sigurnost dolaska paketa na odredište je smanjena, jer kvar na dijelu mreže kojim prolazi virtualni kanal zahtjeva uspostavu novog virtualnog kanala.

Kašnjenje se kod mreža s komutacijom paketa sastoji od vremena predaje, vremena prostiranja i vremena čekanja. Međutim, ovdje nije potrebno čekati prijem cjelokupne poruke, već primljeni paket odmah prosljeđujemo dalje, slika 2.5. Time je ukupno vrijeme kašnjenja poruke skraćeno u odnosu na kašnjenje kod mreža s komutacijom poruka.



*Slika 2.5. - Kašnjenje kod komutacije paketa*

Međutim, daleko važnija posljedica dijeljenja poruke na pakete je u poboljšanju podjele kapaciteta mreže među korisnicima statističkim multipleksiranjem. Kod komutacije poruka, potrebno je čekati da mreža prenese sve poruke u redu čekanja. Kod komutacije paketa, paketi raznih korisnika šalju se naizmjenično, pa je moguće mnogo pravednije zajedničko korištenje kapaciteta kanala. Osim toga, kratki paketi su manje osjetljivi na pogreške u prijenosu, a ponovno slanje (retransmisija) oštećenog paketa je mnogo efikasnije od ponovnog slanja čitave poruke.

- **ATM mreže** se razvijaju sa svrhom integracije prijenosa govora, multimedijских signala i podataka. ATM mreža je zapravo mreža s komutacijom paketa, kod koje se poruke korisnika dijele u male pakete fiksne duljine, nazvane ćelije ili stanice (engl. cell). Ćelije su dovoljno male (53 okteta = 5 okteta zaglavlja, od čega je 1 zaštite, + 48 okteta podataka) kako bi se prosipanje moglo obavljati sklopovljem, te kako bi početno kašnjenje bilo maleno, čime je omogućen prijenos govora.

#### 2.1.4 OSNOVNI STANDARDI

Kod izgradnje računalnih mreža vrlo je značajna standardizacija svih funkcionalnih, mehaničkih i električnih karakteristika opreme. Jedino na taj način uređaji različitih proizvođača i različitih vlasnika, a smješteni na raznim stranama svijeta, mogu uspješno i ekonomično međusobno komunicirati. Standarde donose nacionalne ili međunarodne organizacije za standardizaciju. Međutim, kako je napredak tehnologije često brži od formalna procedure standardizacije, sami proizvođači opreme novim produktima postavljaju tzv. de fakto, interne ili industrijske standarde. Nakon početne faze burnog razvoja, nova tehnologija se naknadno formalno standardizira.

Interne standarde donose pojedine tvrtke ili njihova udruženja (konzorciji), npr.

- \* EIA (Electronics Industries Association USA), standardizira sučelje RS232
- \* LIM (Lotus Intel Microsoft USA), poznata specifikacija proširenja memorije PC-XT računala
- \* ATM - Forum, udruženje proizvođača ATM opreme, aktivno u donošenju niza standarda
- \* VESA, udruga proizvođača grafičkih kartica
- \* ISA (Industry Standard Organization), standardizira sabirnicu PC-AT računala umjesto IBM-a
- \* PCMCIA, konzorcij koji donosi standarde za povezivanje perifernih uređaja u obliku kartica
- \* INTEL, proizvođač 80x86 procesora, standardizira PCI sabirnicu PC računala
- \* IEEE (Institute of Electrical and Electronic Engineering), institut udruženja elektrotehničara čiji su standardi prihvaćeni kao međunarodni, standardizira lokalne mreže (802.x).

Formalne standarde donose međunarodne i nacionalne organizacije, npr.

- \* ISO (International Standardization organization), najčešće formalizira ranije postavljene interne standarde, poznata specifikacija ISO-OSI referentnog modela mrežne arhitekture
- \* ITU - T (International Telecommunications Union - Telecommunications, ranije CCITT), donio niz važnih preporuka s područja telekomunikacija, npr. V preporuke za prijenos podataka preko analogne mreže (modemi), X preporuke za prijenos podataka preko digitalne mreže (X.25 paketna mreža), I preporuke za integrirane mreže (ISDN, među njima i ATM)
- \* ANSI (American National Standardization Institute USA), donio niz standarda sa područja računarstva
- \* NBS (National Bureau of Standardization USA), federalna organizacija za standarde USA.

## 2.2 ELEMENTI RAČUNALNIH MREŽA

Mreže gradimo od kanala, čvorišta i terminala. To su elementi mreža. U samoj mreži imamo čvorišta, posebna računala koja usmjeravaju podatke do odredišta, te kanale koji povezuju čvorišta. Terminali su uređaji povezani na mrežu. Oni mogu biti računala ili terminali u užem smislu.

### 2.2.1 KANALI

#### 2.2.1.1 Podjela prema vrsti fizičkog medija

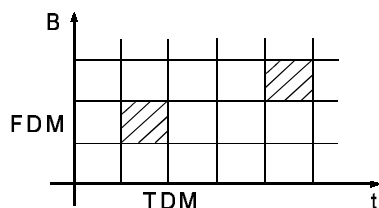
- **Vodovi** su strukture sastavljene od dvaju ili više vodiča, npr.
  - \* **parica** (UTP, Unshielded Twisted Pair) - sastoji se od dva prepletana vodiča. Koristi se za pretplatničke telefonske mreže (brzine do 56000 b/s), te kod lokalnih mreža, npr. Ethernet (10BT brzine 10 Mb/s i 100BTX brzine 100 Mb/s);
  - \* **koaksijalni kabe**li - sastoje se od centralnog vodiča i cilindričnog opleta, primjenjuju se kod mreža kableske TV i Ethernet lokalne mreže (10B2 i 10B5 brzine 10 Mb/s);

- \* **oklopljena parica** (STP Shielded Twisted Pair, FTP Foil-shielded Twisted Pair) - sastoji se od dva prepletena vodiča i cilindričnog opleta, koji može biti i folijski. Koristi se kod novijih instalacija lokalnih mreža.
  - \* **twinax kabe**li - sastoje se od dva centralna vodiča i cilindričnog opleta, primjenjuju se kod prstenastih lokalnih mreža, npr. IBM 16 Mb/s.
  - **Optički vodovi** (svjetlovodi) su strukture od vodljive plastike kroz koje se vodi svjetlosni signal. Imamo dvije vrste optičkih vodova:
    - \* **jednomodno optičko vlakno** omogućava prolaz svjetlosti koja se lomi na samo jedan način. Karakterizira ga manje gušenje i veći doseg signala (oko 15 km), ali i veća cijena vlakna, konektora i opreme. Koristi se za gradnju telekomunikacijskih i WAN mreža.
    - \* **višemodno optičko vlakno** omogućava prolaz svjetlosti koja se lomi na više načina. Karakterizira ga veće gušenje i manji doseg signala (oko 2 km), ali i manja cijena vlakna, konektora i opreme. Koristi se za gradnju LAN mreža.
- Koriste se kod optičke lokalne mreže FDDI (Fiber Distributed Data Interface, brzine 100 Mb/s), ATM korisničkih priključaka i mreža (brzine 48/38 Mb/s, 155 Mb/s i 625 Mb/s) i Ethernet lokalne mreže (10BFL brzine 10 Mb/s i 100BFX brzine 100 Mb/s).
- **Elektromagnetska zračenja** imaju različita svojstva ovisno o frekvenciji signala:
    - \* **infracrvena zračenja**, koriste se za bežično povezivanje unutar jedne prostorije (npr. bežična tastatura),
    - \* **radio kanali**, koriste se za prijenos podataka na područjima gdje nije izgrađena telefonska mreža, ili za mobilne komunikacije (npr. GSM),
    - \* **satelitske veze**, koriste se kao medij za izgradnju telekomunikacijskih mreža.

### 2.2.1.2 Vrste kanala

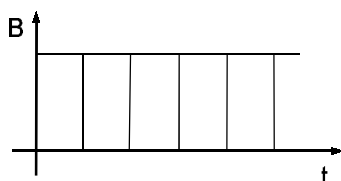
Kanal je spojni put kojim prenosimo podatke. Sastoji se od fizičkog medija i potrebne opreme da bi prijenos podataka bio moguć. Razlikujemo osnovne i izvedene kanale.

- **Osnovni kanal** nastaje potpunim korištenjem kapaciteta fizičkog voda ili medija. Pri tome je najčešće obuhvaćena i istosmjerna komponenta spektra, pa govorimo o osnovnom frekvencijskom području (baseband), od 0 do neke granične frekvencije. Informacijski volumen osnovnog kanala možemo podijeliti na više korisnika, čime dobijemo izvedene kanale.
- **Izvedeni kanali** nastaju podjelom informacijskog volumena osnovnih kanala. Pojedinom korisniku se može fiksno dodijeliti cijeli kapacitet osnovnog kanala u vremenu  $t$  (TDM, Time Domain Multiplexing), ili dio njegovog frekvencijskog opsega (FDM, Frequency Domain Multiplexing), ili kombinirano, slika 2.6.



Slika 2.6. - Kombinirana fiksna podjela po vremenu i frekvenciji

Uređaji za podjelu po frekvenciji su vrlo nefleksibilni zbog nemogućnosti jednostavne promjene frekvencije LC filtera. Fleksibilnija je podjela po vremenu (TDM), slika 2.7.



Slika 2.7. - Podjela po vremenu (TDM)

Podjelu kanala po vremenu nazivamo vremensko multipleksiranje. Ono može biti fiksno i statističko.

Kod **fiksnog multipleksiranja** točno se zna koji je vremenski odsječak predviđen za terminal  $T_1$ , koji za terminal  $T_2$ , itd. Dok traje odsječak predviđen za  $T_1$ ,  $T_1$  prenosi podatke, a kada to vrijeme prođe,  $T_1$  prekida rad i tada počinje raditi  $T_2$ . Mana fiksnog multipleksiranja je u tome, što je raspoloživo vrijeme kanala izgubljeno ako ga terminal ne koristi (npr. trenutno nema podataka za slanje).

Kod **statističkog multipleksiranja** vremenski odsječci nisu fiksno dodijeljeni. Stoga terminal  $T_1$  može npr. koristiti cijeli kapacitet kanala kad  $T_2$  ne radi, i obrnuto. Dok jedan terminal radi, drugi mora čekati. Situacija se poboljšava podjelom poruka na manje dijelove, blokove ili pakete. Karakteristika multipleksiranja je da je kapacitet izlaznog kanala jednak kapacitetu svakog pojedinog ulaznog kanala.

Uređaj za fiksno multipleksiranje se naziva multiplekser. On promet sa više ulaznih medija prebacuje na jedan izlazni medij čiji je kapacitet fiksno podijeljen. Stoga ukupni kapacitet izlaznog medija mora biti veći ili jednak zbroju kapaciteta ulaznih:

$$\text{kapacitet} \geq \sum_i k_i$$

Uređaj za statističko multipleksiranje se naziva se statistički multiplekser. On promet sa više ulaznih medija prebacuje na jedan izlazni medij čiji je kapacitet podijeljen prema podjeli korisnika. Iako dugoročno ukupni promet mora biti manji ili jednak kapacitetu izlaznog medija, aktivnom korisniku se privremeno dodjeljuje puni kapacitet medija. Stoga je kapacitet izlaznog medija jednak kapacitetu pojedinačnog ulaznog medija:

$$\text{kapacitet} = k_i$$

Statističko multipleksiranje se može koristiti kod komutacije kanala. Koncentrator koristi povremenu aktivnost terminala (telefona). Kapacitet izlaznog medija (npr. 5 telefonskih kanala) je znatno manji od kapaciteta ulaznih medija (npr. 50 telefonskih kanala):

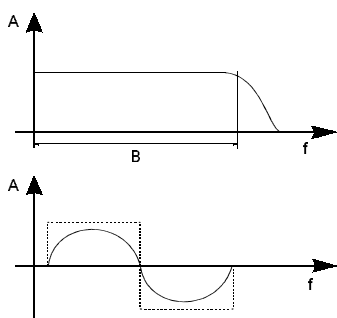
$$\text{kapacitet} < \sum_i k_i$$

Koncentrator dodjeljuje izlazne kanale aktivnim terminalima po principu "tko prvi dođe, prvi je poslužen". Kad su svi izlazni kanali angažirani, nova se veza ne može uspostaviti dok se neki od kanala ne oslobodi raskidom postojeće veze.

### 2.2.1.3 Kapacitet kanala.

Na fizičkoj se razini računarska mreža izravno dodiruje sa prijenosnim medijem. To mogu biti osnovni ili izvedeni kanali izgrađeni za prijenos govora ili podataka. Sam prijenos može biti analogan ili digitalan. Često se za prijenos podataka koriste telefonski kanali.

Kod stvarnih medija, kao što su vodovi, gušenje raste porastom frekvencije signala zbog porasta gubitaka u izolaciji. Postoji neka gornja upotrebljiva frekvencija na kojoj je prijenos signala još uvijek ekonomičan, pa smatramo da se vod ponaša kao niskopropusni filter. Signal koji je propušten kroz niskopropusni filter širine frekvencijskog pojasa  $B$ , može se potpuno obnoviti ako se načini  $2B$  uzoraka u sekundi, slika 2.8. To znači da kanalom širine pojasa  $B$  možemo prenijeti  $2B$  uzoraka, koje nazivamo signalizacijskim simbolima.



Slika 2.8. - Propuštanje signala kroz niskopropusni filter



Kapacitet kanala se najčešće izražava u b/s (bita u sekundi), a za brzinu signalizacije jedinica je Bd (baud, čita se bod, simbola u sekundi). Ako se signal prenosi sa R diskretnih razina, vrijedi:

$$k = B \cdot \log_2 R$$

gdje je  $B$  brzina signalizacije, izražena u simbol/sekunda (Bd). Ako se signalnim elementom prenosi 1 bit, numerička vrijednost b/s i bauda je ista. Najveći mogući kapacitet kanala širine pojasa B iznosi:

$$k = 2B \cdot \log_2 2 = 2B \text{ [b/s]}$$

Ako se uzme idealan bešumni kanal širine pojasa  $B = 3000$  Hz (telefonski kanal), tada se uz dvorazinski prijenos ( $R = 2$ ) može postići najviši kapacitet:

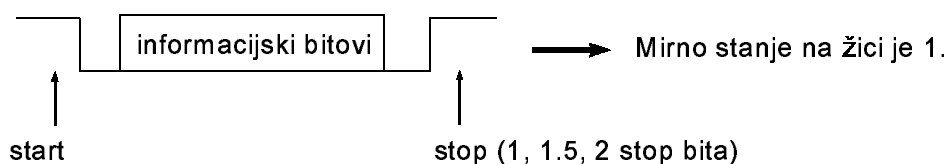
$$k = 2 \cdot 3000 \cdot \log_2 2 = 6000 \text{ [b/s]}$$

Danas se koriste višerazinske modulacije. Za telefonski kanal brzina prijenosa ide do 38000 b/s, odnosno do 56000 b/s za lokalni telefonski priključak prema digitalnoj centrali.

#### 2.2.1.4 Vrste sinkronizacije

Sinkronizacija se odnosi na prepoznavanje početka i kraja prijenosa nekog elementa informacije. Pri tome moramo računati da se radi o prijenosu podataka među uređajima koji su geografski udaljeni, te proizvedeni od različitih proizvođača. Kanali mogu biti sinkroni i asinkroni.

Kod **asinkronog prijenosa**, slika 2.9, podatak (znak) je “uokviren” sa pokretačkim (start) i zaustavnim (stop) bitom. Startni bit je 0, nakon njega dolaze bitovi podatka, eventualno paritetni bit, a onda jedan ili više stop bitova 1. Stanice koje žele komunicirati moraju unaprijed dogovoriti brzinu, ali je zbog kratkoće poruke dozvoljeno nekoliko postotaka odstupanja brzine. Ovakav način prijenosa istovremeno osigurava sinkronizaciju i po bitu i po oktetu (znaku).



Slika 2.9. - Asinkroni prijenos podataka

Kod **sinkronog prijenosa**, osim samih podataka, kanalom se prenosi i takt signala. Time je definiran trenutak uzorkovanja signalizacijskog elementa, ali ne i početak okteta (znaka). Sinkroni prijenosa osigurava samo sinkronizaciju po bitu.

#### 2.2.1.5 Načini prijenosa po smjeru

Po smjeru prijenosa razlikujemo dvosmjerne, obosmjerne i jednosmjerne kanale.

**Dvosmjerni kanal** (duplex) omogućava istovremeni prijenos podataka u oba smjera.

**Obosmjerni kanal** (half duplex) omogućava prijenos podataka u oba smjera, ali u različitim vremenskim odsječcima. Unutar tih odsječaka prijenos je jednosmjernan.

**Jednosmjerni kanal** (simplex) omogućava prijenos podataka u samo jednom smjeru. Za postizanje dvosmjernog prijenosa koriste se dva jednosmjerna kanala.

### 2.2.2 ČVORIŠTA MREŽE

Čvorišta razlikujemo prema razini hijerarhijske strukture na kojoj rade, te prema broju priključaka (2 ili više). Imamo tako obnavljače i zvijezdišta, prenosnike i prospojnice, usmjernike i poveznike.

**Obnavljač** (repeater) je uređaj s dva, a **zvijezdište** (hub) s više priključnica, koji samo pojačava signal i obavlja prilagodbu impedancije. Koriste se na fizičkoj razini za proširenje doseg mreže (obnavljač) ili za povezivanje više kablinskih segmenata u jednu višespojnu (sabirničku) strukturu.

**Premosnik** (bridge) je uređaj s dva, a **prospojnik** (switch) s više priključnica, koji prima okvir protokola podatkovne razine i prosljeđuje ga prema odredištu. Funkcija filtriranja sa samoučenjem efikasno dijeli promet na segmente mreže, i time omogućava povećanje propusnosti mreže.

**Usmjernik** (router) je uređaj koji prima pakete mrežne razine i nekim ih od algoritama prosljeđivanja i usmjeravanja šalje prema odredištu. Raspolaze znanjem o dostupnosti svih dijelova mreže.

**Poveznik** (gateway) je uređaj koji povezuje dvije raznorodne mreže, te pri tome obavlja prevođenje protokola mrežne i prijenosne razine.

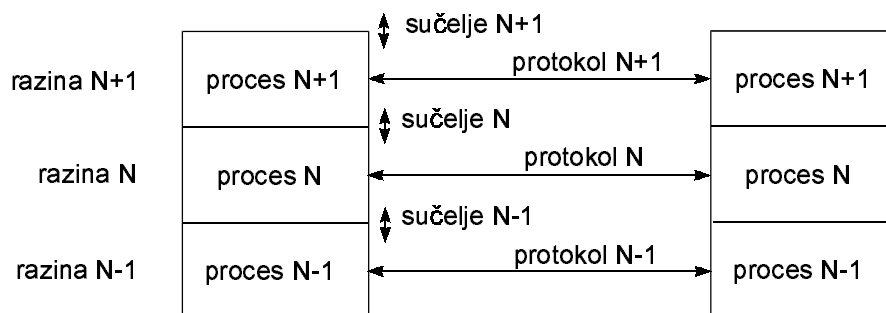
### 2.2.3 TERMINALI MREŽE

Pod pojmom terminal mreže podrazumijeva se svaki uređaj koji je spojen na mrežu. To mogu biti računala i terminali u užem smislu (inteligentni i neinteligentni).

Kod računalnih mreža često se sama računala koriste kao čvorovi (npr. svako UNIX računalo može biti usmjernik ako je povezano na dva segmenta mreže). Takva računala obavljaju istovremeno funkciju čvorišta i terminala mreže.

## 2.3 HIJERARHIJSKI SUSTAVI

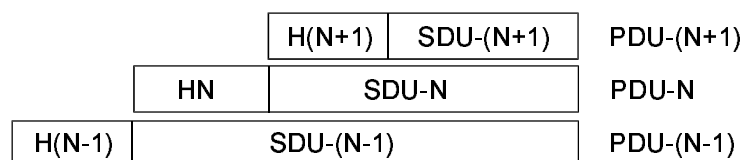
Današnje mreže imaju slojevitú hijerarhijsku arhitekturu, slika 2.10:



*Slika 2.10. - Slojevita hijerarhijska struktura*

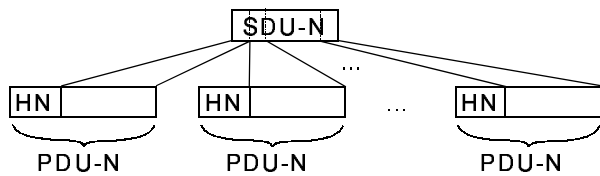
Na jednom uređaju mreže, čvorištu ili računalu, obavljaju se funkcije više razina. Za svaku razinu pokreće se proces koji komunicira sa susjednima (nadređenim i podređenim) preko sučelja (engl. interface). Proces razine N+1 traži uslugu prijenosa podataka od razine N, koja komunicira s korespondentnim procesom druge stanice prema pravilima protokola N. Pri tom razina N koristi usluge razine N-1. Stvarni tok podataka odvija se putem sučelja među susjednim razinama na istom računalu, te komunikacijskim medijem prema udaljenom računalu.

Proces N generira jedinicu informacije PDU (Protocol Data Unit) dodavanjem zaglavlja N korisnikovoj informaciji SDU (Service Data Unit). PDU(N) šalje se preko sučelja N-1 podređenoj razini kao SDU(N-1). Proces N formira SDU(N) odvajanjem zaglavlja sa primljenih PDU, te ga prosljeđuje nadređenoj razini preko sučelja N. Za proces N+1, SDU(N) ima značenje PDU(N+1), slika 2.11:



*Slika 2.11. - Jedinice informacije i dodavanje zaglavlja*

Tijekom pripreme poruke za prijenos na odredište, može se obaviti i dijeljenje (fragmentacija) poruke prema pravilima upotrijebljenog protokola, slika 2.12:



Slika 2.12. - Fragmentacija informacije

Koncepti na kojima se zasnivaju hijerarhijski sustavi su koncept razine, koncept sučelja, koncept protokola, koncept zaglavlja, koncept fragmentacije.

- \* po **konceptu razine**, procesi te razine kroz međusobnu komunikaciju pružaju nadređenoj razini uslugu prijenosa podataka, koristeći pri tome usluge podređene razine. Možemo reći da proces promatrane razine proširuje uslugu podređene razine i tako proširenu pruža je nadređenoj razini.
- \* po **konceptu sučelja**, komunikacija među procesima susjednih razina unutar istog uređaja odvija se preko sučelja. Specifikacija sučelja može biti interna stvar proizvođača računala, ali danas je većina sučelja javno specificirana po principu otvorenosti. Na taj način sustav se može izgraditi korištenjem programskih rješenja i sklopovlja različitih proizvođača.

Kroz sučelje može prolaziti više tokova podataka. Kako bi se identificirao stvarni korisnik informacije, upotrebljava se mehanizam pristupnih točaka (SAP, service access point). To su programski kanali kojima procesi u računalu međusobno komuniciraju. Kod otvaranja kanala dodjeljuje se identifikacijski broj, čijom je upotrebom jednoznačno određen korisnik informacije. Identifikacijske brojeve moguće je dodjeljivati dinamički prema potrebi, ili trajno. Iako dio mehanizma sučelja, identifikatori pristupnih točaka su dio specifikacije protokola.

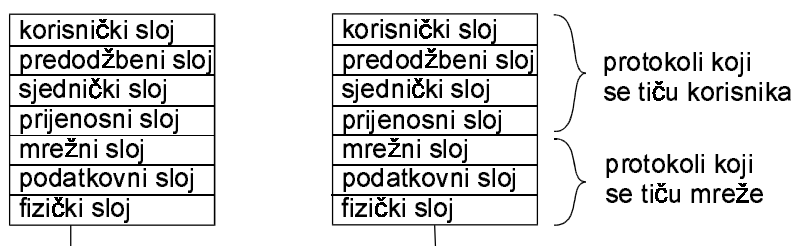
- \* po **konceptu protokola**, na uređajima koji međusobno razmjenjuju podatke, dva procesa iste razine prividno neposredno komuniciraju po pravilima protokola. Oni u stvarnosti komuniciraju koristeći usluge podređenih razina. Stvarni tok podataka i upravljačkih informacija prolazi kroz sučelje. Specificiranje protokola je osnovni način standardizacije komunikacijskih sustava.
- \* po **konceptu zaglavlja**, svaka razina u postupku predaje uzima preko sučelja  $PDU(N+1)$  nadređene razine kao podatke koje treba prenijeti,  $SDU(N)$ , bez ikakvog saznanja o njihovom sadržaju, te im dodaje svoje zaglavlje  $H(N)$ . Tako formira vlastitu jedinicu informacije  $PDU(N)$ , koju šalje sučeljem podređenoj razini. U postupku prijema, razina dobije od podređene razine preko sučelja njen  $SDU(N-1)$  kao svoj  $PDU(N)$ . Nakon korištenja podataka iz zaglavlja, odbacuje zaglavlje  $H(N)$  i dobiveni  $SDU(N)$  šalje sučeljem ka nadređenoj razini. Tu  $SDU(N)$  ima značenje  $PDU(N+1)$ , s tom razlikom da proces  $N+1$  znade sadržaj zaglavlja  $H(N+1)$ .
- \* po **konceptu fragmentacije**, svaki  $SDU(N)$  može u postupku formiranja  $PDU(N)$  biti podijeljen na manje dijelove, tako da od jednog  $SDU(N)$  formiramo jedan ili više  $PDU(N)$ . Pri tome svaki  $PDU(N)$  sadrži, naravno, cjelovit zaglavlje  $H(N)$ . U praksi se, međutim, fragmentacija koliko je to god moguće izbjegava. Dijeljenje  $PDU$  na manje dijelove izaziva veće opterećenje čvorišta funkcijama usmjeravanja, a detekcija pogriješke i gubitka  $PDU$  je otežana. Gubitak jednog fragmenta može značiti gubitak čitavog  $PDU$ . Posebno kod mreža s pojedinačnim usmjeravanjem paketa, kada redosljed pristizanja nije zagarantiran, čvorište mora dosta dugo čekati na izgubljeni fragment prije donošenja konačne odluke da je čitavi  $PDU$  izgubljen. Zbog toga se nastoji korisnikova poruka odmah podijeliti na onolike dijelove, koji nakon uključivanja zaglavlja svih podređenih razina, bez daljnje fragmentacije mogu proći kroz mrežu. Npr. kod Interneta, predajnik pokušava odrediti maksimalnu duljinu fragmenta  $MSS$  (Maximum Segment Size) po posebnom postupku.

Jedinice informacije mogu biti pojedini bitovi, okteti (znakovi), okviri (ili blokovi, blok se sastoji od više okteta), paketi, segmenti, datagrami i poruke.

- \* **bit** (binarna znamenka) je najmanja jedinica informacije koju prenosimo na fizičkoj razini. Kanalom prenosimo vremenski niz signalizacijskih elemenata (serijski prijenos), od kojih svaki može nositi jedan ili više bita. Signal na kanalu može biti oblikovan tako, da osim signalizacijskih elemenata prenosi i taktni signal potreban za njihovo pravovremeno uzorkovanje.

- \* **oktet** (znak) je najmanja kodna riječ, kojom baratamo kao cjelinom. Najčešće PDU podatkovne razine (blok, okvir) nakon serijsko-paralelne pretvorbe pamtimo u memoriji kao niz okteta. Iako su moguće i druge duljine kodne riječi, danas se je ustalilo korištenje okteta zbog organizacije memorije računala, čija je širina kodne riječi višekratnik od osam bita. Kod asinkronog prijenosa, sinkronizacija po oktetu obavlja se na fizičkoj razini, a kod sinkronog na podatkovnoj. Stoga se oktet nekad obrađuje na fizičkoj, a nekad na podatkovnoj razini, u oba slučaja sklopovljem.
- \* **okvir** (blok) je osnovni PDU podatkovne razine. Sastoji se od više okteta (znakova). Njegov početak je sinkroniziran posebnom sinkronizacijskom sekvencom, koju zovemo okvirni znak. Ovo je najmanja jedinica informacije koja ima vlastito zaglavlje. U procesu predaje, okvir se iz memorije prenosi oktet po oktet na serijski vezni sklop, gdje se obavlja paralelno-serijska pretvorba. U prijemnom smjeru postupak je obrnut. Istovremeno s prijemom znakova okvira, obavlja se provjera adrese odredišta i cjelovitosti okvira. U slučaju oštećenja, okvir se odbacuje.
- \* **paket** je osnovni PDU mrežne razine, ujedno i oblik kojim se obavlja promet s kraja na kraj mreže. Obavezno sadrži identifikaciju odredišta, bilo njegovu globalnu adresu ili indikator virtualnog kanala. Nastoji se, ako je to moguće, paket prenijeti jednim okvirom podatkovne razine. Tada nije potrebna posebna sinkronizacija po paketu. Ukoliko paket fragmentiramo, potrebno je označiti okvire koji čine cjeloviti paket.
- \* **segment i datagram** su osnovni PDU prijenosne razine. Termin segment koristimo za dio veće korisnikove poruke, dok je datagram kratka zasebna poruka. Nastojimo jedan segment odnosno datagram prenijeti jednim paketom. To je najčešće moguće lako postići, jer tek na podatkovnoj razini (okvir) duljina PDU ovisi o tehnologiji korištenog kanala.
- \* **poruka korisnika** je najveći PDU, onaj koji formira proces korisnik komunikacije. To može biti kratka poruka u interaktivnom radu, blok podataka koji čini odziv neke baze podataka, datoteka s podacima ili programom, ili neki multimedijски element koji prenosimo samostalno ili kao dio veće cjeline (WEB stranica). Veće poruke fragmentiramo na segmente, a kako pri tome imamo potpunu slobodu, nastojimo odabrati duljinu segmenta koja prolazi kroz mrežu bez potrebe za daljnjim fragmentiranjem. Poruku korisnik dostavlja komunikacijskom sustavu kao cjelinu, ili u dijelovima. Veličina dijelova ovisi o kapacitetu memorijskog spremnika, a mora biti veća od optimalne veličine segmenta.

Kao referentna mrežna arhitektura koristi se ISO/OSI model od 7 razina slika 2.13:

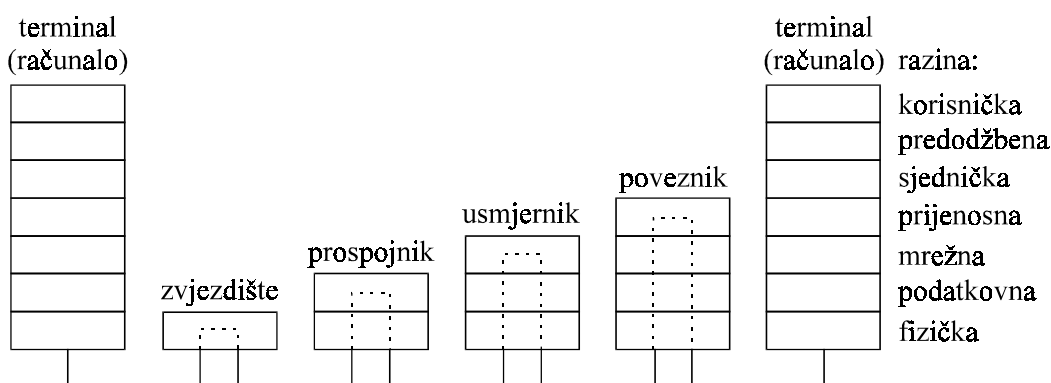


*Slika 2.13. - Razine ISO/OSI modela*

- 1) **Fizička razina** definira sučelje između računala i medija kojeg koristimo za prijenos. Specificiraju se električne, funkcionalne i mehaničke karakteristike kabela, konektora i signala, kako bismo uređaj standardno mogli priključiti na kanal. Ostvaruje se sinkronizacija po bitu ili po bitu i oktetu.
- 2) **Podatkovna razina** neposredno nadzire fizičku razinu tako da upravlja vezom ostvarenom na jednospojnom ili višespojnom mediju. Ostvaruje se sinkronizacija po okviru ili po oktetu i okviru.
- 3) **Mrežni sloj** osigurava prijenos poruke sa kraja na kraj mreže. Paketi se usmjeravaju kroz mrežu.
- 4) **Prijenosni sloj** osigurava vezu od korisnika do korisnika. Obavlja se kontrola pogriješki i kontrola toka.
- 5) **Sjednički sloj** provjerava cjelovitost poruke. Isporučuje poruku na pravo odredište unutar računala.

- 6) **Predodžbeni sloj** obavlja prevođenje informacija sa formata koji su standardni na mreži, na format standardan na terminalu.
- 7) **Korisnički sloj** poslužuje korisničke procese i mrežne usluge.

Sada možemo prikazati strukturu različitih vrsta čvorišta, slika 2.14:



*Slika 2.14. - Čvorišta prema razinama ISO/OSI modela*

Zvjezdište i prospojnik povezuju istovrsne mreže podatkovne razine. Usmjernik povezuje istovrsne mreže mrežne razine, ali segmenti podatkovne razine mogu biti različiti. Poveznik povezuje različite mreže i obavlja potrebne pretvorbe protokola.

## 2.4 KOMUNIKACIJSKI PROTOKOLI

Komunikacijski protokol je skup pravila po kojima procesi iste razine razmjenjuju jedinice informacije, PDU, u čijim zaglavljima je sadržana kontrolna informacija potrebna za obavljanje funkcije promatrane razine hijerarhijskog sustava. Treba imati u vidu da se komunicirajući procesi odvijaju na odvojenim računalima, često geografski udaljenim, tako da su primljeni PDU jedina informacija o radu korespondentnog procesa. Na osnovu primljenih PDU i sadržaja njihovih zaglavlja, ili na osnovu izostanka očekivanih PDU, komunicirajući proces treba sa što većom točnošću odrediti stanje korespondentnog procesa kako bi u svakom trenutku bio u stanju poduzeti odgovarajuće mjere, sve s ciljem pružanja usluge prijenosa podataka procesu nadređene razine.

Kako su udaljeni uređaji često u vlasništvu različitih osoba i proizvedeni od strane različitih proizvođača, od vitalnog je značaja za funkcioniranje promatrane razine, kao i mreže kao cjeline, striktno i formalno specificiranje protokola, odnosno njihovo usvajanje kao industrijskih ili međunarodnih standarda. Tek će uređaji koji su u potpunosti sukladni sa svim protokolima mreže uspješno međusobno komunicirati.

U praksi je donošenje standarda vrlo složen i mukotrpan posao. S jedne strane postoji pritisak korisnika i proizvođača da se nove, perspektivne tehnologije što prije standardiziraju radi komercijalizacije novih proizvoda. S druge strane, svaka brzopletost u donošenju standarda može rezultirati propustima u funkcionalnoj specifikaciji, čije ispravljanje kasnije može izazvati znatne nepredviđene troškove. Stoga se nove tehnologije detaljno ispituju simulacijom u laboratorijima i pokusnim radom na ispitnim mrežama, a na osnovu predloženih (draft) standarda. Nakon postizanja zadovoljavajućih rezultata donosi se formalni standard. Svaki standard je podložan naknadnim modifikacijama i usavršavanjima. Kod standardizacije komunikacijskih protokola, razlikujemo dvije grupe pravila. To su vanjska i unutarnja specifikacija protokola.

**Vanjska specifikacija** protokola odnosi se na oblik PDU kao cjeline, uključujući i format zaglavlja. U zaglavlju se definiraju polja, format podataka u njima, te značenje koje mora biti jednoznačno za sve uređaje sukladne protokolu. Jednom donesena vanjska specifikacija protokola vrlo teško se mijenja, zato jer je potrebno istovremeno obaviti korekcije na tisućama uređaja koji već koriste raniju varijantu. Najčešće je jednostavnije uvesti potpuno novi protokol. Stoga neki protokoli raspolažu s mogućnošću

korištenja dodatnih neobaveznih funkcija prema dogovoru korespondentnih procesa. Dodavanjem novih funkcija moguće je donekle ublažiti nedostatke prvobitne vanjske specifikacije protokola.

**Unutrašnja specifikacija** protokola odnosi se na pravila rada procesa, algoritme protokola, kojima se obrađuju informacije iz zaglavlja PDU i donose odluke o radu procesa. Algoritmi protokola mogu se u znatnoj mjeri naknadno modificirati, pod uvjetom da je vanjska specifikacija očuvana. Pri tome, naravno, treba očuvati i funkcionalnost protokola u cjelini. Dobar je primjer TCP protokol Interneta, čija je unutrašnja specifikacija kontinuirano mijenjana u svrhu poboljšanja kontrole toka, a da pri tom nije mijenjana vanjska specifikacija. Štoviše, ostvarena je i funkcionalna kompatibilnost uređaja koji rade po starim i novim specifikacijama.

Da bi različiti proizvođači uspješno uskladili rad svojih proizvoda s usvojenim standardima, potrebno je osigurati njihovo jednoznačno tumačenje. To osigurava formalno specificiranje protokola korištenjem posebnih formalnih jezika. To može biti govorni jezik, neki stvarni ili formalni programski jezik, ili grafički jezik dijagrama stanja.

Funkcije pojedine razine hijerarhijske strukture znatno se razlikuju i načelno su definirane ISO-OSI specifikacijom. Ipak, u obavljanju svoje funkcije komunicirajući procesi moraju voditi računa o ispravnom tumačenju primljenih PDU, o radu korespondentnih procesa, o identifikaciji PDU, o pojavi pogreški, te o usklađivanju brzine rada s mogućnostima korespondentnog procesa i mreže u cjelini. Stoga se protokol pojedine razine promatra kroz obavljanje tih pojedinačnih zadaća. Govorimo o četiri osnovna mehanizma protokola, o adresiranju, sinkronizaciji, kontroli pogrešaka i kontroli toka.

#### 2.4.1 ADRESIRANJE

Mehanizam adresiranja jednoznačno identificira korisnika. Zahtjev jednoznačnosti implicira korištenje dugačkih adresa, pa je u zaglavlju PDU potrebno osigurati polje dovoljne duljine, kako bi broj raspoloživih adresa bio dovoljan za sve korisnike u predviđenom roku uporabe protokola. Poznat je primjer nedovoljne duljine adrese IP protokola Interneta (32 bita), nastao jer nije bilo moguće predvidjeti današnji rast broja podmreža i priključenih računala. Dugačke adrese, međutim, dodatno opterećuju komunikacijski sustav jer se znatan dio kapaciteta kanala potroši na prijenos sadržaja zaglavlja. Format zaglavlja u cjelini, pa i duljina korištene adrese, kompromis su između univerzalnosti rješenja i efikasnosti protokola.

Ukupna adresa sastoji se od dijelova, koji se koriste po razinama hijerarhijske strukture. Adresiranje je moguće organizirati striktno, kada adresa nadređene razine implicira stvarne adrese svih podređenih razina. Takvo adresiranje doprinosi potpunom odvajanju funkcija pojedinih razina. Adresiranje se može koristiti i distribuirano, kada ukupnu adresu čine adrese svih razina. Ovaj pristup zahtijeva čvršću povezanost među razinama, ali omogućuje lakše upravljanje adresama i korištenje poznatih adresa za pojedine mrežne usluge.

Adresirati možemo fizičke uređaje, kao što su kompletna računala i priključci na mrežu, ili procese, kao što su procesi razina hijerarhijske strukture ili procesi korisnici komunikacije. Fizičkim uređajima dodjeljujemo adrese prema potrebama promatrane razine hijerarhijske strukture. U većini slučajeva dovoljno je odrediti adresu uređaja na podatkovnoj i mrežnoj razini. Procese identificiramo kroz pristupne točke (SAP, u Internet terminologiji "port") kojima podaci prolaze preko sučelja. Procesima mrežne i prijenosne razine hijerarhijske strukture dodjeljujemo stalne pristupne točke, kojima zapravo identificiramo korištene protokole tih razina. Dinamičko dodjeljivanje pristupnih točaka ovdje nije potrebno jer se radi o poznatim procesima. Od sjedničke razine naviše imamo veze koje iniciraju korisnici, tako da je ovdje primjereno korištenje dinamičkih pristupnih točaka. Iznimka su poslužnički procesi viših razina, koji također koriste fiksne pristupne točke.

Adresa odredišta može biti pojedinačna (unicast), grupna (multicast) ili univerzalna (broadcast). Kod pojedinačnog adresiranja PDU je namijenjen samo jednom odredišnom uređaju ili procesu, dok ga ostali (na višespojnom mediju) nakon provjere adrese odbacuju. Kod grupnog adresiranja, PDU je namijenjen ranije definiranoj grupi uređaja ili procesa, koji su u stanju prepoznati grupnu adresu odredišta. Kod univerzalnog adresiranja, svi uređaji ili procesi primaju PDU. Adresa izvorišta PDU može biti samo pojedinačna.

Adrese na pojedinoj razini neke mreže mogu biti lokalno ili globalno administrirane (određene). Oštra granica mora postojati na prijelazu između privatne i javne mreže. Adrese na privatnoj mreži mogu biti lokalno administrirane, dok one na javnoj moraju biti određene od strane ovlaštenog tijela u upravi mreže kao organizacije. Često se, međutim, i u privatnim mrežama koriste globalno administrirane adrese, kako bi se smanjila količina posla u upravljanju mrežom. Poseban slučaj su nepovezane (autonomne) i skrivene (intranet) mreže, za koje se preporučuje upotreba za njih predviđenih adresa.

Na **fizičkoj razini** načelno nemamo potrebe za adresiranjem. Ukoliko koristimo neku javnu, npr. telefonsku mrežu s komutacijom kanala, adresom na fizičkoj razini možemo smatrati pozivni broj telefonskog priključka kojeg pozivamo.

Na **podatkovnoj razini** adresiranje koristimo ovisno o načinu povezivanja. Kod jednospojnog povezivanja adresiranje se koristi za ostvarivanje više logičkih kanala, od kojih će jedni biti na raspolaganju korisniku, a drugi će služiti za upravljanje mrežom. Kod višespojnog povezivanja imamo pravi proces adresiranja, gdje identificiramo fizički uređaj kao odredište i izvorište okvira. Adresa odredišta može biti pojedinačna, grupna ili univerzalna, a administriranje može biti lokalno ili globalno. Tako npr. kod lokalnih mreža možemo koristiti globalno administriranu adresu ugrađenu u vezni sklop. Iako je ta adresa globalno jednoznačna, ne može se koristiti kao konačna adresa na javnoj mreži, jer nema načina kojim bi se na osnovu te adrese odredio put kroz mrežu do uređaja. Doseg univerzalnih adresa podatkovne razine ograničen je dosegom višespojnog medija.

Na sučelju između podatkovne i mrežne razine pojavljuje se potreba za identifikacijom procesa mrežne razine. Kod modernih mreža, na mrežnoj razini se koristi više vrsta protokola, pa je potrebno koristiti pristupne točke. Tako npr. okvir podatkovnog protokola lokalne mreže mora sadržavati identifikator odredišnog protokola mrežne razine. Ovdje koncept dinamički dodijeljenih pristupnih točaka nije potreban. Zbog činjenice da oba udaljena uređaja komuniciraju po istom mrežnom protokolu možemo koristiti fiksne, globalno administrirane identifikatore protokola.

Na **mrežnoj razini** mora postojati jedinstvena globalna adresa korisnika, koja omogućuje usmjeravanje paketa ka odredištu. Pakete u mrežama s prospajanjem paketa prosljeđujemo pojedinačno ili po virtualnom kanalu. U slučaju pojedinačnog prosljeđivanja, svaki paket mora nositi globalnu adresu odredišta. U slučaju prosljeđivanja po virtualnom kanalu, samo prvi paket nosi globalnu adresu. Nakon prolaska kroz mrežu uspostavlja se virtualni kanal kao put po kojem prolaze svi paketi veze. ostali paketi moraju nositi samo kratki identifikator virtualnog kanala.

Kod IP protokola Interneta, globalna adresa ukupne duljine 32 bita sastoji se od adrese podmreže i adrese računala. Adresa podmreže koristi se za određivanje puta do odredišta i taj dio se administrira globalno. Adresa računala koristi se kada paket stigne na odredišnu podmrežu, i taj dio administrira se lokalno. Korisnik koji želi uspostaviti vezu s određenim računalom, mora znati IP adresu tog računala, dakle oba njena dijela. Globalnu adresu nose svi paketi, jer se prosljeđivanje obavlja pojedinačno.

Kod X.25 protokola mrežne razine, globalna adresa ukupne duljine do 14 dekadskih znakova sastoji se od identifikatora nacionalne mreže, identifikatora područne mreže i identifikatora priključka. Pozivni broj se formira slično telefonskom broju. Globalnu adresu nosi samo prvi paket veze, jer se prosljeđivanje obavlja po virtualnom kanalu. Svi ostali paketi nose identifikator virtualnog kanala duljine 12 bita (mogućih 4096 virtualnih kanala).

Na **prijenosnoj razini** obavlja se identifikacija prijenosnog protokola. Koristi se mehanizam pristupnih točaka s fiksnim identifikatorom.

Na **sjedničkoj razini** obavlja se identifikacija procesa korisnika unutar računala. Koristi se mehanizam pristupnih točaka s dinamičkom dodjelom identifikatora. Iznimka su poslužnički procesi, npr. HTTP (WEB) poslužitelj, koji koriste fiksne identifikatore.

ISO-OSI arhitekturom razdvojena je prijenosna od sjedničke razine, iako u praksi one koriste isti PDU koji prema mrežnoj razini koristi pristupne točke vezane za protokol prijenosne razine, a prema predodžbenoj razini pristupne točke vezane za procese korisnike. Kod Interneta su ove dvije razine objedinjene u jednu (prijenosnu) razinu. Isto tako, kod Interneta su objedinjene predodžbena i korisnička

razina (u korisničku), jer je prirodno da prevođenje sa formata mreže na format računala obavlja proces koji pruža ili koristi promatranu mrežnu uslugu.

Adresiranje na predodžbenoj i korisničkoj razini nije potrebno, jer su procesi već identificirani kroz sjedničku razinu.

## 2.4.2 SINKRONIZACIJA

Mehanizam sinkronizacije odnosi se na izdvajanje cjelovitih PDU iz beskonačnog niza bita, kao i na usklađeni rad procesa iste razine.

### 2.4.2.1 Sinkronizacija PDU

Po razinama obavlja se sinkronizacija sljedećih PDU:

Na **fizičkoj razini** sinkronizacija se obavlja ovisno o tome da li je prijenos kanalom asinkron ili sinkron. Kod sinkronog prijenosa imamo sinkronizaciju po bitu, dok se kod asinkronog prijenosa ostvaruje istovremeno sinkronizacija po bitu i po oktetu.

Na **podatkovnoj razini** sinkronizacija također ovisi o načinu prijenosa na fizičkoj razini. Ako je prijenos sinkron, imamo sinkronizaciju po oktetu i okviru, a ako je asinkron, samo po okviru.

Na **mrežnoj razini** imamo sinkronizaciju po paketu, samo kad je paket podijeljen na više okvira podatkovne razine.

Na **prijenosnoj razini** sinkronizacija po segmentu ili datagramu je rijetka, jer se najčešće cjeloviti PDU prenose jednim paketom mrežne razine.

Na **sjedničkoj razini** obavlja se sinkronizacija po poruci, tj. poruka se sastavlja od primljenih segmenata ili datagrama.

Sinkronizacija PDU na višim razinama nije potrebna.

### 2.4.2.2 Sinkronizacija rada procesa

Proces N obavlja svoju zadaću na osnovi pretpostavljenog poznavanja stanja korespondentnog procesa na udaljenom računalu. Jedina informacija o udaljenom procesu su primljeni PDU. Algoritmi rada procesa N trebaju biti takvi da omoguće prijenos podataka u uvjetima gubitaka PDU i pogrešnih pretpostavki o stanju korespondentnog procesa.

Komuniciraju će proces promatrane razine odvija se u nejednolikom diskretnom vremenu, određenom pristizanjem PDU sa podređene i SDU sa nadređene razine. Takav proces može se smatrati automatom, jer on za uspješan rad mora pamtit i prethodne događaje. Odatle mogućnost specifikiranja protokola dijagramom stanja. U stvarnosti, po pravilima protokola komuniciraju dva istovrsna udaljena protokola, od kojih se svaki u promatranom trenutku nalazi u nekom stanju. Par stanja predstavlja stanje veze. Analizom svih parova stanja, možemo zaključiti da su neki parovi normalni kao stanje veze, uzrokovani kašnjenjem u međusobnoj komunikaciji istovrsnih procesa i gubicima PDU. Drugi parovi stanja ne mogu biti normalno stanje veze, već su rezultat neusklađenog rada korespondentnih procesa. Protokol mora imati sposobnost oporavka od takvih nepoželjnih stanja veze.

## 2.4.3 KONTROLA POGRJEŠKI

Kontrolom pogreški osiguravamo da informacija korisnika stigne na odredište. Kontrolu pogreški organiziramo ovisno o količini redundancije u informaciji, o dozvoljenom ukupnom kašnjenju, te o dozvoljenom kašnjenju među dijelovima informacije. Informacije možemo grubo svrstati u dvije grupe.

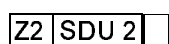
U grupi koju karakterizira **prijenos govora** ukupno kašnjenje i razlika kašnjenja po dijelovima mora biti mala, dok velika redundancija sadržana u govoru omogućava zadovoljavajuću razumljivost u uvjetima umjerene količine pogreški. Kontrolu pogreški ćemo organizirati korištenjem kodova za korekciju pogreški na strani prijemnika, jer zbog zahtjeva za malim kašnjenjem (zakašnjeli signal se ne može naknadno reproducirati) nema mogućnosti retransmisije. Kodovi za korekciju pogreški, da bi bili



ekonomični, osiguravaju korekciju samo najčešćih pogriješki (npr. jednostrukih). To je za slučaj govora prihvatljivo, zbog spomenute visoke razine redundancije.

U grupi informacija koju karakterizira **prijenos podataka** najvažniji zahtjev je apsolutna točnost prenesene informacije, dok su dozvoljeni veće kašnjenje, varijacije kašnjenja i varijacije brzine prijena. Kontrolu pogriješki ćemo organizirati korištenjem kodova za detekciju pogriješki i mehanizmom ponovnog slanja (retransmisije). Dakle, kontrola pogriješki obavlja se u dva koraka, u prvom se pogriješka otkriva, a u drugom se veza oporavlja od gubitka.

**Detekcija pogriješki** zasniva se na kodovima s korištenjem redundancije i kodne udaljenosti (distance). Dodavanjem kontrolnih bita kodnoj riječi koncentriranog koda, umjetno se povećava broj mogućih kodnih riječi koda. Kako je broj iskorištenih ostao isti, povećan je broj neiskorištenih kodnih riječi. Kontrolni bitovi se smatraju dijelom zaglavlja, iako ih zbog sklopovskog računanja često dodajemo na kraju PDU, slika 2.15.



kontrolni bitovi

*Slika 2.15. - Dodavanje kontrolnih bitova jedinici informacije*

Kada smetnja ispravnu kodnu riječ prevede u neku od neiskorištenih, takvu je pogriješku moguće detektirati, a kada je pretvori u drugu korištenu kodnu riječ, pogriješku je nemoguće detektirati. U praksi su višestruke pogriješke rjeđe od jednostrukih, tj. vjerojatnost višestrukih pogriješki je manja, pa je za konstrukciju koda važna distanca (broj različitih bita u kojima se promatrane kodne riječi razlikuju). Ukoliko je minimalna distanca  $d$ , potrebna je  $d$ -struka pogriješka da bi jednu ispravnu kodnu riječ pretvorila u drugu ispravnu, pa je moguće otkriti sve pogriješke do uključivo  $d-1$ -struke.

Nakon detekcije pogriješke potrebno je osigurati **oporavak veze**. Postavlja se pitanje što napraviti s oštećenim PDU. Kod za detekciju pogriješki ne daje nam informaciju gdje je unutar PDU nastupila pogriješka, pa ne znamo da li je PDU namijenjen promatranom procesu (pogriješka na adresi), koji mu je točno redni broj (pogriješka na numeraciji), ili je oštećen neki drugi vitalni dio zaglavlja. Takav oštećeni PDU je najjednostavnije odbaciti, izbrisati iz memorije, kao da nikad nije ni stigao na čvorište. Odbacivanje PDU je kompatibilno s drugim mehanizmom gubitaka PDU u paketnim mrežama, a to je zagušenje. Kod pojave zagušenja napuni se memorija čvorišta paketima koji čekaju na prosljeđivanje, te su paketi za koje nema mjesta u memoriji izgubljeni. Kod današnjih mreža, naročito kod korištenja optičke tehnologije, broj gubitaka PDU zbog smetnji je zanemariv. Ogromna većina (preko 99%) PDU izgubi se zbog zagušenja.

Da bi proces razine mogao detektirati gubitak PDU, potrebno je pojedine PDU identificirati. To se radi brojevanjem oznakama, odnosno numeracijom PDU. U zaglavlju PDU predvide se polja u kojima se šalje redni broj PDU. Kako su ta polja konačne duljine, numeracija se nužno obavlja po modulu, gdje je modul određen duljinom polja. Da ne bi došlo do miješanja PDU, predajnik nikada ne smije poslati na mrežu dva PDU s istom numeracijom. Sljedeći PDU se ne smije poslati prije nego je prethodni PDU istog broja napustio mrežu. Stoga je maksimalni broj PDU kojeg predajnik može poslati jednak modulu numeracije. Ova se veličina, tj. broj PDU na mreži, naziva prozorom ( $W$ , window), a prozor ne može biti veći od modula numeracije. Naravno, stvarni broj PDU (trenutni prozor) može biti manji od prozora numeracije. Predajnik može doznati da li je PDU napustio mrežu na osnovu potvrde prijemnika (ACK, acknowledgment).

Protokoli koji sadrže mehanizam kontrole pogriješki u smislu numeracije PDU, detekcije izostanka PDU i retransmisije nazivaju se **spojevni** protokoli (connection oriented). Po takvi protokolima, procesi na početku prijena podataka moraju uskladiti početnu numeraciju PDU, što se zove uspostavom logičkog kanala. TCP protokol Interneta je spojevni protokol.

Protokoli koji ne sadrže mehanizme oporavka od pogriješke (eventualno samo otkrivaju pogriješke i odbacuju PDU) nazivaju se **bespojni** protokoli (connectionless). Kod takvih protokola gubitak PDU ne izaziva nikakvu reakciju. Konzistentnost korisnikove poruke treba osigurati neki od protokola nadređenih

razina. Primjer bespojnog protokola je IP protokol mrežne razine Interneta, a često se koristi u kombinaciji s nadređenim spojevnim TCP protokolom (otud kovanica TCP/IP).

Detekcija gubitka PDU u praksi je otežana načinom prosljeđivanja PDU. Kod mrežne razine s pojedinačnim prosljeđivanjem, dio paketa može ići alternativnim putovima, pa da redosljed pristizanja paketa na odredište nije zagarantiran. Potrebno je adaptivno odrediti vrijeme čekanja da zakašnjeli PDU stigne. Ukoliko je ovo vrijeme kratko, inicirati će se nepotrebne retransmisije. Ukoliko je ono predugo, retransmisija će biti prekasno inicirana, pa može doći do pada brzine prijenosa i slabije iskorištenosti kapaciteta mreže.

Nakon što je gubitak PDU detektiran, potrebno ga je dojaviti predajniku. Ovo možemo postići slanjem posebne poruke kojom zahtijevamo retransmisiju. Međutim, kako za svaki primljeni PDU prijemnik treba poslati potvrdu (zbog mehanizma prozora), predajnik može na osnovu potvrda jednako efikasno detektirati gubitak PDU, kao i prijemnik na osnovu izostanka PDU. Štoviše, predajnik će detektirati i gubitak potvrde. Bez obzira da li potvrda izostaje zbog gubitka originalnog PDU ili potvrde, predajnik odlučuje o retransmisiji PDU i neposredno nakon odluke može retransmisiju stvarno izvršiti. Time se štedi na vremenu potrebnom za dojavu gubitka od strane prijemnika.

Algoritmi detekcije gubitka PDU i donošenja odluke o retransmisiji su vrlo složeni. U praksi je najpoznatiji algoritam TCP protokola Interneta, kod kojega predajnik mjeri vrijeme obilaska i varijancu vremena obilaska, te izračunava optimalno vrijeme čekanja da PDU pristigne (RTO, retransmission timeout). Proces retransmisije se može ubrzati, ako prijemnik za prekoredne PDU šalje ponovljene (duplicirane) potvrde. Kod TCP protokola, uveden je algoritam brze retransmisije, kod kojega se PDU ponovno šalje nakon tri uzastopne duplicirane potvrde (fast retransmit).

Sama retransmisija može se obaviti na dva načina. Jednostavniji i često korišteni način je **grupna retransmisija**, (go-back-N), kada predajnik ponovno šalje izgubljeni PDU i sve ostale koji slijede, bez obzira da li su stvarno i oni izgubljeni ili ne. Složeniji način je **selektivna retransmisija**, kod koje se šalje samo izgubljeni PDU, a na osnovu selektivnih pozitivnih ili negativnih potvrda (dojava prijema ili dojava gubitka). U praksi selektivna retransmisija oduzima nekoliko vremena obilaska, pa je isplativa samo na kanalima s velikom vjerojatnošću pogriješki ( $10^{-5}$  i gore), kao što su radio kanali.

Specifičnosti kontrole pogriješki po razinama hijerarhijske strukture su:

Na **fizičkoj razini** kontrola pogriješki na razini bita nije isplativa, osim ako linijski kod ne omogućava automatsku detekciju pogriješke. Takav linijski kod je Manchester-II, korišten kod lokalnih mreža za prijenos podataka.

Na **podatkovnoj razini** kontrola pogriješki je jedna od osnovnih funkcija. Okvir se štiti kodom za otkrivanje pogriješki. Oštećeni okviri se odbacuju. Izostanak okvira, detektiran na osnovu numeracije, aktivira retransmisiju na osnovu zahtjeva prijemnika ili izostankom potvrde. Kako se radi o neposrednom nadzoru jednospojnog ili višespojnog medija, bez čvorišta među krajnjim stanicama, može se smatrati da će redosljed isporuke okvira biti očuvan, te da će kašnjenje biti malo (s iznimkom satelitskih kanala). Algoritam detekcije gubitka PDU je jednostavan zbog očuvanog redosljeda pristizanja, a zbog malog kašnjenja moguće je neposredno tražiti retransmisiju, npr. okvir REJ, (reject), ili SREJ, (selective reject), bitovno orijentiranih protokola.

Na **mrežnoj razini** često dolazi do gubitaka zbog zagušenja. Protokoli su često bespojni jer je kontrolu pogriješki optimalno obaviti na prijenosnoj razini.

Na **prijenosnoj razini** optimalno je obaviti kontrolu pogriješki. Kopije PDU za retransmisiju nalaze se kod predajnika, pa ne opterećuju mrežu, a prijemnik bezuvjetno mora kontrolirati konzistentnost primljenih podataka. Na složenim mrežama s komutacijom paketa PDU na putu do odredišta prolazi kroz nekoliko čvorišta, te kašnjenje može biti veliko. Ukoliko se na mrežnoj razini paketi prosljeđuju pojedinačno, ni redosljed pristizanja nije zagarantiran. Stoga je detekcija gubitka PDU otežana, a neposredna dojava gubitka nije efikasna. Analizom pristizanja potvrda predajnik će detektirati gubitak PDU, te donijeti odluku o retransmisiji.

Optimalno je detekciju pogriješki obaviti na podatkovnoj i mrežnoj razini, a detekciju izostanka PDU i retransmisiju na prijenosnoj razini, npr. kao kod Interneta

## 2.4.4 KONTROLA TOKA KAO MEHANIZAM PROTOKOLA

Kontrola toka nam služi za usklađivanje brzine prijenosa podataka među učesnicima, a s obzirom na prijenosni kapacitet i opterećenje mreže. Kontrola toka, kao mehanizam protokola, dio je upravljanja prometom, odnosno njegovog dijela, kontrole zagušenja.

Na **fizičkoj razini** kontrola toka ostvaruje se na sučelju DTE-DCE korištenjem posebnih signala sučelja. Konkretno, inteligentni modemi raspolažu s funkcijama sažimanja podataka, kontrole pogrješki i izbora optimalne brzine prijenosa. Vezu terminal-modem ostvarimo maksimalnom brzinom, a eventualne zastoje razriješimo kontrolom toka.

Na **podatkovnoj razini** imamo neposrednu vezu dvaju uređaja, pa je moguća neposredna kontrola toka (naredbama stani i nastavi). Na vezama s velikim kašnjenjem (satelitske veze) moguća je i prozorska kontrola toka. Ako su okviri numerirani, a numeracija je jedino moguća po modulu, predajnik smije poslati samo onoliko okvira koliko ima slobodnih brojeva. Modul numeracije je implicitno i maksimalni prozor. Potvrdom prijemnika oslobađaju se brojevi za slanje sljedećih okvira.

Na **mrežnoj razini** pojavljuju se kašnjenja zbog velikog broja čvorova kojima paket prolazi do odredišta, a potvrda natrag do izvorišta (vrijeme obilaska). Neposredna kontrola toka je neefikasna. Moguća je prozorska ili kontrola brzine predaje. Pri tome se brzina usklađuje s propusnim kapacitetom mreže. Mreža u slučaju zagušenja najčešće može samo odbaciti prekobrojne pakete.

Na **prijenosnoj razini** je optimalno organizirati kontrolu toka, jer neposlani paketi ne opterećuju zagušenu mrežu. S obzirom na kašnjenje, sve što vrijedi za mrežnu razinu, vrijedi i za prijenosnu. Predajnik određuje optimalnu brzinu slanja ili optimalni prozor na osnovu mjerenja vremena obilaska (RTT, Round Trip Time) ili intenziteta gubitaka paketa. Predajnik na mrežu šalje optimalni prozor paketa s obzirom na zagušenost mreže, ali ne više od prozora prijemnika.

Na višim razinama klasične kontrole toka, u smislu sposobnosti računala da obradi podatke, nema. Ograničenje prozora prijemnika garantira da će u memoriji prijemnika biti dovoljno prostora za sve pakete koje predajnik smije poslati, i tu oni mogu čekati na obradu korisnikovog procesa.

## 2.5 UPRAVLJANJE PROMETOM

Upravljanje prometom provodi se na svim vrstama mreža s ciljem postizanja optimalnog iskorištenja mreže i kakvoća usluge. Provodi se kroz postupke usmjeravanja prometa i kontrole zagušenja.

**Usmjeravanje prometa** je postupak kojim se primarno ostvaruje dostupnost među korisnicima. Kod paketnih mreža može se obavljati usmjeravanjem individualnih paketa ili konceptom virtualnih kanala (ATM, X.25). Usmjeravanje prometa alternativnim putem osnovna je metoda izbjegavanja zagušenja za mreže s prospajanjem kanala. To je pomoćna metoda izbjegavanja zagušenja kod paketnih mreža. Alternativni putovi su dulji i zagušenje se širi na do tada nezahvaćene dijelove mreže, pa je za kontrolu zagušenja paketnih mreža poželjno koristiti druge metode.

**Kontrola zagušenja** za paketne mreže obuhvaća postupke izbjegavanja i otklanjanja zagušenja. Pod izbjegavanjem podrazumijevamo postupke kada do zagušenja još nije došlo, a pod otklanjanjem postupke kada do zagušenja dođe iz bilo kojeg mogućeg razloga.

### 2.5.1 KONTROLA ZAGUŠENJA

Kontrola zagušenja je jedan od ključnih mehanizama mrežne arhitekture. Ona omogućava pružanje usluga tražene kakvoće korisniku, uz optimalno iskorištenje kapaciteta mreže. Zagušenje možemo definirati kao situaciju kada je u promatranom vremenskom periodu ponuđeni promet veći od prijenosnog kapaciteta mreže. Tada dolazi do gubitaka prometa i do smanjenja kakvoće usluge. Kontrolu zagušenja provodimo kroz postupke izbjegavanja i otklanjanja zagušenja.

Postupci **izbjegavanja zagušenja** provode se dok mreža još nije zagušena i cilj im je ograničiti ulazni promet, te održati mrežu u optimalnoj radnoj točki. To je točka koja osigurava traženu kakvoću usluge korisnicima uz optimalno iskorištenje mreže, dakle optimalnu ekonomičnost rada mreže. Postupci **otklanjanja zagušenja** aktiviraju se kada mreža dođe u stanje zagušenja, kako bi posljedice trajale što

kraće i po mogućnosti bile ograničene na što uže područje. Mjere izbjegavanja i otklanjanja zagušenja provode se na svim razinama upravljanja i vođenja mreže, te na svim vremenskim razinama.

Među mjerama izbjegavanja zagušenja kod mreža s prospajanjem paketa značajno mjesto pripada mehanizmima **kontrole toka**. Njihov je zadatak regulirati brzinu predaje izvorišta tako da dolazni promet bude optimalan po kriterijima kakvoće usluge i iskorištenja kapaciteta mreže. Kontrola toka se ostvaruje unutar vremena trajanja logičkog kanala. Ona u stvarnom vremenu, s obzirom na kašnjenja u mreži, održava mrežu u optimalnoj radnoj točki.

### 2.5.1.1 Kontrola zagušenja prema vrsti prospajanja

Kontrola zagušenja u mrežama s **komutacijom kanala** provodi se odbacivanjem zahtjeva za prospajanjem, dakle kontrolom pristupa mreži (CAC, Connection Admission Control). Korisnik će eventualno kasnije ponoviti svoj zahtjev, a kad konačno ostvari vezu kakvoća usluge mu je zagarantirana kroz karakteristike fizičkog kanala prosposjenog s kraja na kraj mreže.

Kod mreža s **komutacijom paketa**, raspoloživi kapacitet kanala dijeli se na mnogo korisnika vremenskom razdiobom, odnosno statističkim multipleksiranjem paketa. Kontrola zagušenja treba održati broj paketa u mreži (u prijenosu i memorijama čvorišta) na optimalnoj razini kontrolom brzine predaje paketa izvorišta. Manjak paketa u mreži znači lošu iskorištenost kapaciteta, a višak znači da je smanjena kakvoća usluge zbog povećanog vremena kašnjenja i povećanih gubitaka paketa (popunjenost memorije čvorova).

U **ATM mrežama**, koje trebaju omogućiti funkcionalnu integraciju svih vrsta prometa, kontrola zagušenja ima slične ciljeve kao kod paketnih mreža, tj. održati broj ćelija u mreži na optimalnoj razini. Zbog velike predviđene brzine prijenosa i prospajanja, kontrola zagušenja se odvija kroz ograničenje pristupa i uobličivanje prometa izvorišta za CBR (Constant Bit Rate) i VBR (Variable Bit Rate) korisnike, te uobličivanjem s dinamičkom promjenom brzine za ABR (Available Bit Rate) korisnike. UBR (Unspecified Bit Rate) korisnici pristupaju preostalom dijelu kapaciteta mreže bez ikakvih garancija za kakvoćom usluge, tako da mreža jednostavno odbacuje višak ćelija.

### 2.5.1.2 Vrste zagušenja

Zagušenje smo definirali kao situaciju kod koje je, u promatranom vremenskom periodu, dolazni promet veći od prijenosnog kapaciteta mreže. U toj definiciji ostalo je neodređeno trajanje vremenskog perioda promatranja. S obzirom na njegovu duljinu, zagušenje može biti trajno, periodičko (sezonsko, tjedno i dnevno), privremeno i trenutno. Zagušenja imaju različite uzroke, te se poduzimaju različite mjere za njihovo otklanjanje i izbjegavanje na paketnim mrežama, tablica 2.1.

vrsta zagušenja:	postupci izbjegavanja	postupci otklanjanja
TRAJNO	pravovremeno planiranje razvoja i izgradnja potrebnih kapaciteta	izgradnja i zakup vodova
PERIODIČKO	tarifna politika, kontrola pristupa, usmjeravanje prometa	korištenje kapaciteta mreža s drugim profilom korisnika ili iz drugih vremenskih zona
PRIVREMENO	kontrola toka	odbacivanje viška prometa
TREKUTNO	uobličivanje prometa	osiguranje dovoljnog kapaciteta memorije čvorišta

*Tablica 2.1. - Vrste zagušenja za paketne mreže*

**Trajno** zagušenje je rezultat naraslih potreba korisnika i nepravodobnih investicija u proširenje kapaciteta mreže. Otklanja se izgradnjom ili zakupom novih prijenosnih kapaciteta (kanala i čvorišta), a izbjegava planiranjem i predviđanjem budućih potreba.

**Periodička** zagušenja rezultat su životnog i radnog ritma korisnika, koji istu uslugu traže istovremeno. Ova zagušenja otklanjaju se korištenjem kapaciteta drugih mreža sa različitim rasporedom opterećenja, ili kanala iz drugih vremenskih zona, te uvođenjem kontrole pristupa korisnika. Izbjegavaju se stimulacijom korisnika da usluge traži u vrijeme niskog opterećenja (tarifna politika), kontrolom pristupa, te usmjeravanjem prometa.

Trajanje **privremenog** zagušenja je reda veličine minuta i sekunda. Ono nastaje i nestaje unutar vremena trajanja pojedine veze među korisnicima, ali traje duže od vremena obilaska (kašnjenja) na mreži. Rezultat je statističkog rasporeda zahtjeva korisnika, koji na toj vremenskoj razini uspostavljaju i raskidaju svoje veze. Otklanja se odbacivanjem viška ponuđenog prometa (paketa), a izbjegava korištenjem funkcija kontrole toka.

**Trenutna** zagušenja, čije je trajanje reda veličine desetinki sekunde, kraća su od vremena kašnjenja na mreži. Rezultat su nejednolikog intenziteta ponuđenog prometa izvorišta, te kašnjenja mehanizma kontrole toka. Otklanjaju se ugradnjom dovoljnog kapaciteta memorija čvorišta, koje trebaju predvidive količine podataka prihvatiti bez gubitaka. Ne mogu se izbjeći kontrolom toka, ali pomaže uobličivanje prometa izvorišta.

### 2.5.1.3 Kakvoća usluge i kontrola zagušenja

Kod mreža s komutacijom kanala korisnik raspolaze s cijelim kapacitetom prospojenog kanala i u tom smislu je kakvoća usluge zagaranirana. Kakvoća se stvarno mjeri kakvoćom kanala, tj. širinom pojasa i odnosom signala i šuma za analogne, te brzinom prijenosa i vjerojatnošću pogreške za digitalne kanale. Korisnici su dužni nadzirati integritet vlastitih prenesenih podataka.

Kod mreža s komutacijom paketa bez rezervacije kapaciteta, npr. Interneta, usluga se pruža po principu najbolje moguće usluge (best effort), bez ikakvih garancija za točnost (na mrežnoj razini), brzinu i kašnjenje. Paketi se usmjeravaju na osnovu težine putova, višak paketa se odbacuje, a korisnici su dužni nadzirati integritet vlastitih podataka i obavljati kontrolu toka na prijenosnoj razini (TCP). Mreža je efikasna za prijenos podataka, ali neprimjerena za prijenos informacija u stvarnom vremenu (govor i slika). Eksperimentalni mehanizmi rezervacije kapaciteta ispituju se na Internetu (RSVP, Reservation Protocol).

Kod paketnih mreža koje rezerviraju kapacitet, kao što je ATM mreža, paketi se usmjeravaju virtualnim kanalom. Mreža garantira kakvoću usluge, ali zbog konačne vjerojatnosti nedetektirane pogreške korisnici trebaju nadzirati integritet podataka. ATM mreže će se graditi sa ciljem integracije svih vrsta prometa. Stoga je potrebno za svaku vrstu garantirati specifičnu kakvoću usluge, te tu kakvoću zaštititi od prometa izvora koji rade većom brzinom od ugovorene. Usluge koje su za sada predviđene za ATM mreže su prijenos nekomprimiranog govora i video signala (CBR), komprimiranog govora, video i multimedijских signala (VBR), te prijenos podataka s garantiranom (ABR) i negarantiranom (UBR) kakvoćom prijenosa.

## 2.5.2 KONTROLA TOKA

Mehanizmi kontrole toka najznačajniji su dio mjera za izbjegavanje privremenih zagušenja na mrežama s komutacijom paketa. Kontrola toka odvija se u stvarnom vremenu i nadzorom nad brzinom rada predajnika održava mrežu u optimalnoj radnoj točki.

### 2.5.2.1 Optimalna radna točka mreže

Optimalna radna točka mreže može se definirati kao vektor stanja svih elemenata mreže, koji omogućava optimalan odnos iskorištenja mreže i kakvoće usluge. Ova dva suprotna kriterija, stanovišta vlasnika i korisnika mreže, imaju zajedničko ishodište u želji da se ponuđeni promet posluži što prije, dakle s minimalnim kašnjenjem. Kriterij kašnjenja je za korisnika jasan, dok za mrežu ima smisla da sav trenutno raspoloživi kapacitet ponudi korisnicima i posluži njihove zahtjeve, oslobađajući kapacitet za buduće zahtjeve. Za prijenos podataka, gdje gubitaka na korisničkoj razini ne smije biti, to znači da treba izbjegavati gubitke na nižim razinama izazvane zagušenjem, i tako spriječiti nepotrebna ponavljanja (retransmisije) koja povećavaju kašnjenje i doprinose zagušenju, te smanjuju efikasnost mreže.

Stanje elementa paketne mreže je broj paketa u redu čekanja za prijenos. Optimalna radna točka mreže je vektor stanja u kojem su svi članovi, dakle stanja svih elemenata, na optimalnoj razini. Problem određivanja optimalne radne točke usko je povezan s modelom posluživanja i prometa na mreži. Paketi (ili ćelije) putuju kanalima i stižu u čvorišta gdje se usmjeravaju i upućuju u izlazne repove, na čekanje reda za prijenos odlaznim kanalima. Zagušenje se na nekom kanalu pojavljuje kad je dolazni promet veći od odlaznog, tako da se paketi gomilaju u memoriji čvorišta, a kašnjenje povećava. Nasuprot tome, kada su redovi prazni, raspoloživi kapacitet je nedovoljno iskorišten. Dakle, potrebno je održati broj paketa u redu takvim da kašnjenje bude optimalno, a iskorištenje mreže visoko.

Gornji fizički model analitički se iskazuje matematskim modelima sustava s posluživanjem. Za analizu se najčešće koriste sustavi s Markovljevim (Poissonovim, M/M/1) ili generalnim (G/G/1) modelima prometa i posluživanja, a značajan je i determinirani (D/D/1) model kao posebni slučaj generalnog. Optimalna radna točka najčešće se nalazi kao maksimum "snage mreže" (Power), definirane kroz omjer propusnosti i vremena kašnjenja:

$$P = \frac{L}{T} [\text{b/s}^2] \quad 2-1$$

gdje je P "snaga", L korisni promet, a T vrijeme kašnjenja (obilaska). Korisni promet L koji mreža prenese korisnik vidi kao broj paketa (okteta, bita) prenesenih u jedinici vremena. Ako korisnik poštuje princip očuvanja broja paketa u mreži (prozor), onda će sljedeći paket poslati nakon prijema potvrde za jednog od prethodnih. Kod kontrole toka mehanizmom prozora, predajnik će poslati onoliko paketa koliko mu dozvoljava širina prozora W, a potvrdu za neki paket će primiti nakon vremena obilaska RTT, dakle nakon što pun prozor paketa prođe kroz mrežu:

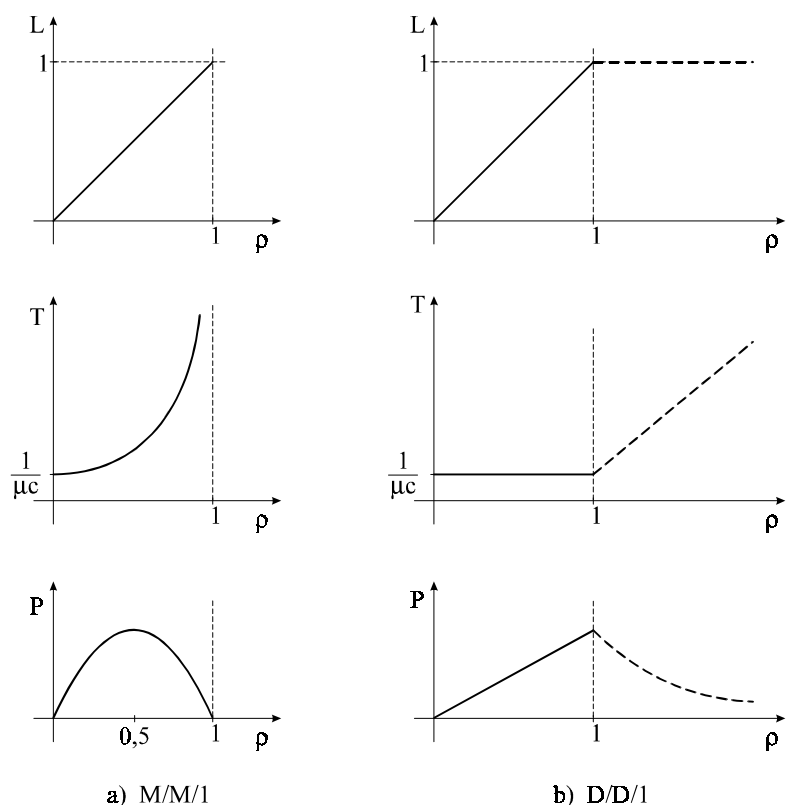
$$L = \frac{W}{RTT} = \frac{W}{T} \quad 2-2$$

Optimalna radna točka za M/M/1 model je pri prosječnoj duljini reda od jednog paketa, uz iskorištenje mreže od 50%. Zbog velike varijance, smatra se da M/M/1 model može poslužiti kao "najgori slučaj". Skica grafova za M/M/1 model prikazana je na slici 2.16.a.

Determinirani model izvorišta i posluživanja opravdan je kada sva izvorišta šalju pakete približno iste duljine jednolikim ritmom. To je specijalni slučaj G/G/1 modela, kod kojega su varijance intenziteta dolazaka i posluživanja jednake nuli. U praksi se mogu naći opravdanja za takvu aproksimaciju, pogotovo za model posluživanja kod ATM mreža (konstantna duljina ćelije). Na osnovi pretpostavke da će se u svakom ciklusu posluživanja red isprazniti, D/D/1 model daje konstantno kašnjenje jednako vremenu posluživanja za podopterećenu mrežu, te skok kašnjenja u beskonačnost za mrežu opterećenu preko nazivnog kapaciteta. Za konstantan broj paketa u mreži (prozorska kontrola toka), model daje linearni porast kašnjenja za opterećenja "veća" od 100%, a sve do trenutka popune memorije čvorišta kada dolazi do gubitaka. Optimalna radna točka za D/D/1 model je pri opterećenju mreže od 100%.

D/D/1 model nije dovoljno precizan da bi se na toj osnovi gradili mehanizmi kontrole toka, ali daje značajan rezultat: optimalnu radnu točku koja se približava potpunom iskorištenju mreže. To znači da će kontrola toka nastojati održati radnu točku mreže na visokom stupnju iskorištenja, a stvarne procese dolazaka i posluživanja zahtjeva uobličiti prema zahtjevima determiniranog modela. Skica grafova za D/D/1 model prikazana je na slici 2.16.b.

Prva grupa grafova prikazuje korisni promet. Do dostizanja kapaciteta mreže, preneseni promet je jednak ponuđenom. Nakon toga, zbog gubitaka, za M/M/1 mrežu promet pada na 0, dok uz uvjet konačnog prozora za D/D/1 model ostaje konstantan. Pri tome kašnjenje za M/M/1 model raste u beskonačnost, dok za D/D/1 model s konačnim prozorom raste linearno s porastom prozora. Donji red grafova prikazuje promjenu snage mreže ovisno o opterećenju, koja kod M/M/1 ima maksimum za 0,5, a kod D/D/1 modela za opterećenje od 1,0.



Slika 2.16. - Skice krivulja za propusnost, kašnjenje i snagu mreže

### 2.5.2.2 Jednakost korisnika i pravednost

Pravednost (Fairness) je, osim pružanja tražene kakvoće usluge, drugi elementarni cilj kontrole toka. Ona osigurava da svi korisnici dobiju na raspolaganje podjednak dio kapaciteta mreže, tj. da ne bude privilegiranih, kao ni oštećenih korisnika.

U najjednostavnijem obliku, kod mreža bez rezervacije kapaciteta, pravednost bi trebala težiti za dodjelom jednakog dijela prijenosnog kapaciteta mreže svakom korisniku. U stvarnosti, problemi nastaju zbog različitih potreba korisnika, odnosno zbog različitih putova kojima njihovi podaci prolaze kroz mrežu. Optimalno bi bilo za svakog korisnika odrediti kanal najmanjeg kapaciteta, tzv. usko grlo (Bottleneck), te mu taj kapacitet rezervirati na svim ostalim kanalima. Nakon toga, preostali kapacitet kanala dijeliti na korisnike koji ga mogu stvarno i iskoristiti.

Kod mreža s rezervacijom kapaciteta, prednost se daje korisniku koji je prvi zatražio uslugu. Ukoliko mreža nije u stanju ispuniti traženu uslugu, zahtjev korisnika se odbacuje (kontrola pristupa).

### 2.5.2.3 Funkcije elemenata mreže

Elementi mreže, čvorišta i terminali (prijemnici i predajnici) imaju različite uloge u ostvarivanju funkcije kontrole toka na mreži.

**Čvorišta** primaju pakete s dolaznih i usmjeravaju ih ka odlaznim kanalima. Pri tome pakete spremaju u redove čekanja za odlazne kanale. Paketi se iz reda čekanja na kanal šalju prema algoritmu posluživanja, koji treba osigurati ugovorenu kakvoću posluživanja, te razdvajati tokove pojedinih korisnika radi zaštite od onih koji ne poštuju ugovorene parametre. Razlikujemo posluživanje bez posebnog algoritma (FIFO, First in First out), stohastičke i determinističke algoritme.

- FIFO, poslužuje korisnika čiji je zahtjev prvi pristigao, u slučaju popunjenosti memorije odbacuje paket koji je posljednji stigao (drop-tail).

- Stohastički, odbacuje pakete slučajno (npr. RED, Random Early Detection), zasniva se na pretpostavci da korisnik koji šalje više paketa od optimalnog, ima veći broj paketa u redu, te je

vjerojatnost odbacivanja njegovih paketa veća. Funkcionira u uvjetima jako opterećene mreže, odnosno u režimu rada s dugačkim redovima čekanja.

- Deterministički, vodi računa o svim tokovima podataka i donosi odluku o individualnom posluživanju svakog paketa (npr. FQ, Fair Queuing) koji pokušava simulirati fiksno multipleksiranje na razini okteta. Mana mu je velika potrebna količina obrade kod posluživanja svakog paketa.

Pri tome je **tok podataka** svaki niz podataka (PDU) koji čvorište smatra jedinstvenom cjelinom, te nad njim obavlja funkcije kontrole toka. Pod **multipleksiranjem** podrazumijevamo postupak kojim se više tokova nadređene razine šalje istim tokom promatrane razine. Rezolucija čvorišta je sposobnost čvorišta da ukupni tok podataka kroz neki kanal dijeli finije ili grublje na individualne tokove. Rezolucija se može kretati od niske, kada razlikujemo samo izvorišnu i odredišnu podmrežu, preko srednje, kada identificiramo parove terminala, do visoke, kada identificiramo parove korisničkih procesa, uključujući i mogućnost da isti korisnici razmjenjuju više tokova istovremeno.

**Izvorišta** (predajnici paketa) primaju podatke s nadređene razine i formiraju pakete (segmentacija), te donose odluku o trenutku slanja paketa. Poslani paket se čuva do prijema potvrde radi eventualnog ponovnog slanja (retransmisije). Ako je detektiran gubitak paketa, npr. izostankom potvrde u predviđenom vremenu ili prijemom dupliciranih potvrda, paket se ponovo šalje na mrežu. Izvorište obavlja algoritme kontrole toka donoseći odluku o brzini slanja paketa i širini prozora.

**Odredišta** (prijemnici paketa) primaju pakete i šalju potvrde kao odvojene kratke pakete, ili uključene u pakete toka podataka suprotnog smjera. Donose odluku o trenutku slanja potvrde i pomaku gornje granice prijemnog prozora radi izbjegavanja segmentacije korisnikovih podataka na male pakete. Za potrebe kontrole toka bitno je da se potvrda šalje za svaki primljeni paket i da kasni što manje. U slučaju poremećaja redoslijeda pristizanja paketa, odredište može ponoviti posljednju potvrdu (duplicirane potvrde).

#### 2.5.2.4 Detekcija zagušenja

Čvorišta i terminali mreže će na različite načine otkrivati pojavu zagušenja. Čvorišta raspolažu s podatkom o trenutnoj dužini redova na izlaznim kanalima, mogu voditi računa i o vremenu zadržavanja (kašnjenja) pojedinog paketa u čvorištu, ili pratiti učestalost gubitaka paketa zbog popunjenosti redova čekanja. Na osnovu toga će započeti s nekim od postupaka dojava izvorištima, odnosno koristit će podatke za potrebe algoritama usmjeravanja i odbacivanja paketa.

Osnovna posljedica zagušenja kod paketnih mreža je gomilanje paketa u memoriji čvorišta. Zbog toga raste kašnjenje na mreži, te nakon popune memorije dolazi do gubitaka paketa. Nestanak paketa izaziva istek vremenskih sklopova predajnika, koji u predviđenom vremenu ne primi potvrdu prijema. Istek vremena retransmisije (RTO) i povećano kašnjenje su implicitne indikacije zagušenja. Čvorišta mogu načinom rada potencirati ove indikacije, npr. unaprijednim selektivnim ili slučajnim odbacivanjem paketa (RED) i time ostvariti funkcije kontrole toka mrežne razine. Izvorišta nakon detekcije zagušenja trebaju smanjiti brzinu predaje, korištenjem nekog od algoritama predajnika.

Predajnici pojavu zagušenja mogu otkriti eksplicitno, dojavom sa čvorišta indikacije zagušenja ili podatka o dozvoljenoj brzini, ili implicitno, mjerenjem parametara prijenosa. To su podatak o kašnjenju potvrde, tj. o vremenu obilaska T ili RTT, (Round Trip Time), podatak o trenutnom prozoru W (window) i, nakon pojave preopterećenja, učestalost gubitaka paketa (ćelija).

Kod eksplicitne dojave, čvorovi nakon detekcije mogućeg zagušenja koriste rezervirana polja u zaglavljima PDU ili posebne PDU za dojavu zagušenja izvorištu. U izvorištu je potrebno ostvariti korištenje primljene indikacije na mrežnoj ili prijenosnoj razini. Poznat je niz konkretnih mehanizama eksplicitne dojave zagušenja. To su povratno korištenje kontrolnih poruka, povratno ili unaprijedno korištenje indikatora, te eksplicitna dojava optimalne brzine predaje.

Povratne kontrolne poruke (npr. Source Quench kod ICMP protokola Interneta) čvorište šalje izvorištu kada odbaci paket zbog zagušenja. Izvorište treba smanjiti brzinu predaje, te time doprinijeti smanjenju zagušenja. U praksi se je pokazalo, da u uvjetima zagušenja kontrolne poruke doprinose



zagušenju, a istovremeno teško pronalaze put do izvorišta koja nastavljaju sa slanjem paketa nepromijenjenom brzinom.

Povratni indikatori su bitovi u zaglavlju PDU suprotnog smjera koje čvorište postavlja u jedinicu kada otkrije zagušenje (BCN, Backward Congestion Notification). Kada primi indikator, izvorište smanjuje brzinu predaje na polovinu. Kada nema indikatora zagušenja, izvorište udvostručuje brzinu u svakom periodu oporavka, koji je proporcionalan sa postignutom brzinom. Metoda ne doprinosi jednakosti korisnika. Problem se pojavljuje kod paketnih mreža, kada promet suprotnog smjera ne prolazi istim putem. Prednost metode je u skraćenom vremenu odziva.

Unaprijedni indikatori su slični povratnim, ali se koriste paketi koji putuju prema odredištu (EFCI, Explicit Forward Congestion Indication). Odredište kopira indikatore u pakete povratnog prometa, čime se rješava problem razdvojenog usmjeravanja. Kada primi indikaciju zagušenja, izvorište usklađuje brzinu predaje multiplikativnim smanjenjem, a kada indikacija izostane, povećava je aditivnim porastom (izvorišno upravljanje tokom). Druga je mogućnost da odredište na osnovu indikacije zagušenja korigira parametre kontrole toka (npr. širinu prozora) koji inače služe za usklađenje brzine među korisnicima (odredišno upravljanje tokom). Simulacije i praksa su pokazali da unaprijedna indikacija daje bolje rezultate od povratne, iako je kašnjenje duže.

Složeniji algoritmi omogućavaju dojavu mjere zagušenja, pa čak i optimalne brzine slanja paketa.

### 2.5.2.5 Filtriranje informacije

Kod eksplicitnih i implicitnih metoda dojave (detekcije) zagušenja pojavljuje se problem trenutnih promjena mjernih veličina. To su one promjene, koje nastaju zbog statističkih svojstava prometa na nižim vremenskim razinama, kraćim od vremena kašnjenja na mreži (trenutno zagušenje). Zbog toga je nužno trenutno mjerene vrijednosti filtrirati, kako bi se iz niza mjerenih vrijednosti dobila tražena informacija za višu vremensku razinu.

Problem filtriranja se komplicira činjenicom da je frekvencija uzorkovanja često varijabilna, da mjerni podaci kasne, da je podataka nekad premalo (frekvencija uzorkovanja preniska, naročito u uvjetima zagušenja), te da isti algoritam protokola koristimo za veze s vrlo kratkim, kao i za one s vrlo dugim kašnjenjem, odnosno vremenom obilaska.

Često korišteni algoritam filtriranja je eksponencijalno uprosječivanje, gdje se sukcesivni uzorci množe faktorom pojačanja  $\alpha$  i pribrajaju sumi, prethodno pomnoženoj s  $(1-\alpha)$ . Tako je udio  $i$ -tog prošlog uzorka proporcionalan s  $\alpha^i$ . Za neku veličinu  $x$  bit će:

$$x(n+1) = (1-\alpha)x(n) + \alpha m(n) \quad 2-3$$

gdje je  $m(n)$  trenutna izmjerena vrijednost. Prednost metode je u tome što ne zavisi o vremenu, a pogodnim izborom pojačanja realizira se cjelobrojnom aritmetikom.

### 2.5.2.6 Algoritmi predajnika

Nakon detekcije, odnosno dojave zagušenja, predajnik treba uskladiti brzinu predaje s nastalom situacijom. Taj postupak nazivamo kontrolom brzine predaje, odnosno algoritmom predajnika. Postavlja se problem određivanja nove brzine predaje, a s ciljem postizanja kakvoće usluge i pravednosti. Pri tome je nemoguće računati na centralizirane, već se treba osloniti na distribuirane algoritme predajnika.

Kod eksplicitnih dojava raspoloživog kapaciteta, predajnik jednostavno nastavlja odašiljanje novom dozvoljenom brzinom. Kod eksplicitne ili implicitne dojave zagušenja, podatak o raspoloživom kapacitetu nije poznat i korekcija brzine predaje odvija se na osnovu ugrađenih algoritama predajnika. Za slučaj zagušenja, predajnik će smanjiti brzinu, a za slučaj podopterećenja mreže, povećati će brzinu predaje. Pokazalo se je da je optimalan algoritam predajnika koji koristi aditivni porast kod podopterećene mreže, i multiplikativno smanjenje brzine kod pojave zagušenja. Na taj način korisnici koji nepravedno koriste veći dio kapaciteta brže smanjuju svoju brzinu, dok kod podjele novooslobođenog kapaciteta svi imaju podjednaku šansu.

Poznate su dvije grupe mehanizama kontrole toka predajnika, prozorska kontrola (window control) i kontrola brzine predaje (rate control).

**Prozorska kontrola** zasniva se na ograničenju broja paketa (ćelija) koje predajnik smije poslati prije nego dobije potvrdu prijema od odredišta. Prozor je apsolutno ograničen modulom numeracije PDU. Najveći dozvoljeni prozor ima vrijednost slobodnog dijela memorije prijemnika. Na taj se način sprječava slanje i prijenos paketa koje prijemnik ne bi bio u stanju primiti. Predajnik šalje brzinom koja ovisi o širini prozora prijemnika RWIN (Receiver Window) i vremenu obilaska T, prema formuli 2-2. Isti mehanizam moguće je koristiti za izbjegavanje zagušenja na mreži korekcijom širine prozora zagušenja CWIN (Congestion Window) nakon prijema implicitne ili eksplicitne dojave zagušenja. Predajnik šalje na mrežu onoliko paketa koliko je dozvoljeno prozorom zagušenja, a najviše onoliko koliko je dozvoljeno prozorom prijemnika:

$$L = \frac{\min(\text{RWIN}, \text{CWIN})}{T} \quad 2-4$$

Prozorska kontrola je prirodan način kontrole toka kada je kapacitet kojim se upravlja ograničen količinom memorije u čvorištima. Ona efikasno nadzire broj paketa u mreži. Mana je prozorske kontrole što ne nadzire efikasno ulazni promet, te izvorišta često generiraju praskove paketa.

**Kontrola brzine predaje** zasniva se na korekciji perioda emitiranja paketa, gdje je propusnost obrnuto proporcionalna periodu emitiranja paketa  $\tau$ :

$$L = \frac{1}{\tau} \quad 2-5$$

Predajnik smanjuje brzinu predaje radi izbjegavanja zagušenja. Prednost metode je u izbjegavanju praskova paketa, tako da se karakteristike predajnika približavaju determiniranom modelu izvorišta. Mana joj je što ne ograničava broj paketa u mreži i tako ne štiti spremnike čvorišta od popunjenosti. Kontrola brzine predaje je prirodan način kontrole toka kada je upravljani kapacitet ograničen brzinom prijenosa (komunikacijski kanal) ili obrade (usmjernik). Ona efikasno nadzire ulazni promet.

Zbog prednosti i mana dvaju pristupa, očekuje se primjena algoritama kontrole toka koji su kombinacija prozorske kontrole i kontrole brzine predaje. Kontrola brzine treba spriječiti pojavu praskova prometa, a prozorska kontrola spriječiti nekontrolirano popunjavanje redova u usmjernicima.