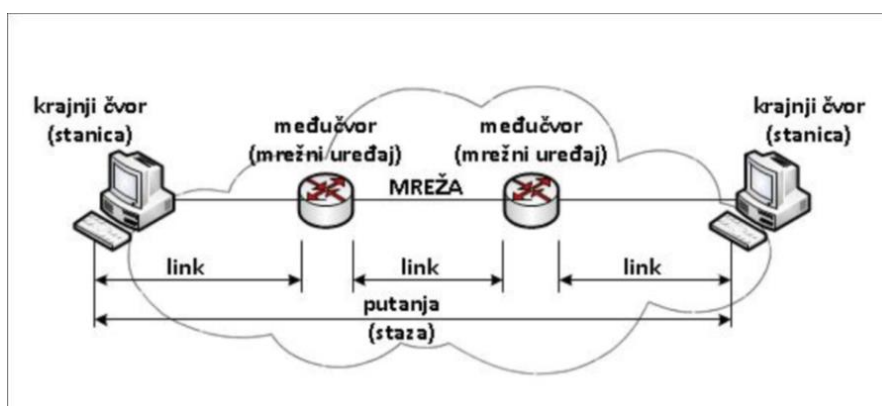


Računarske mreže III

1. Lokalne mreže – LAN

Prednosti umrežavanja i klasifikacija mreža

Računarska mreža je grupa povezanih samostalnih računara. Samostalni znači da svaki računar može sam da obavlja obradu podataka, ali po potrebi koristi resurse drugih uređaja.



Svaka stanica u okviru mreže naziva se čvor. Postoji više vrsta čvorova. Završna, krajnja stanica je završni čvor, a svaka između tih završnih čvorova međučvor. Kanal koji povezuje dva čvora naziva se link, a skup linkova i čvorova koji povezuju dve krajnje stanice nazivaju se putanje ili staze.



DTE – Data Terminal Equipment (uređaj koji generiše digitalne podatke, najčešće krajnji uređaji, računari...)

DCE – Data Circuit-terminating Equipment (uređaj koji podatke koji idu iz DTE-a prilagođava tako da mreža može da ih primi i obrnuto, odnosno digitalne podatke prilagođava medijumu za prenos, liniji preko koje se prenosi signal dalje proz mrežu)

Da bi umrežili dva računara potrebno je:

- Povezati ih
- Moraju da koriste iste protokole

Prednost umrežavanja:

- Deoba resurasa
- Jednostavna komunikacija

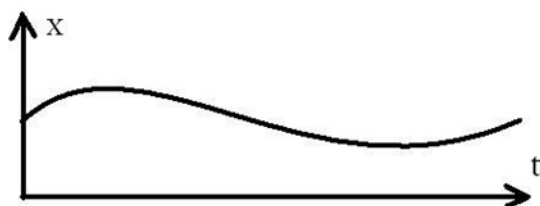
Primena mreže:

- Marketing i trgovina
- Finansijski servisi
- Proizvodnja (prijektovanje proizvoda i upravljanje proizvodom)
- Elektronska pošta
- Informacioni servisi
- Telekonferencija

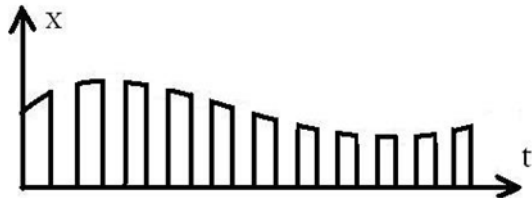
Poruka može biti:

- Kontinualna
- Diskretna
- Digitalna

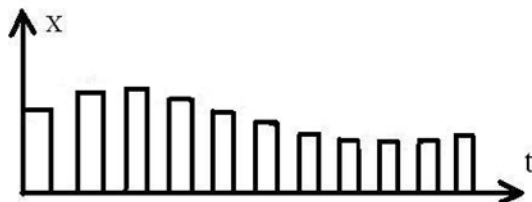
Kontinualne poruke vezane su za sisteme čija su stanja definisana u svakom trenutku tokom datog perioda posmatranja i koje u nekom određenom opsegu imaju beskonačno mnogo stanja. Kontinualne poruke prirodno se predstavljaju kontinualnim, odnosno analognim signalima.



Diskretne poruke vezane su za sisteme koji imaju definisana stanja u određenim vremenskim intervalima. Signali koji služe za prenos diskretnih poruka mogu se predstaviti u obliku impulsa, pri čemu amplituda može imati beskonačan broj vrednosti u datom opsegu. Da ne bi prenosili ceo signal, prenose se samo neki delovi signala tako da se signal može verno rekonstruisati. U kratkim vremenskim intervalima, periodima, pratimo kretanje signala (propustimo signal), tako da signal može imati bilo koju trenutnu vrednost, nemamo nikakvih ograničenja.



Ako signal postoji samo u diskretnim vremenskim trenucima i pritom može da uzima samo konačan broj trenutnih vrednosti onda je reč o digitalnom signalu. Diskretan signal, odnosno delove signala koje smo propustili sada svodimo na neke unapred određene nivoe, tako da signal u datom (bilo kom) trenutku možemo predstaviti samo tačno određenim nivoom signala.



Klasifikacija računaskih mreža

Klasifikacija prema konfiguraciji linka:

- Tačka – tačka



- Tačka – više tačaka



Klasifikacija prema topologiji, najgrublje se dele na:

1. Difuzne mreže
2. Od tačke do tačke
 - a) Komutirane
 - i. Komutacija kola
 - ii. Komutacija paketa
 - b) Nekomutirane

1. Difuzne mreže: postoji samo jedan komunikacioni kanal koji koriste svi računari u mreži. To znači da kada neki korisnik pošalje neku poruku ona stiže do svih korisnika u mreži. Po prijemu poruke svaka stanica proverava adresu odredišta, ako vidi da poruka nije njoj namenjena odbacuje je, u suprotnom smešta je u svoj bafer i obrađuje je. Osnovni problem u ovim mrežama je definisati pristup zajedničkom medijumu za prenos, odnosno dodela kanala za prenos samo jednoj stanici da ne bi došlo do kolizije.

2. Karakteristika ove mreže je da su svake dve stanice povezane posebnim linkom. Nekomutirane mreže su mreže kod kojih postoji stalna veza između svih stanica povezanih tom mrežom. U ovim mrežama ne postoje međučvorovi. Komutirane mreže su mreže kod kojih postoji više veza između parova stanica, pa se podaci prenose kroz niz međučvorova, komutatora.

Prema načinu slanja:

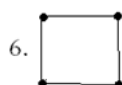
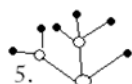
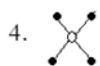
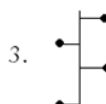
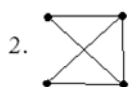
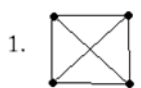
- Unicasting (stanica – stanica); poruka je namenjena samo jednoj stanici
- Multicasting (stanica – više stanica); poruka je namenjena grupi stanica
- Broadcasting (stanica – sve stanice); poruka je namenjena svim stanicama

Klasifikacija prema veličini:

- PAN – *Personal Area Network*, dometa prečnika od 4 do 6 metara
- LAN – *Local Area Network*, domet do par kilometara
- CAN – *Campus Area Network*, povezuje više LAN-ova u jednoj organizaciji
- MAN – *Metropolitan Area Network*, gradska mreža
- GAN – *Global Area Network*, mobilna komunikacija kroz proizvoljan broj bežičnih LAN-ova u oblasti pokrivenosti jednog satelita
- WAN – *Wide Area Network*, regionalna mreža, povezuje države i kontinente

Klasifikacija prema topologiji:

1. Potpuno povezane mreže
2. Nepotpuno povezane mreže
3. Magistrala
4. Zvezda
5. Stablo
6. Prsten



1. Svaki računar povezan je posebnim linkovima sa svim ostalim računarima u mreži. Ova topologija se retko koristi u praksi i to je nekomutirana mreža.

Prednosti: svaka stanica ima na raspolaganju pun kapacitet linka, ako dođe do prekida nekog linka prekida se veza samo između korisnika koji su bili povezani tim linkom, ostatak veze normalno funkcioniše.

Mane: sa porastom broja stanica naglo raste broj linkova, mali stepen iskorišćenosti linka.

2. Nepotpuno povezane mreže predstavljaju komutirane mreže, odnosno do svakog uređaja postoje bar dve putanje čime se obezbeđuje da ako dođe do prekida informacija može stići alternativnom putanjom. Upravo ova osobina čini ovu topologiju vrlo pouzdanom.

3. Magistrala je višetačkasta mreža u kojoj su sve stanice povezane na jedan komunikacioni kanal (najčešće na koaksijalni kabal) koga nazivamo magistrala. Svaka stanica je povezana preko završne linije i hardverskog interfejsa na magistralu. Na krajevima magistrale nalaze se terminatori koji apsorbiraju signal i sprečavaju refleksiju.

Prednosti koje se ostvaruju su laka instalacija i malo kablova.

Mane: ukoliko dođe do prekida magistrale ispadaju svi terminali, stanice iz komunikacije, i ograničeno je maksimalno rastojanje između krajnjih stanica i broj priključaka na magistrali. Ova ograničenja proističu iz slabljenja signala u kablju i refleksije signala na priključcima.

4. Zvezda: svi korisnici povezani su na interfejs haba i tako povezani u mrežu preko centralnog čvora. Haba prosleđuje poruke na sve portove bez obzira kome je namenjen paket, sve što stigne na jedan port prosleđuje se na sve ostale portove. Stoga je ova topologija logička topologija magistrala pa u jednom trenutku samo jedna stanica može da emituje signal.

Prednosti, ako dođe do prekida linka iz komunikacije ispada samo stanica koja je tim linkom vezana za hab, umrežavanje novih korisnika je jednostavno.

5. Stablo: ova topologija predstavlja generalizaciju topologije u obliku magistrale, tako da sva pravila koja važe za magistralu, važe i za stablo.

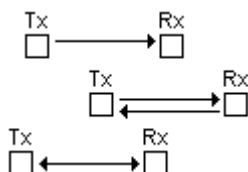
6. Prsten: ova mreža se sastoji od grupe regeneratora spojenih linkovima koji formiraju zatvorenu petlju. Za razliku od magistrale ne postoji krajnja tačka terminator, a sam prsten predstavlja skup linkova od tačke do tačke.

Prenos u prstenu odvija se samo u jednom smeru. Svaka stanica pored koje prolazi paket proverava adresu odredišta i ukoliko je paket upućen toj stanici kopira sadržaj paketa i paket nastavlja dalje. Paket se apsorbira kada napravi ceo krug, odnosno u regeneratore izvorne stanice. Broj regeneratora u prstenu ograničen je zbog kašnjenja koje unosi svaki od njih. Ako dođe do prekida nekog linka između regeneratora pada cela mreža.

Načini prenosa podataka

Prema smeru prenosa u telekomunikacionim mrežama razlikujemo tri vrste veze:

- Simpleks
- Poludupleks
- Dupleks



Simpleksna veza omogućava prenos samo u jednom smeru, jedan korisnik je uvek i samo predajnik, a drugi korisnik je uvek i samo prijemnik, tako da oni ne mogu da menjaju uloge.

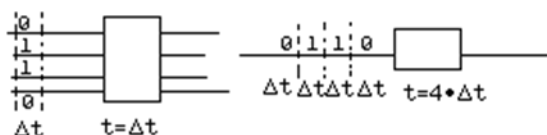
Poludupleksna veza omogućava prenos u oba smera, ali nikako u isto vreme, tako da dok jedan emituje signal drugi korisnik miruje i prima signal, odnosno u jednom vremenskom trenutku jedan uređaj radi isključivo kao predajnik, a drugi kao prijemnik. U narednom vremensko intervalu oni menjaju uloge.

Dupleksna veza omogućava nam istovremen prenos signala u oba smera, svaki korisnik može u isto vreme i da prima signal i da emituje signal, odnosno da se ponaša i kao prijemnik i kao predajnik.

Paralelni i serijski prenos podataka:

Kod serijskog prenosa podataka binarne reči se prenose samo kroz jednu liniju za prenos podataka, to znači da će stizati sukcesivno jedan za drugim. Vreme potrebno za prenos jedne reči određeno je brojem bita i vremenom prenosa jednog bita, tako da ako se prenosi jedan bajt potrebno vreme je 8 puta vreme prenosa jednog bita. Podaci između terminala i računara u mreži najčešće se prenose serijskom vezom.

Paralelna veza predstavlja vezu između dva uređaja i delova računara koja sadrži više paralelnih linija za prenos. Tako da ako prenosimo binarne podatke istovremeno se prenosi onoliko bitova koliko postoji linija za prenos podataka. Npr. ako se prenosi jedan bajt i imamo 8 linija za prenos ceo bajt će se preneti za vreme prenosa jednog bita. Najčešće se koristi na kretkim relacijama i udaljenostima.



Sinhroni i asinhroni prenos:

Kod asinhronog prenosa da bi izvršili sinhronizaciju prijemnika i predajnika neophodno je u kodne reči koje prenosimo ubaciti neke dodatne bite. Ti dodatni biti koji se utiskuju u kodnu reč najčešće se nalaze na početku i kraju kodne reči, tako da prijemniku damo informaciju kada počinje kodna reč (startni bit, najčešće 1) i kad se završava kodna reč (stop bit, najčešće 0). Karakteristika asinhronog prenosa je da raste broj bita prilikom slanja na liniji veze zbog ubacivanja dodatnih bita. Asinhroni prenos se koristi kod sistema gde nemamo čestu razmenu podataka već se koristi za rafalni prenos.

Sinhroni prenos podrazumeva kontinualni prenos podataka. Da bi se realizovao prenos podataka između prijemnika i predajnika neophodno je pre početka prenosa podataka realizovati sinhronizaciju. To se ostvaruje razmenom i prenošenjem niza bita za sinhronizaciju, odnosno sinhro grupom, najčešće 10010110. Ponavljanjem ove kodne reči izvrši se neophodno sinhronizovanje prijemnika i predajnika nakon čega je moguće obavljati nesmetani prenos podataka.

Komutirane mreže

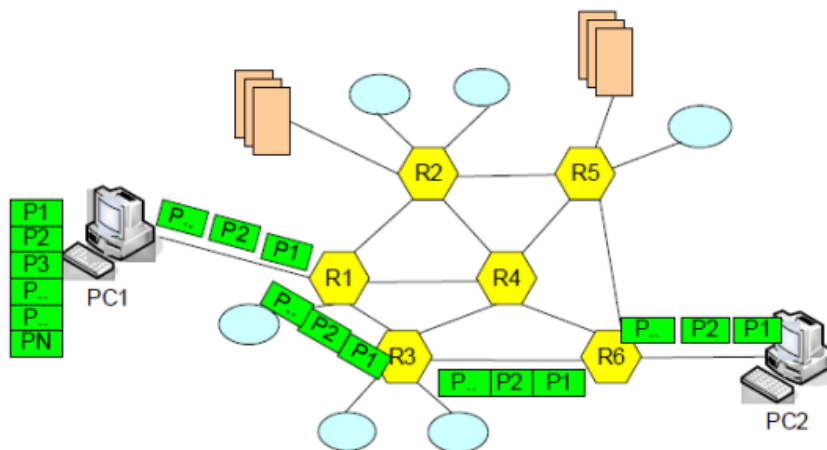
Komutirane mreže možemo podeliti na:

- Mreže sa komutacijom kola (linija, veza)
- Mreže sa komutacijom paketa

Mreže sa komutacijom kola:

Kod mreža sa komutacijom kola prenos podataka od izvora do odredišta obavlja se po sledećem principu: korisnik koji želi da pošalje podatke ka drugom korisniku obraća se mreži i šalje zahtev za uspostavom veze, odnosno traži od mreže da mu obezbedi liniju za prenos podataka. Mreža na osnovu trenutnog stanja u mreži i pomoću mehanizama koje poseduje traži optimalnu putanju i rezerviše linkove od početka do kraja.

Kada izvrši rezervaciju linkova fizički je uspostavljena konekcija prijemnika i predajnika tako da prenos podataka može da počne. Linkovi koji su rezervisani za datu konekciju između dva korisnika ostaju zauzeti, odnosno nedostupni za druge prenose sve dok se ne završi razmena podataka između ova dva korisnika, na taj način korisnici mogu da koriste pun kapacitet propusnog opsega koji poseduju ovi linkovi. Svi podaci idu samo jednom putanjom, onom kojom su rezervisani dati linkovi. Ukoliko dođe do prekida nekog linka, onemogućena je dalja komunikacija između dva korisnika.



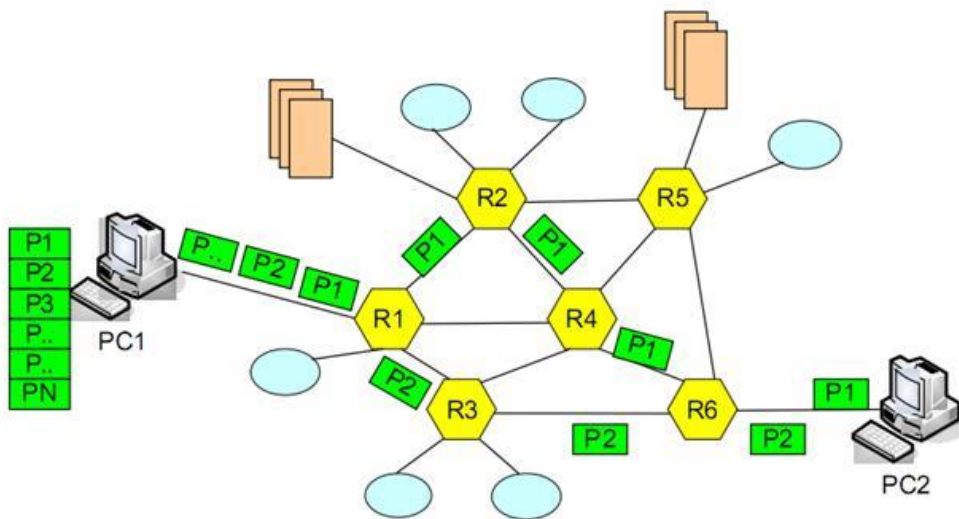
Mreže sa komutacijom paketa:

Mreže sa komutacijom paketa omogućavaju prenos podataka preko više konekcija. Kada se informacija prenosi preko mreže nije unapred poznata putanja kojom će se podaci prenositi.

Originalni podaci se rastavljaju na manje pakete. Svaki paket poseduje oznaku koja sadrži odredišnu adresu i identifikaciju rednog mesta u odnosu na druge pakete. Putanja kojom putuje svaki paket najbolja je aktivna putanja, odnosno najoptimalnija je putanja u datom trenutku slanja u zavisnosti od trenutnog stanja mreže, opterećenja i uslova prenosa.

Link kroz koji prolazi paket nije rezervisan samo za prenos jednog paketa, na čijoj se putanji nalazi dati link, tako da se može koristiti i za prenos drugog saobraćaja. Ukoliko dođe do prekida nekog od linkova nova trasa, nova optimalna putanja se formira na osnovu trenutnog stanja mreže i implementiranog protokola rutiranja, tako da je omogućeno da paket stigne do odredišta drugom putanjom.

Mreže sa komutacijom paketa su brže i efikasnije i poseduju sopstvene metode rutiranja saobraćaja. Finansijski su isplative za korisnika. Tarifiranje se vrši na osnovu ostvarenog saobraćaja.



Topologija LAN mreža

Lokalne računarske mreže najčešće se koriste za povezivanje računara na manjim udaljenostima, međutim da ne bi imali fizička ograničenja u razdaljini između računara i mrežnih uređaja, lokalnom računarskom mrežom smatra se mreža koja radi na drugom sloju OSI referentnog modela, odnosno sloju veze podataka. Ako se za njeno funkcionisanje, pravilan rad i razmenu poruka između krajnjih korisnika koriste samo funkcije i protokoli drugog sloja možemo je smatrati lokalnom mrežom.

Lokalne računarske mreže svrstavaju se u difuzne mreže što podrazumeva jedan komunikacioni kanal, odnosno jednu liniju za prenos podataka, tako da bilo ko da emituje neku poruku ona će stići do svih korisnika. Osnovni problem koji se ovde javlja je dodela zajedničkog kanala za prenos jednom korisniku da ne bi došlo do kolizije. Osim po samoj fizičkoj konfiguraciji mreže, LAN mreže možemo podeliti i prema protokolu koji se koristi za pravilnu raspodelu zajedničkog kanala za prenos.

Prirodu jedne LAN mreže određuje:

- medijum za prenos koji se koristi
- topologija mreže
- protokol za pristup medijumu za prenos

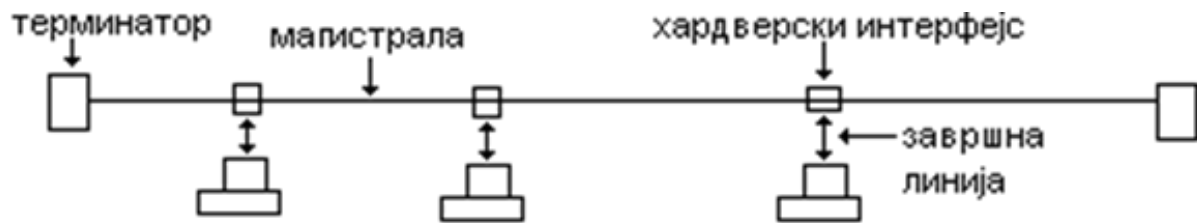
Kao medijum za prenos najčešće se koriste upredene parice zbog niske cene ili da bi iskoristili već postojeću infrastrukturu, instalacija u nekom objektu. Postižu se brzine do nekoliko Mb/s. Koaksijalni kabl pruža bolje performanse od upredenih parica ali gledano sa ekonomske strane predstavlja skuplju varijantu. Propusni opseg ovakvog medijuma za prenos omogućava realizaciju prenosa na većim brzinama. Koristi se i prenos u osnovnom opsegu i širokopojasni prenos, odnosno prenos više signala smeštenih u različite podopsege u isto vreme. Ako su neophodne velike brzine prenosa koriste se optički kablovi. Bežični prenos je još jedna vrsta realizacije LAN mreža.

Što se tiče topologija koje se koriste pojavljuju se magistrala, prsten, stablo i zvezde. Sve ove varijante predstavljaju logičku topologiju magistrala.

Topologija u obliku magistrale

Mreža u obliku magistrale predstavlja višetačkastu mrežu koja poseduje jednu liniju za prenos na koju su korisnici direktno povezani preko mrežnog hardverskog interfejsa. Na krajevima zajedničke linije za prenos nalaze se krajnje tačke ili terminatori koji imaju ulogu da zaštite kanal od eha, odnosno neželjenog vraćanja signala unazad. Kada jedan korisnik pošalje nešto na liniju za prenos, odnosno emituje neku poruku, ona se prostire na obe strane od interfejsa preko koga je prikačen taj korisnik duž linije za prenos. Na taj način signal dolazi do svih

korisnika u mreži. Korisnik kome je namenjena poruka (ram) prihvata poruku dok je ostali samo odbacuju.

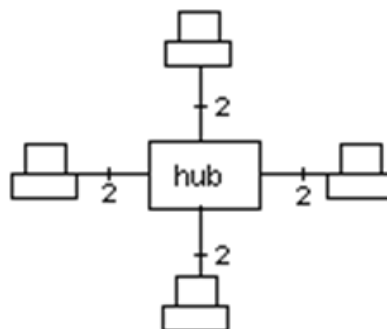


Pošto svi korisnici koriste istu liniju za prenos, za pravilan i uspešan rad cele mreže neophodno je da samo jedan korisnik vrši transmisiju podataka u jednom trenutku. Ukoliko dva ili više korisnika emituju istovremeno doći će do kolizije. Zato je naravno potrebno da postoji neki mehanizam u mreži za dodelu zajedničkog kanala za prenos korisnicima koji se nalaze u mreži, odnosno mehanizam za regulaciju pristupa medijumu za prenos.

Osnovne mane koje se javljaju kod ovakve konfiguracije su: ukoliko negde dođe do prekida zajedničke linije za prenos iz funkcije ispadaju svi korisnici, pravedna dodela u zavisnosti od potreba korisnika i obima saobraćaja linije za prenos je još jedan od problema, javlja se i problem snage emitovanja signala u zavisnosti od veličine mreže, dužine medijuma za prenos.

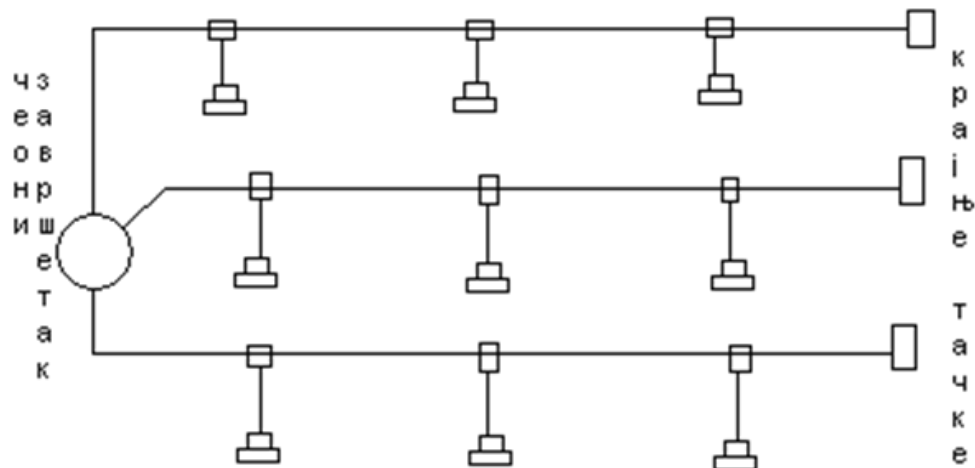
Topologija u obliku zvezde

Kod ove topologije svi korisnici vezani su za centralni čvor, zvezdastu spojnicu, tako da kao i kod magistrale emitovani ram stiže do svih korisnika. Ukoliko dođe do prekida nekog linka iz mreže ispada samo jedan korisnik koji je bio vezan tim linkom za centralni čvor.



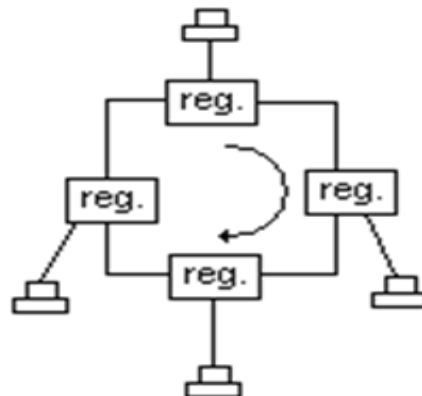
Topologija u obliku stabla

Sve što važi za topologiju magistrala ova topologija nasleđuje. Javlja se razlika u samoj fizičkoj realizaciji koja donosi neka poboljšanja u odnosu na magistralu. Stablo kreće iz čeonog završetka iz kog polazi više grana na koje su prikačeni krajnji korisnici. U slučaju emitovanja rama, signal se prostire duž svih grana i do svih korisnika. Poboljšanje se ogleda u tome da ukoliko da dođe do prekida nekog linka iz funkcionisanja, iz mreže ispadaju samo oni korisnici koji su priključeni na tu granu.



Topologija u obliku prstena

Ova mreža se sastoji od grupe regeneratora spojenih linkovima koji formiraju zatvorenu petlju. Za razliku od magistrale ne postoji krajnja tačka terminator, a sam prsten predstavlja skup linkova od tačke do tačke.



Prenos u prstenu odvija se samo u jednom smeru. Svaka stanica pored koje prolazi paket proverava adresu odredišta i ukoliko je paket upućen toj stanici kopira sadržaj paketa i paket nastavlja dalje. Paket se apsorbuje kada napravi ceo krug, odnosno u regeneratoru izvorne stanice. Broj regeneratora u prstenu ograničen je zbog kašnjenja koje unosi svaki od njih. Ako dođe do prekida nekog linka između regeneratora pada cela mreža.

Mreže ravnopravnih računara (Peer to Peer, P2P)

U mrežnoj arhitekturi ravnopravnih računara svaki računar ima podjednake mogućnosti i odgovornosti. Za P2P mreže važi:

- Nema namenskog servera niti hijerarhije računara
- Računari su jednostavno povezani u radnu grupu
- Svaki računar je istovremeno i klijent i server
- Ne postoji administrator koji odgovara za celu mrežu, odnosno korisnik sam određuje koji se resursi na njegovom računaru mogu deliti preko mreže

Prednosti:

- Peer2peer mreže su praktične za radne grupe do 12 računara, što je česta situacija u SOHO (Small Office Home Office) okruženjima gde svaki računar radi nezavisno i pamti podatke na svom hard-disku, ali može da ih deli sa svim ostalim računarima u mreži
- P2P mreža može da se definiše kao deljenje računarskih resursa i usluga pomoću direktne razmene, što nam nudi brojne tehničke prednosti
- Korisnici P2P mogu lako da formiraju svoje sopstvene online zajednice
- Zbog svoje jednostavnosti često su jeftinije od mreža zasnovanih na serverima

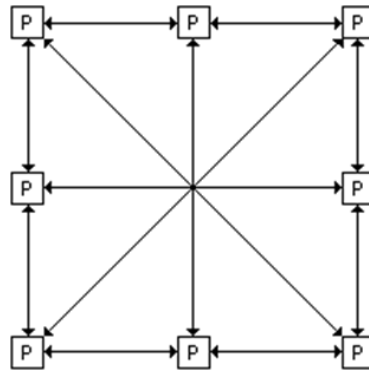
Mane:

- Velika slabost je bezbednost P2P. Svaki korisnik za sebe postavlja mere bezbednosti, a resursi koji se zajednički koriste mogu postojati na bilo kom računaru, pa je teško ostvariti centralizovanu kontrolu. Ovakva organizacija drastično ugrožava bezbednost mreže jer neki korisnici slabo primenjuju mere bezbednosti

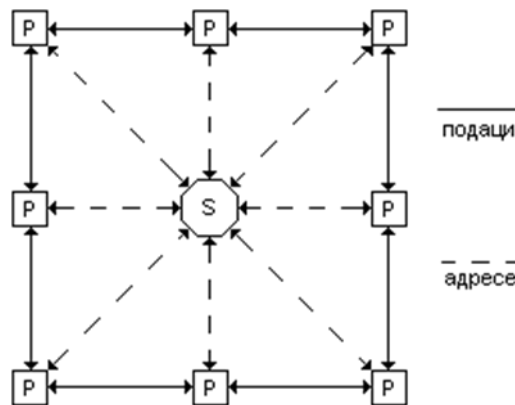
Podela prema stepenu centralizacije:

1. Decentralizovane
2. Centralizovane
3. Hibridne

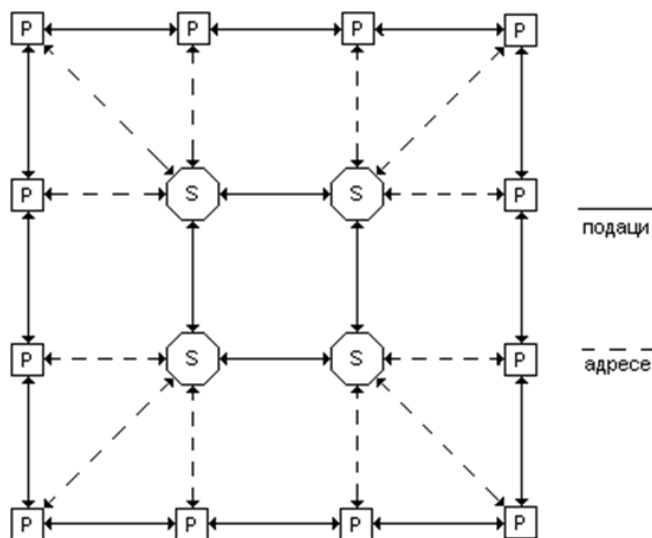
1. Decentralizovane su mreže kod kojih ne postoji centralni registar članova već se otkrivanje ostalih vrši preko internih protokola, najčešće korišćenjem broadcast poruka.



2. Centralizovane su mešavine P2P i klijent-server mreže. Postoji centralni server čiji je zadatak evidentiranje peer članova.



3. Hibridna arhitektura je centralizovana varijanta P2P mreže. Koristi se u slučajevima kada se mreža sastoji iz velikog broja čvorova i/ili uloga servera podrazumeva i dodatne operacije sem evidencije članova.



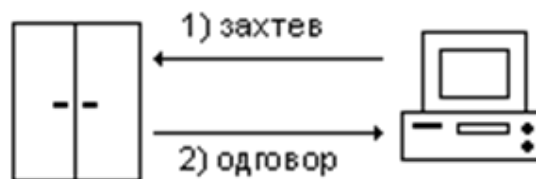
Peer2peer je najbolji izbor kada:

- Ima manje od 12 računara
- Se u mreži dele resursi, a ne treba server
- Bezbednost ne mora da bude na visokom nivou
- Mreža raste samo do određene granice

Klijent server mreže

Ovo je veoma česta konfiguracija, naročito ukoliko mreža sadrži veliki broj korisnika. Ovakav sistem se sastoji od više klijenata i jednog ili više servera. Klijent može da bude računar ili program. Server je takođe računar ili program i ima dva zadatka: pružanje usluga klijent-računarima i klijent-programima, i da nadgleda mrežu.

Na zahtev klijenta server obavlja poslove koje klijent ne može da realizuje, npr. zbog nedovoljne procesorske moći ili zbog nedostatka memorijskog prostora. Komunikacija se obavlja tako što klijent šalje zahtev serveru, server prima zahtev i obrađuje ga, a zatim šalje odgovor klijentu. Dakle klijent prvi započinje dijalekt.



Server može da obrađuje zahteve na dva načina:

- Iterativno i
- Konkurentno

1. Kod iterativnog načina obrade zahteva, server osluškuje čekajući zahtev klijenta. Nakon prijema jednog zahteva ostali se odbijaju ili čekaju u ulaznom baferu sve dok se prihvaćeni zahtev ne obradi i pošalje odgovor klijentu. Mane ovog sistema su manji broj zahteva obrađen po jedinici vremena, ali ostvarujemo prednost u jednostavnosti funkcionisanja.



2. Kod konkurentne obrade zahteva moguća je obrada većeg broja zahteva paralelno. To se omogućava pokretanjem novog procesa za obradu zahteva kod svakog klijentskog zahteva. Ostvarujemo prednost efikasnosti jer se vrši obrada većeg broja zahteva po jedinici vremena, ali sadrže manu kompleksnosti.



Specifičnosti mrežnog operativnog sistema

Osnovni zadatak OS je da upravlja resursima i da detalje hardvera i softvera sakrije od korisnika.

MOS omogućava povezivanje heterogenih računarskih sistema u mrežu, pri čemu svaki čvor u mreži ostaje nezavistan i upravlja svojim resursima.

Način rada

Proces u jednom čvoru se obraća MOS-u koji utvrđuje da li taj proces zahteva neke nelokalne resurse. Ukoliko je to slučaj MOS posmatranog čvora se obraća MOS-u koji poseduje tražene resurse i uz podršku lokalnog OS omogućava pristup tom resursu.

Iako je ovaj postupak jednostavan i omogućava deljenje resursa između heterogenih računarskih sistema ima 2 značajna nedostatka:

- Globalno upravljanje resursima nije moguće. Kao posledica sistem može da postane neuravnotežen, odnosno pojedini čvorovi su nezaposleni, a drugi preopterećeni, pa padaju performanse sistema.
- Ne zadovoljava transparentnost. Korisniku su vidljivi čvorovi i resursi u sistemu. On može da se priključi na udaljene resurse ili računare, ali za to mora da upotrebi određenu naredbu.

Prednosti:

- Heterogenost. Korišćenjem MOS-a omogućeno je da se više različitih heterogenih sistema poveže u cilju ostvarivanja međusobne komunikacije i deljenja sopstvenih resurasa i kapaciteta sa drugim korisnicima, kao i pristup udaljenim resursima.
- Nezavisnost stanica. Sve stanice ostaju i dalje nezavisne, samostalno upravljaju svojim resursima i samostalno iniciraju korišćenje resurasa drugih sistema.

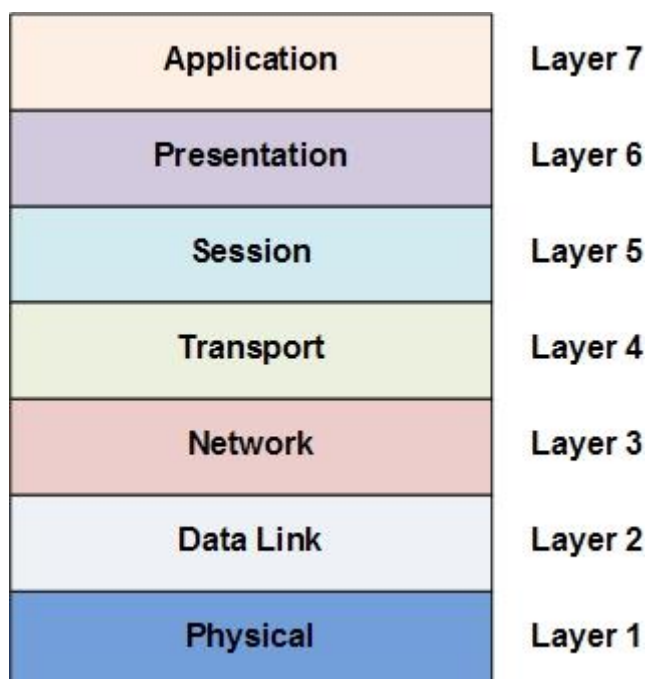
OSI (Open Systems Interconnection) referentni model

Međunarodna organizacija za standardizaciju ISO 1984. godine definisala je standard koji je poznat pod nazivom OSI (Open Systems Interconnection) referentni model. Naziva se „otvoreni sistem“ jer ne zahteva bilo kakve izmene u hardveru i softveru sistema koji komuniciraju, bez obzira na to koliko se oni razlikuju. **OSI nije protokol** već model koji ima za cilj da olakša razumevanje i projektovanje mrežne arhitekture (mrežna arhitektura – skup slojeva i protokola).

Pored OSI modela postoje i drugi modeli sa manje slojeva (npr. TCP/IP), ali svi ostali modeli definišu se preko OSI modele, odnosno upoređuju sa njim, tako da OSI model predstavlja reper za sve ostale modele. Pri pravljenju modela proces prenošenja informacije se razlaže na najelementarnije delove. Svaki sloj definiše skup funkcija koji se razlikuje od funkcija ostalih slojeva. Projektant modela raspoređuje funkcije i određuje broj slojeva.

Na svakom sloju definisane su potrebne funkcije i protokoli tako da se bez obzira na proizvođača uređaja i softvera koji koristi taj uređaj obezbeđuje univerzalnost u komunikaciji upotrebom i poštovanjem standarda koji su definisani u datim slojevima.

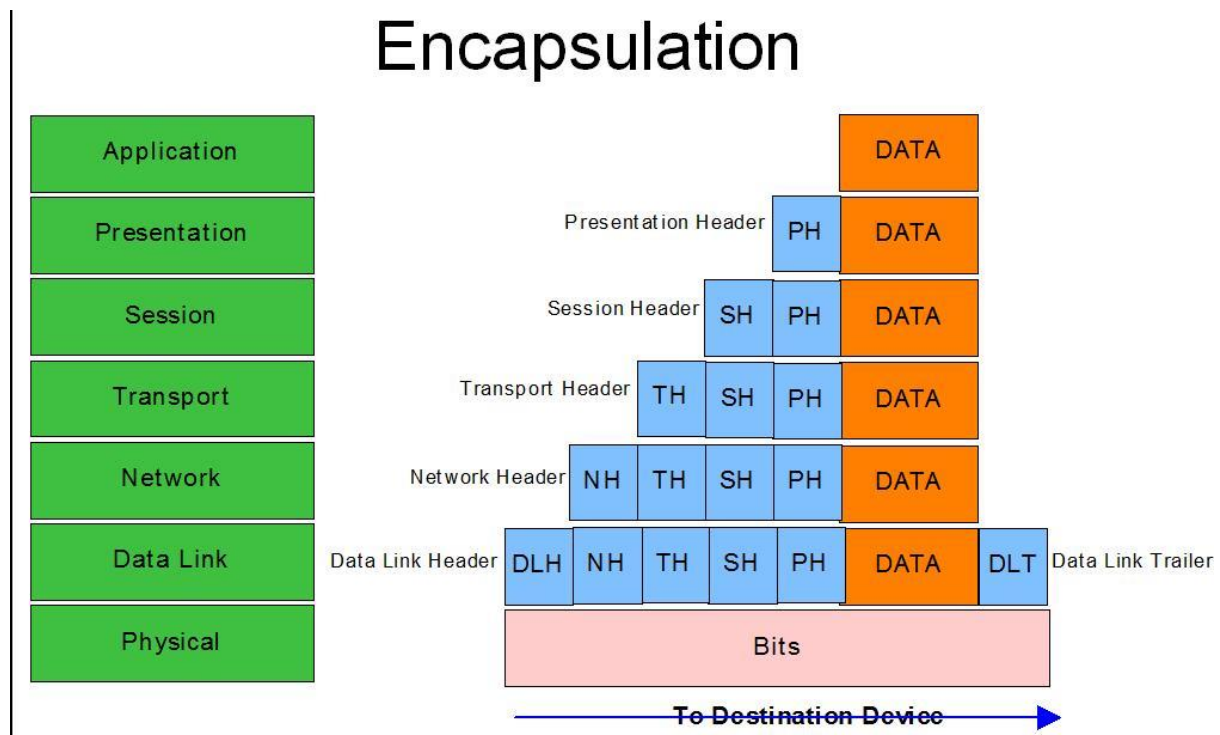
OSI referentni model se sastoji od 7 slojeva. Svaki sloj se oslanja samo na funkcije nižeg sloja i obezbeđuje usluge (servise, funkcije) višem sloju. Promene na jednom sloju ne zahtevaju izmene ostalih slojeva. Slojevi u OSI modelu kroz koje mora da prođe informacija na putu od izvora da odredišta su:



Svaki sloj ima svoju protokolsku jedinicu podataka (PDU-Protocol Data Unit) koju obrađuje, a generiše je dodavanjem svog zaglavlja odnosno repa na PDU iz višeg sloja. Niži sloj (n) ne

zna koji deo primljenog paketa višeg sloja (n+1) predstavlja zaglavlje a koji deo su podaci, on prihvata sve kao jednu celinu i dodaje svoja zaglavlja i rep koji sadrže odgovarajuća polja u skladu sa potrebama i funkcijama koje obavlja dati sloj.

Ovo prihvatanje PDU-a višeg sloja i dodavanje zaglavlja i repa, odnosno dodavanje novih polja na datom sloju naziva se **enkapsulacija**.



Protokol je skup pravila i konvencija koje se koriste u komunikaciji dva ista sloja različitih terminala (u stvarnosti ova komunikacija ne postoji, informacije se ne prenose između dva ista sloja).

Interfejs određuje operacije i usluge koje niži sloj nudi višem.

Osnovne funkcije slojeva definisanih OSI modelom su:

1. Fizički sloj:

- obezbeđuje transparentni prenos niza bita preko fizičkog medijuma za prenos (zadužen je za prenos sirovih bita preko datog medijuma za prenos, odnosno da obezbedi najoptimalniji način prenosa preko odgovarajućeg kanala koji se koristi za prenos)
- definiše: naponske nivoe, vreme trajanja bita, da li je veza dupleks, način uspostave i prekida veze, tip konektora (fizičke karakteristika signala koji se prnosi za prenos)

- interfejs između računara i modema predstavlja primer protokola fizičkog sloja (RS-232) (fizičke karakteristike konektora i portova, standardizacija i univerzalnost konektora i spojnice, standardizacija funkcija pinova)

2. Sloj veze:

- fizičko adresiranje (MAC adrese)(korisnici, uređaji se razlikuju po svojoj MAC jedinstvenoj adresi koja se sastoji od 48 bita predstavljenih heksadecimalnim brojevima, prva polovina brojeva označava fabriku, proizvođača, a druga serijski jedinstveni broj uređaja)
- formiranje rama (jedinica podataka na ovom sloju je frame, ram ili okvir, u zavisnosti od protokola koji se koristi veličina varira, kao i polja u ramu, paket sa trećeg sloja upakovan je u ram, tako da drugi sloj ne vidi sadržaj paketa, postoji i polje sa izvorišnu i odredišnu MAC adresu)
- kontrola pristupa zajedničkom medijumu (protokoli za raspodelu pristupa, žetoni, ovde se definišu protokoli za raspodelu vremena korišćenja zajedničkog medijuma za prenos jer su mreže koje rade na ovom nivou difuzne, logička magistrala, pa je neophodan mehanizam za smanjenje verovatnoće nastanka kolizije u mreži)
- upravljanje protokom
- kontrola greške (neki od mehanizama za utvrđivanje nastanka grešaka pri prenosu, samo utvrđivanje bez retransmisije i ispravke)
- sloj zadužen za kontrolu protoka na jednom linku

3. Mrežni sloj:

- prenos podataka s kraja na kraj mreže (prenos podataka sa kraja na kraj mreže, od izvora do odredišta kroz celu mrežu, odnosno prenos jednog paketa, ruta kojom paketi prolaze određuje se na ovom sloju na osnovu IP adrese i protokola koji se koristi za rutiranje)
- logičko adresiranje (IP)
- rutiranje (statičko, dinamičko, protokoli za rutiranje određuju najoptimalniju putanju na osnovu trenutnog stanja i uslova mreže i mehanizma koji se koristi)
- kontrola zagušenja (kontrola zagušenja u na raskrsnim čvorovima)
- fragmentovanje paketa
- povezivanje heterogenih mreža
- organizacija mreže u slučaju otkazivanja u uslovima jednog ili više otkaza

4. Sloj transporta:

- segmentacija i desegmentacija (poruka se deli na pakete i utvrđuje se pravilan redosled paketa, veličina paketa zavisi od protokola koji se koristi)

- potpuno povezuje dva kraja mreže (isporuka cele poruke ne samo paketa, vodi se računa pri prijemu paketa da se pre rekonstrukciji poruke redosled paketa ispoštuje)
- prenos bez gubitaka i grešaka (mehanizmi za ispravku grešaka kod neispravnih paketa i mehanizmi za slanje obaveštenja za retransmisiju izgubljenih paketa izvoru)
- postoji garantovani QoS (Quality of Service)

5. Sloj sesije (session – period komunikacije):

- upravljanje dijalogom (uspostava, održavanje i uljudno raskidanje veze-raskidanje po završetku slanja podataka i svih potrebnih koraka)
- umetanje kontrolnih tačaka - omogućava da ukoliko dođe do kvara u toku prenosa, nije potrebno reemitovati ceo fajl ponovo, već samo deo od poslednje kontrolne tačke posle koje je došlo do kvara
- upravljanje komunikacijom između aplikacija

6. Sloj prezentacije:

- šifrovanje
- kodovanje
- kompresija
- enkripcija
- bavi se sintaksom i semantikom prenetih informacija
- omogućava komunikaciju između računara koji podatke prezentuju na potpuno različite načine

7. Sloj aplikacije:

- softver (aplikacija) koji generiše podatke koje treba preneti
- protokoli koji služe da obezbede direktnu interakciju korisnika i računara
- primer protokola za prenos hiperteksta (Hypertext Transfer Protocol HTTP)

Primeri poznatih protokola na određenim nivoima:

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
	Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
	Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	Transport Layer	TCP, UDP
Internet Layer	Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Link Layer	Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
	Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Bežične mreže

Medijum koji se koristi kod sistema koji koriste bežični prenos je etar (vazduh).

Tehnike prenosa koje se koriste za bežični prenos su:

- Konvencionalni prenos (prenos u osnovnom opsegu, infra red, radio...)
- Tehnike proširenog spektra (osnovna karakteristika je da se koristi mnogo veći opseg od minimalno potrebnog opsega za prenos signala)

Topologije bežičnih mreža:

- Ad – hoc
- Celularne (ćelijske)
- Point-to-point

Za realizaciju ad – hoc mreža nije potrebna postojeća infrastruktura, svaka stanica (čvor) se ponaša kao komutator, svič.

Pri realizaciji ćelijske topologije neophodna je postojeća infrastruktura (bazna stanica). Svodi se na činjenicu da se jedno geografsko područje deli na određeni broj manjih područja pokrivenosti, odnosno ćelije. Svaka ćelija ima pristupnu stanicu koja emituje i prima signale uređaja koji su u njenom dometu.

U point-to-point topologije spadaju sistemi sa usmerenim antenama i zračenjem, sa ciljem da antena na jednoj strani šalje signal ciljano u određenu tačku na kojoj se nalazi druga stanica sa antenom, tako da je signal namenjen samo njoj.

Radio prenos: Podela frekvencijskog opsega

ULF	0,3 – 3 KHz	Koriste se za prenos na velike daljine
VLF	3 – 30 KHz	
LF	30 – 300 KHz	
MF	0,3 – 3 MHz	AM radio, navigacija
HF	3 – 30 MHz	
VHF	30 – 300 MHz	FM radio, VHF TV
UHF	0,3 – 3 GHz	UHF TV
SHF	3 – 30 GHz	Koriste se za satelitski prenos
EHF	30 – 300 GHz	

U – Ultra

L – Low

F – Frequence

V – Very

M – Medium

H – High

S – Super

E – Extremely

Za emitovanje na većini frekvencija neophodna je dozvola. Za frekvencije manje od 9 KHz nije potrebna dozvola, takođe i za ISM opseg nije potrebna dozvola, oko 2, 4 GHz i oko 5,1 GHz. (ISM – Industrial, Scientific and Medical radio band)

Načini propagacije signala:

1. Površinski (VLF, LF)



2. Troposferski (MF)



3. Jonosferski (HF)



4. Zemaljski direktni (VHF, UHF)
5. Kosmički direktni (SHF, EHF)

2. Ethernet

Razvoj Etherneta 802.3

Ethernet predstavlja skup pravila (protokola) kojim se definiše (standardizuje) način prenosa podataka između računarskih sistema u okviru LAN mreže koju čine veći broj stanica (računara) priključenih na zajednički prenosni medijum, zajednički medijum za prenos.

Ethernet standard definiše:

- Strukturu Ethernet okvira (*Ethernet frame*)
- Standardizovano značenje pojedinih polja frejma
- Skup pravila za fer pristup deljenom prenosnom kanalu
- Fizički medijum za prenos signala

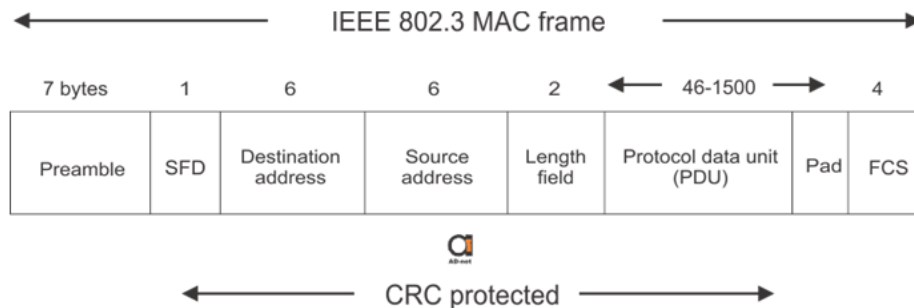
Struktura Ethernet i 802.3 frejma

Standard IEEE 802.3 odnosi se na lokalne mreže sa perzistentnim CSMA/CD protokolom. Opisuje celu familiju CSMA/CD sistema koji rade različitim brzinama i sa različitim medijuma.

Ethernet strogo gledano predstavlja verziju CSMA/CD sistema sa protokom od 10Mb/s.

802.3 standard u ramu ima polje koje definišu dužinu, a u Eternetu polje koje definiše tip. Eternet danas podrazumeva 802.3 mreže.

Eternet je tehnika difuznog prenosa sa raspodeljenim (decentralizovanim) upravljanjem pristupu medijumu za prenos pri čemu usluga nije pouzdana već najbolja moguća. Difuzna - jer svaka poruka stiže do svih stanica. Raspodeljeno upravljanje pristupu medijumu - u mreži ne postoji centralni arbitar koji daje pravo stanici da emituje. Najbolja moguća – izvor ne dobija obaveštenje da li je poruka stigla ili ne (ako se ne detektuje kolizija tokom slanja smatra se da je poruka ispravno stigla).



Svaki ram počinje preambulom koja je dugačka 7 bajtova, a svaki bajt predstavlja niz od po četiri naizmenične jedinice i nule 10101010. Osnovna svrha preambule je sinhronizacija prijemnika sa predajnikom.

SFD Start of Frame Delimeter (Flag) dolazi posle preambule dužine jednog bajta i označava početak samog rama i ima strukturu 10101011.

Slede polja od po 6 bajtova i to adresa odredišta i adresa izvorišta.

Sledi polje od 2 bajta koje označava ili (Type) tip koje ukazuje na protokole višeg sloja ili (Length) dužinu koje ukazuje na dužinu polja sa podacima.

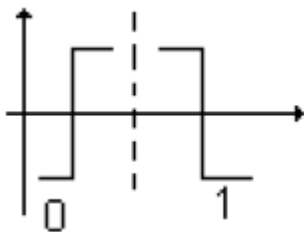
Polje za podatke je dužine do 1500 bajtova.

Polje dopune ima dužinu od 0 do 46 bajta. Da bi se otkrila kolizija pre nego što se završi sa prenosom rama, ram mora da ima minimalnu dužinu. Neophodno je otkriti da je do kolizije došlo pre nego što izvor završi sa emitovanjem rama, jer u suprotnom kolizija uopšte neće biti detektovana, a ram će biti izgubljen. Sve ovo posledica je toga što po Ethernet standardu smatramo prenos uspešnim ukoliko u toku emitovanja ne detektujemo koliziju (pošto ne postoji potvrda o prijemu). Da bi se otkrila kolizija, ram bez preambule i SFD polja treba da bude veličine 64 bajta. Ukoliko ram ne zadovolji ove uslove usled male veličine polja podataka onda se u polje dopune upisuju nule sve dok ram ne dostigne veličinu od 64 bajta.

CRC pilje se nalazi na kraju, veličine je 4 bajta i koristi se za proveru ispravnosti rama, odnosno vrši se provera ciklične redundantnosti.

Standardne vrste Eterneta

Svi Ethernet standardi sa protokom od 10Mbit/s koriste mančester kod.



Kabliranje

Najčešće se koriste 4 tipa kabliranja, svaka verzija 802.3 ima maksimalno dozvoljenu veličinu segmenta.

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Protokoli za pristup medijumu za prenos

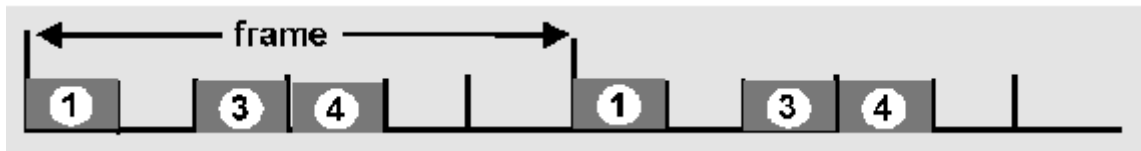
U svim difuznim mrežama glavni problem koji se javlja je dodela kanala za prenos samo jednom korisniku u trenutku kada više korisnika želi da emituje signal. Protokoli koji obezbeđuju da ne dođe do kolizije i koji regulišu ovako nastalu situaciju pripadaju sloju veze podataka. Osnovna podela načina dodeljivanja medijuma podrazumeva:

1. Statičko dodeljivanje kanala (FDMA, TDMA), unapred utvrđeno vreme slanja i frekvencijski podopseg kanala i nije pogodan za primenu u računarskim mrežama gde je saobraćaj uglavnom rafalni.
2. Dinamičko dodeljivanje medijuma (Aloha, Slot Aloha, CSMA), linija za prenos se dodeljuje krajnjim korisnicima za emitovanje u zavisnosti od trenutne situacije i uslova u mreži.

MAC protokoli sa podelom kanala: TDMA

TDMA: deljivi pristup sa vremenskom podelom (Time Division Multiple Access):

- pristup kanalu se obavlja kružno, u ciklusima
- svaki čvor dobija vremenski interval fiksne veličine (slot) u svakom ciklusu
- ako nema podataka za slanje, slot je prazan (neiskorišćen)

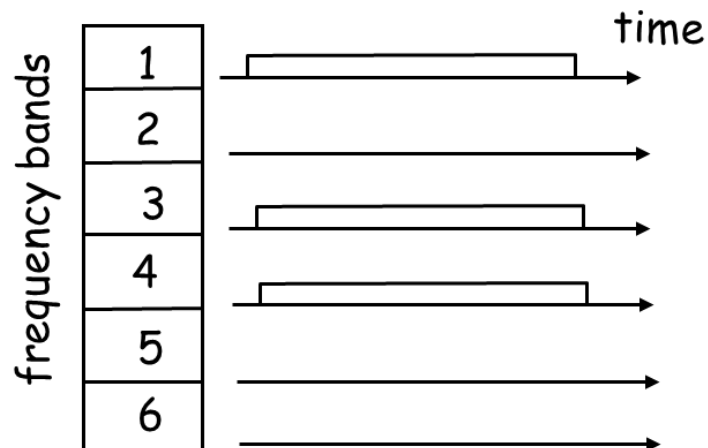


Primer: LAN sa 6-stanica, 1,3,4 imaju pakete, slotovi 2,5,6 prazni.

MAC protokoli sa podelom kanala: FDMA

FDMA: podela frekvencija (Frequency Division Multiple Access):

- kanalni spektar podeljen na frekvencijski bandove
- svakoj stanici dodeljen fiksni frekvencijski band (kao kod radio stanica)
- ako nema podataka za slanje, ne koristi se (ostaje prazan)



Primer: LAN sa 6-stanica, 1,3,4 imaju pakete, frekvencijski opsezi 2,5,6 prazni.

Protokoli sa slučajnim pristupom (Random Access Protocols)

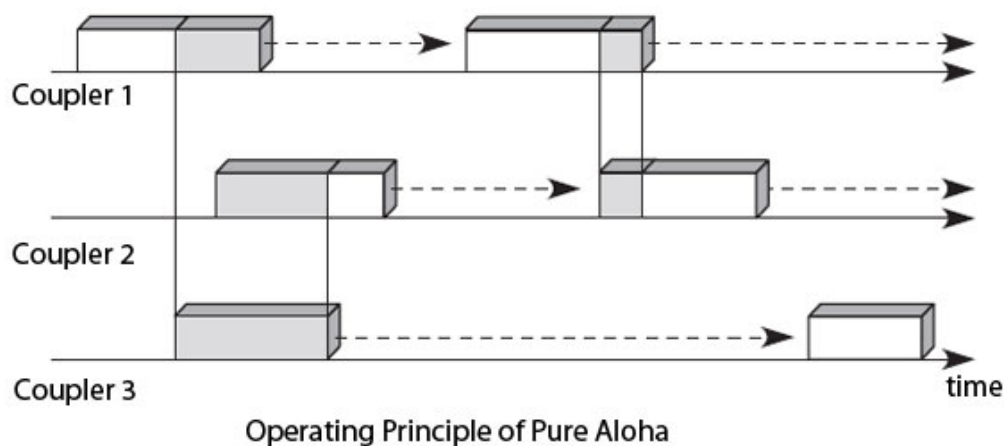
Random access MAC protokoli:

- ALOHA
- Slotted ALOHA
- CSMA, CSMA/CD

Aloha

Osnovna ideja kod ovakvog načina realizacije dodele zajedničkog medijuma za prenos krajnjem korisniku je sledeći: korisnik kada ima nešto za slanje automatski emituje ram bez obzira da li je linija zauzeta ili ne. Nema mehanizma da sazna da li je linija zauzeta ili ne. Ukoliko je došlo do kolizije, istovremenog slanja rama dva ili više korisnika, korisnici poseduju mehanizam za detektovanje kolizije i čekaju nasumično određeni vremenski trenutak, pa ponovo šalju ram na liniju veze.

Ukoliko je došlo do preklapanja makar i jednog bita između dve i više poruka različitih korisnika, retransmisija ramova se obavlja u celosti, odnosno ponovo se šalju celi ramovi nakon slučajno izabranog trenutka.



Iskorišćenost linka je 20% i nije potrebno izvršiti sinhronizaciju. Ovakav način slanja nije pogodan za mreže sa velikim brojem korisnika koji imaju potrebe za čestom razmenom informacija, podataka.

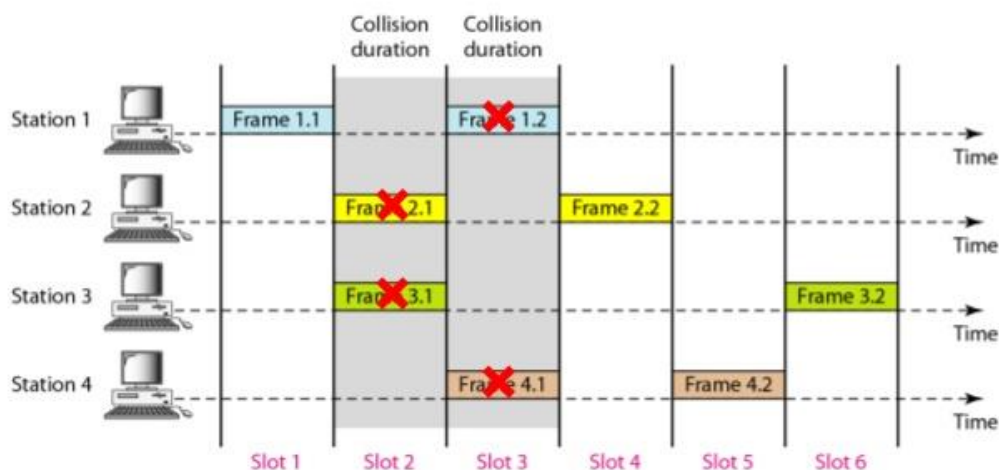
Slot Aloha

Kod slot Alohe izvršeno je poboljšanje radi bolje iskorišćenosti zajedničke linije za prenos. Vreme se deli na jednake vremenske slotove određene dužine tako da ram može da stane u svaki od ovih slotova. Sve stanice su sinhronizovane i znaju tačno kada počinju slotovi. Svaka stanica može da emituje samo na početku slota.

Princip rada slot Alohe:

- Stanica ima okvir za slanje, čeka početak slota i ceo okvir, ram šalje na liniju veze, odnosno predaje linku.
- Ukoliko ne dođe do kolizije u početku slota, znači da nijedna druga stanica nije emitovala ram u tom slotu, pa prenos će biti uspešno obavljen.
- Ukoliko se pojavila kolizija u toku slota, stanica to detektuje pre kraja slota. Pre početka sledećeg slota stanica generiše slučajan broj u intervalu od 0 do 1. Ako je broj manji od 0,5 stanica ne emituje u sledećem slotu. Za naredni slot ponovo generiše broj između 0 i 1 i sve tako redom dok broj ne bude veći od 0,5. Tada stanica, korisnik emituje ram u sledećem slotu. Postupak se ponavlja sve dok se ne izvrši uspešno slanje rama.

Slotted ALOHA



Maksimalna iskorišćenost kanala kod slot Alohe je 37%. Ovo poboljšanje smo dobili zbog vremena u kom traje kolizija i odbacivanja ramova. Zapravo kod Alohe ako se i jedan bit preklopi sa drugim ramom odbacuju se oba zbog nastale kolizije i potrebno je ponovo izvršiti slanje ramova. Vreme koje se izgubi je najmanje vreme trajanja jednog rama ako se u

potpunosti preklope ramovi, do skoro vreme trajanja dva rama ako se preklope poslednji bit jednog i prvi bit drugog rama. Kod slot Alohe preklapanje ramova može da nastane samo u granicama jednog vremenskog slot, tako da je vreme neiskorišćenosti kanala, odnosno izgubljeno vreme zbog nastale kolizije kraće.

CSMA protokoli (Carrier Sense Multiple Access Protocols)

Kod sistema koji koriste Alohu za raspodelu dodele medijuma za prenos signala, generalno gledano iskorišćenost kanala je mala jer korisnici koji imaju nešto za slanje otpočinju slanje odmah bez obzira da li je kanal zauzet ili nije. Tek nakon što su pokušali slanje signala utvrđuju da li je došlo do kolizije ili nije. Potrebno je uvesti mehanizam koji će doneti takvo poboljšanje da korisnici pre slanja osluškiju da li je kanal zauzet ili nije, pa tek onda da započnu slanje podataka ukoliko je zajednička linija slobodna. To se postiže novim protokolom CSMA.

Ovakav protokol, kao i što samo ime kaže, protokol sa ispitivanjem nosećeg signala, pomaže u boljem iskorišćenju kanala za prenos tako što korisnici ne emituju signal kad oni to žele, već prvo stanice moraju da osluškiju da li je linija slobodna za transmisiju, pa tek onda ukoliko je slobodna da pošalju podatke kroz zajedničku liniju za prenos. Postoje tri osnovna protokola ovakve vrste:

- Perzistentni CSMA
- Neperzistentni CSMA
- CSMA sa detekcijom kolizija (CSMA/CD (CSMA with Collision Detection))

Perzistentni CSMA radi na sledećem principu. Korisnik koji želi nešto da pošalje preko mreže prvo ispituje zajedničku liniju za prenos da li je slobodna, odnosno da li je neko već zauzeo sa slanjem podataka. Ukoliko je slobodna otpočinje slanje svojih podataka. Da ne bi došlo do kolizije ukoliko je linija za prenos zauzeta korisnik ne šalje ništa, već i dalje ostaje u fazi osluškivanja i bez prekida osluškuje liniju dok se ne oslobodi i kreće u slanje rama.

Ukoliko dođe do kolizije stanica će sačekati izvestan period, slučajno odabrano vreme, i ponovo započeti postupak osluškivanja. Bez obzira na osluškivanje kanala za prenos, nosećeg signala, i ako se utvrdi da je linija slobodna, može doći do kolizije. Ona može nastati ako dva ili više korisnika otpočinu slanje podataka, rama, u isto vreme. Takođe usled određene brzine prostiranja signala datom linije veze ili zbog udaljenosti korisnika koji imaju nešto za slanje, usled kašnjenja signala i vremena propagacije signala od jednog do drugog kraja, jedan korisnik može pomisliti da je linija slobodna bez obzira što je drugi korisnik započeo slanje podataka, rama. Tako da je kolizija ovako nastala verovatnija ako je linija veze sporija i ukoliko su veće udaljenosti korisnika.

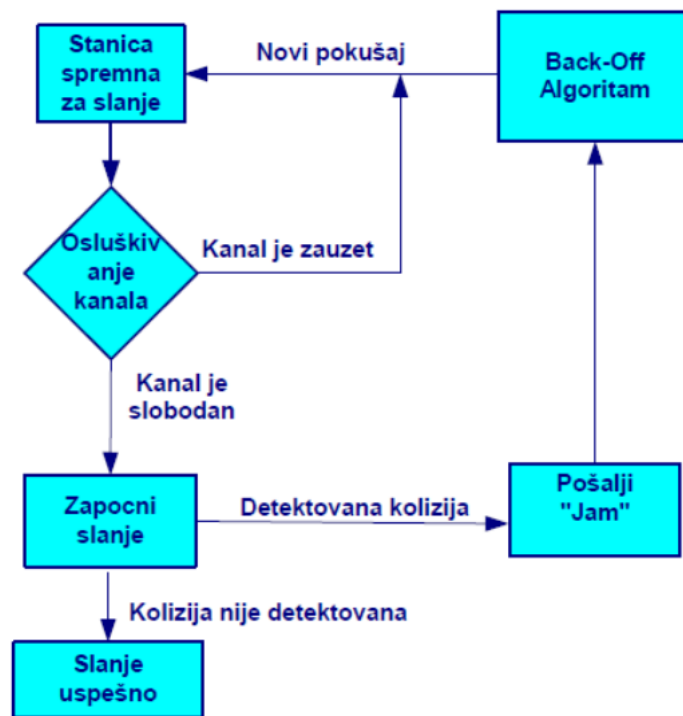
Neperzistentni CSMA za razliku od perzistentnog kod kog korisnik neprekidno ispituje liniju veze sve dok ona ne bude slobodna, funkcioniše tako da korisnik koji ima nešto za slanje osluškuje liniju za prenos, ukoliko je zauzeta, korisnik čeka određeni vremenski period pa ponovo osluškuje da li je slobodna. Ostali postupak je isti.

CSMA/CD

Ova verzija protokola unosi još jedno poboljšanje. Ukoliko dođe do kolizije korisnici, stanice na osnovu strukture nosioca signala, naponskog nivoa, širine opsega poslatog i primljenog signala, utvrđuju da je došlo do kolizije i automatski prekidaju slanje signala. Nakon određenog vremenskog perioda, slučajno odabranog, ponovo ispituju, osluškuju liniju veze.

Da bi pravilno mreža funkcionisala ako je implementiran ovaj protokol potrebno je ispuniti sledeće uslove i pravila:

1. Okvir koji treba da se prenese kroz liniju veze potrebno je smestiti u privremenu memoriju.
2. Pri osluškivanju kanala, kanal je slobodan ako niko ne otpočne slanje signala određeni vremenski period, po 802.3 standardu to je vremenski period trajanja 96 bita. Ukoliko za ovaj vremenski period kanal ostane slobodan korisnik može da otpočne emitovanje. Ako je kanal zauzet čeka se da se kasnije oslobodi, odnosno ispituje se ponovo nakon određenog vremenskog perioda.
3. Dok prenosi ram stanica, korisnik osluškuje da li je neko u međuvremenu započeo emitovanje, tako da može doći do kolizije, ako niko nije započeo slanje u tom periodu smatra se da je ram uspešno poslat.
4. Ako je stanica otkrila signale drugih stanica, odnosno ako neko u isto vreme vrši emitovanje signala, stanica zaustavlja emitovanje i šalje na liniju veze signal zagušenja kako bi signalizirala ostalim stanicama da je došlo do zagušenja (po 802.3 standardu signal zagušenja traje 48 bita).
5. Posle prekida slanja rama stanica ulazi u fazu eksponencijalnog odstupanja. Tačnije bira se slučajni vremenski period čekanja do ponovnog ispitivanja, osluškivanja linije veze iz unapred utvrđenog skupa vremenskih perioda. Nakon n-te kolizije za taj ram koji želi da pošalje bira vrednost k iz skupa $\{0,1,\dots,2^m-1\}$ gde je $m=\min[n,10]$, i po standardu 802.3 stanica čeka $k*512$ vremenskih intervala trajanja jednog bita, a zatim se vraća na korak 2.



Npr:

Posle 1. kolizije k se bira iz skupa $\{0,1\}$

Posle 2. kolizije k se bira iz skupa $\{0,1,2,3\}$

Posle 2. kolizije k se bira iz skupa $\{0,1,...,7\}$

...

Posle 11. kolizije k se bira iz skupa $\{0,1,...,1023\}$

Magistrala sa žetonom (IEEE 802.4 standard)

Ovakva konfiguracija organizovana je po principu zajedničkog kanala za prenos, ali korisnici su logički organizovani u konfiguraciju prsten, odnosno svaki korisnik zna po adresi koji korisnik mu se nalazi sa leve, a koji sa desne strane. Korisnici su numerisani u krug, počinje se od korisnika sa najvećim brojem. Dozvola za slanje predstavljena je žetonom. Samo korisnik koji poseduje žeton može da šalje podatke, kako u mreži postoji samo jedan žeton, u bilo kom trenutku samo će jedan korisnik moći da šalje podatke pa neće doći do kolizije.

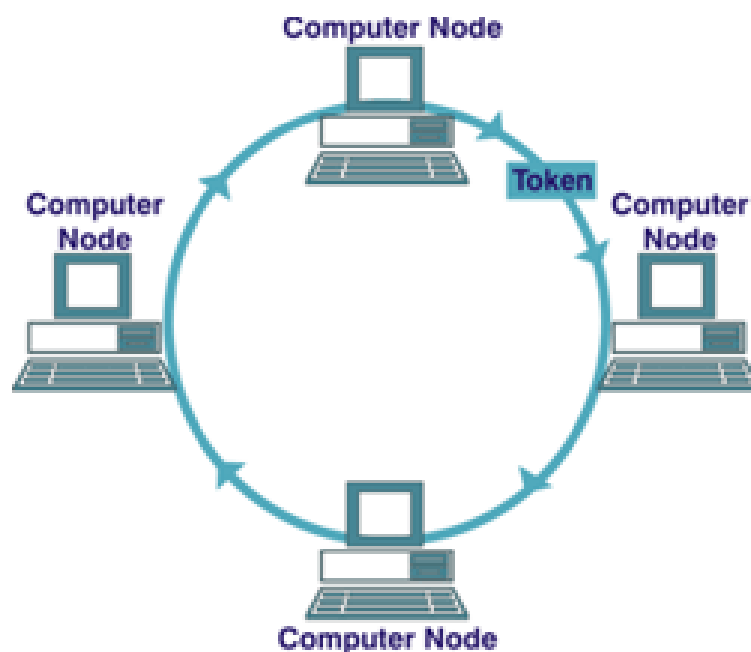
Žeton u stvari predstavlja ram od nekoliko bajtova čiji je sadržaj unapred utvrđen tako da korisnici mogu da ga prepoznaju. Posedovanje žetona, odnosno krug počinje od korisnika sa najvećim brojem. Kada završi slanje žeton se prosleđuje do sledećeg suseda i sve tako redom, ali pravo na slanje ima samo korisnik koji poseduje žetom. U zavisnosti od unapred dogovorenih uslova vreme slanja jedne stanice je ograničeno, nakon čega prosleđuje žeton sledećem korisniku.

Ukoliko se neki korisnici naknadno fizički priključe na liniju za prenos, i dalje se ne nalaze u logičkog prstenu, krugu za deljenje zajedničkog kanala sve dok ih protokol 802.4 ne uključi u redosled primanja žetona i ne dodeli im broj.

Ram koji korisnik emituje stiže do svih korisnika, na osnovu odredišne adrese odgovarajući korisnik će primiti paket njemu namenjen, ostali će odbaciti paket.

Prsten sa žetonom (IEEE 802.5 standard), Token Ring

Ovim standardom definiše se fizička konfiguracija mreže u obliku prstena i njeno pravilno funkcionisanje i raspodela zajedničkog kanal za prenos krajnjim korisnicima. Korisnici se fizički spajaju u krug linkovima i na taj način dolazi do realizacije mreže u obliku kruga, prstena. Pravo na emitovanje da ne bi došlo do kolizije realizuje se pomoću žetona.



Žeton u ovom slučaju predstavlja ram od tri bajta čiji je sadržaj unapred određen i poznat svim korisnicima. Žeton kruži od korisnika do korisnika u jednom smeru, i samo korisnik koji poseduje žeton može da emituje podatke na mrežu prema ostalim korisnicima. Postoje dva stanja krajnjih korisnika. U stanju osluškivanja korisnik očekuje ili korisne podatke ukoliko su

namenjeni njemu, prepoznaje ih prema odredišnoj adresi, ili žeton, odnosno ram sa poznatim sadržajem ukoliko ima nešto za slanje. Kada prihvati žeton on delimično promeni sadržaj tog rama i enkapsulira ga u poruku koju šalje. Sada se nalazi u stanju slanja. Kada poruka obiđe ceo krug korisnik je dužan da vrati ram u prvobitno stanje i vrati ga u prsten, mrežu, sledećem korisniku kako bi neko drugi mogao da koristi liniju za prenos.

Problem koji se ovde javlja je dužina prstena jer u zavisnosti od brzine prenosa potrebno je da ceo ram stane na liniju veze, odnosno da ceo ram stane u prsten. Da ne dođe do situacije da žeton obiđe ceo krug, a još nije završeno njegovo emitovanje na liniju veze ka drugom korisniku.

HDLC (High-level Data Link Control)

HDLC protokol je protokol sloja veze podataka i koristi se za sinhroni prenos podataka. Ovaj protokol predstavlja preteču X.25 protokola i koristi se u konfiguracijama tačka-tačka, kao i u višetačkastim vezama, u poludupleksnom i dupleksnom režimu. Takođe podržava režim rada u mreži i ravnopravnih računara i podređenih/nadređenih računara.

HDLC definiše tri vrste stanica:

1. Primarna stanica je odgovorna za upravljanje vezom. Primarna stanica je nadređena stanica koja inicira komunikaciju i poruke koje generiše ka drugim stanicama nazivaju se naredbe.
2. Sekundarna stanica je podređena primarnoj stanici, odnosno radi pod njenom kontrolom. Generiše poruke koje se nazivaju odgovori koji predstavljaju odziv stanice na upućene zahteve, naredbe sekundarne stanice.
3. Kombinovana stanica sadrži i odlike i primarne i sekundarne stanice. Ima sposobnost da generiše i naredbe i odgovore.

HDLC definiše dve konfiguracije veze:

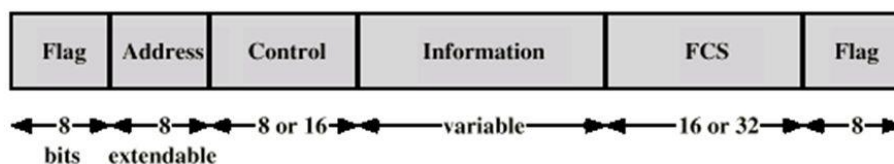
1. Nebalansirana konfiguracija podrazumeva realizaciju mreže pomoću jedne primarne i jedne ili više sekundarnih stanica. Koristi se u vezama tačka-tačka i višetačkastim mrežama i podržava i poludupleksni i dupleksni prenos.
2. Balansirana konfiguracija sastoji se od dve kombinovane stanice i koristi se samo u vezama tačka-tačka, podržava i poludupleksni i dupleksni režim.

HDLC definiše tri načina (moda) rada pri prenosu podataka:

1. Normalni mod predstavlja u stvari nebalansiranu konfiguraciju i to na sledeći način. Postoje primarna i sekundarna stanica. Primarna stanica inicira prenos i razmenu podataka, odnosno inicira, ostvarivanje sesije sa sekundarnom stanicom slanjem zahteva i naredbi sekundarnoj stanici. Sekundarna stanica generiše poruke u obliku odgovora samo kad dobije zahtav od primarne stanice. Često se koristi u konfiguraciji mreže kad jedan računar proziva više terminala koji su vezani za centralni računar. Takođe se koristi i u konfiguraciji tačka-tačka.
2. Asinhroni balansni mod predstavlja balansiranu konfiguraciju. Bilo koja kombinovana stanica može da inicira poziv ili da odgovori na nečiji zahtev bez traženja odobrenja od neke druge kombinovane stanice. Dupleksna veza koja se realizuje na ovakav način je efikasnija jer nema gubljenja vremena oko prozivanja sagovornika na drugoj strani.
3. Asinhroni mod predstavlja sličnu konfiguraciju kao i normalni mod, odnosno koristi se nebalansirana konfiguracija ali sa jednom razlikom. Sekundarna stanica ima mogućnost da inicira prenos podataka i bez prethodnog traženja dozvole od primarne stanice. Primarna stanica i dalje zadržava odgovornost kontrole linije i otkrivanja greške ali sekundarna stanica može da šalje podatke i bez dozvole primarne stanice.

HDLC protokol koristi format poruka koji se sastoji od šest polja. Imamo polje korisnih podataka koji treba da se prenesu, 24 u zaglavlju i 24 u repu. U zaglavlju postoje 8-bitna polja: polje (niz bitova) koji označavaju početak rama, polje za adrese i polje podataka za upravljanje. U repu razlikujemo dva polja: 16-bitno polje za kontrolnog zbira i 8-bitno polje koje označava završetak rama.

HDLC Frame Structure



(a) Frame format

Početak i završetak rama označeni su nizom bitova 01111110 koji označavaju početak na jednom kraju i završetak rama na drugom kraju rama. Ukoliko u korisnim podacima, bitovima postoji niz od šest uzastopnih jedinica ili više, potrebno je detektovati ovakav niz i prekinuti ga ubacivanjem 0 na odgovarajućem mestu posle pet uzastopnih jedinica da se ne bi prenela pogrešna informacija o početku i kraju rama. Na prijemu potrebno je odgovarajućim mehanizmom rekonstruisati pravilno niz, odnosno izbaciti ubačene nule.

Polje adresa značajno je za identifikaciju odgovarajuće stanice ukoliko postoji više stanica u realizovanoj mreži.

U upravljačkom polju smeštaju se upravljačke naredbe, redni broj rama ukoliko je kompletna informacija podeljena u više ramova za prenos, podaci za potvrđivanje prijema rama na prijemnoj strani.

Polje podataka nema definisanu dužinu ali se vodi računa da dužina ovog polja ne bude prevelika da ne bi došlo do povećanja verovatnoće preške pri prenosu podataka.

U polju kontrolnog zbira vrši se provera ispravnosti pristiglog paketa i utvrđivanja grešaka nastalih prilikom prenosa rama kroz liniju za prenos.

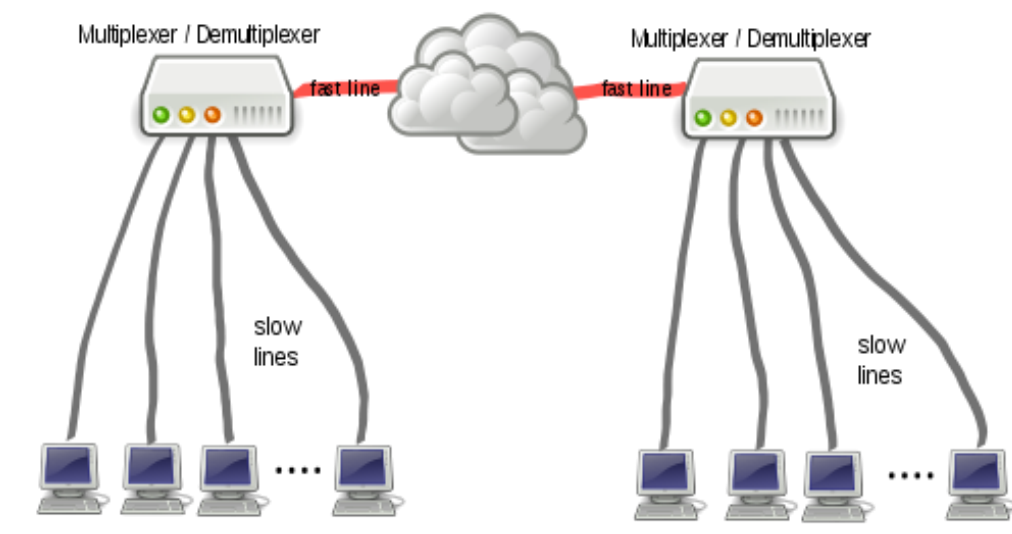
3. Aktivni mrežni uređaji

Multiplekser

Multiplekser je uređaj koji omogućava povezivanje više ulaznih linija na jednu izlaznu liniju, odnosno prenos više signala iz različitih izvora preko jedne linije veze. Multiplekser se nalazi na strani na kojoj se šalje signal. Za dupleksni prenos potreban je multiplekser na drugoj strani i na kraju svake linije demultiplekser. Multiplekser ukupan frekventijski opseg ili vreme korišćenja linije veze raspoređuje korisnicima određenim mehanizmom tako da korisnici imaju utisak kao da je linija veze samo njihovo.

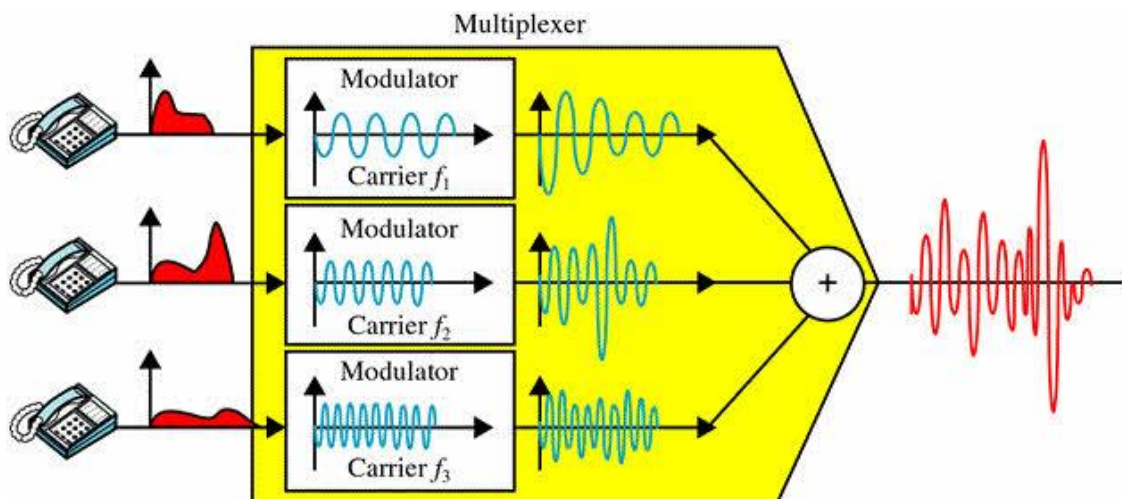
Postoje dva tipa multipleksera:

- Multiplekser sa frekvencijskom raspodelom kanala
- Multiplekser sa vremenskom raspodelom kanala

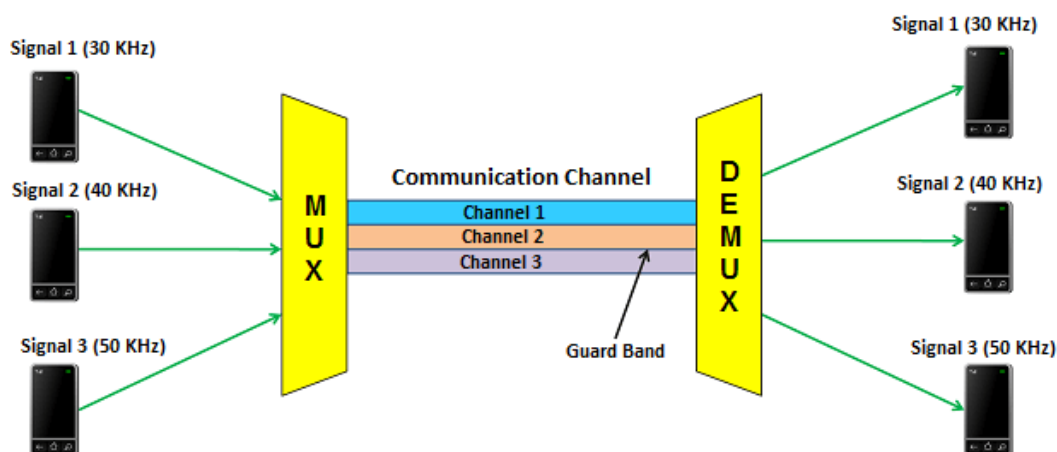
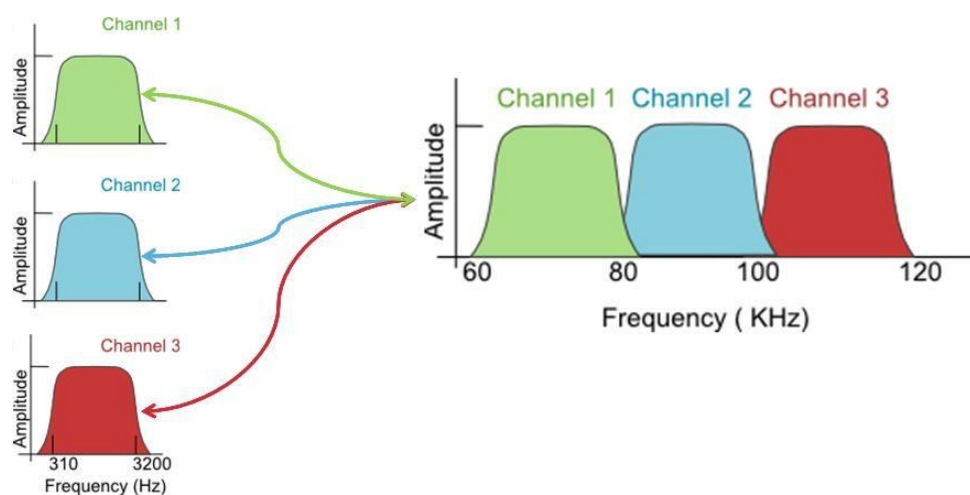


Multiplekser sa frekvencijskom raspodelom kanala

Kod multipleksa sa frekvencijskom raspodelom kanala dozvoljeni propusni opseg kanala koji podržava data linija veze (u zavisnosti od vrste kanala koji se koristi, fizičkih karakteristika) deli se na manje podopsege i dodeljuje odgovarajućim izvorima, korisnicima. Tako da je cela linija veze podeljena na uže, manje kanale, i to tako da između njih postoji mali razmak ili zaštitna zona da ne bi došlo do mešanja ili interferencije signala.



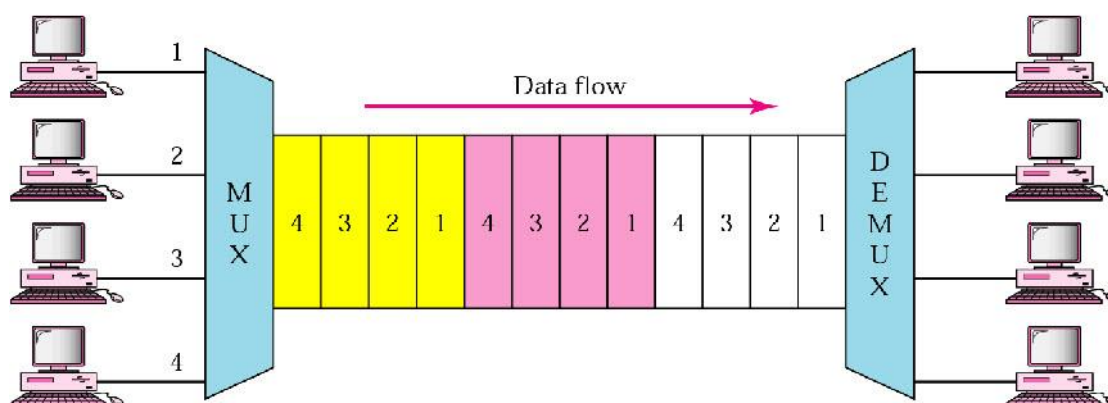
Dolazeći signali koji je potrebno preneti preko linije veze u multiplekseru se modulišu nekom frekvencijom i na taj način translira, pomeru u tačno odgovarajući kanal, frekvencijski podopseg. Modulacija se vrši nekom nosećom frekvencijom tako da na liniji veze sada dobijamo analogni signal za prenos koji se konvertuje u digitalni u demultiplekseru na prijemu. Spektar signala svakog korisnika, izvora smešta se u odgovarajući frekvencijski podopseg na multiplekseru.



Frequency Division Multiplexing

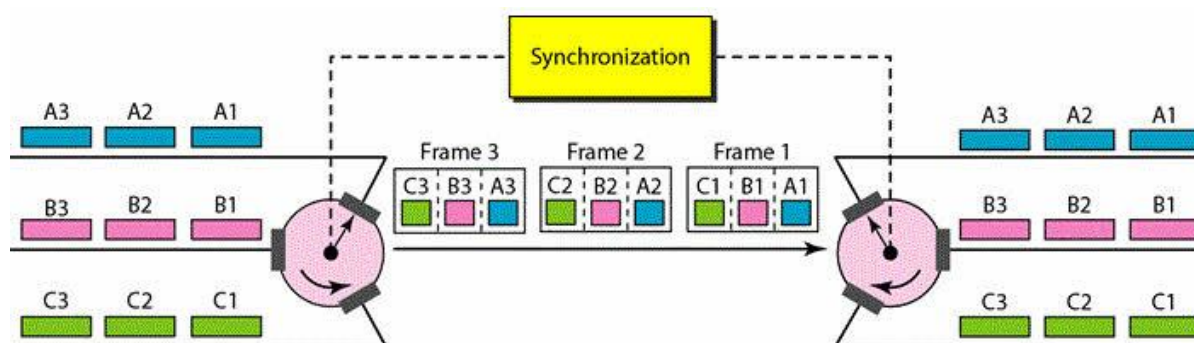
Multiplekser sa vremenskom raspodelom kanala

U slučaju multipleksera sa vremenskom raspodelom signala svakom korisniku se dodeljuje fiksni vremenski interval da koristi liniju za prenos. Taj vremenski interval možemo posmatrati kao vremenski slot. Korisnici imaju tačno određeno vreme kada smeju da koriste liniju za prenos, tako da u jednom vremenskom trenutku samo jedan korisnik može da vrši transmisiju podataka preko linije veze. Podaci u različitim vremenskim slotovima poređani su jedan za drugim tako da imamo neprekidno slanje podataka na liniji veze, na prijemu demultiplekser raspoređuje pristigle podatke odgovarajućim korisnicima.



Vremenski slotovi se raspoređuju korisnicima ravnomerno, pa u zavisnosti od veličine tih slotova ukoliko neki korisnik nema ništa za slanje imaćemo praznine u prenosu podataka na vezi, odnosno neiskorišćenost maksimuma linije veze, što predstavlja manu.

w



Koncentrator

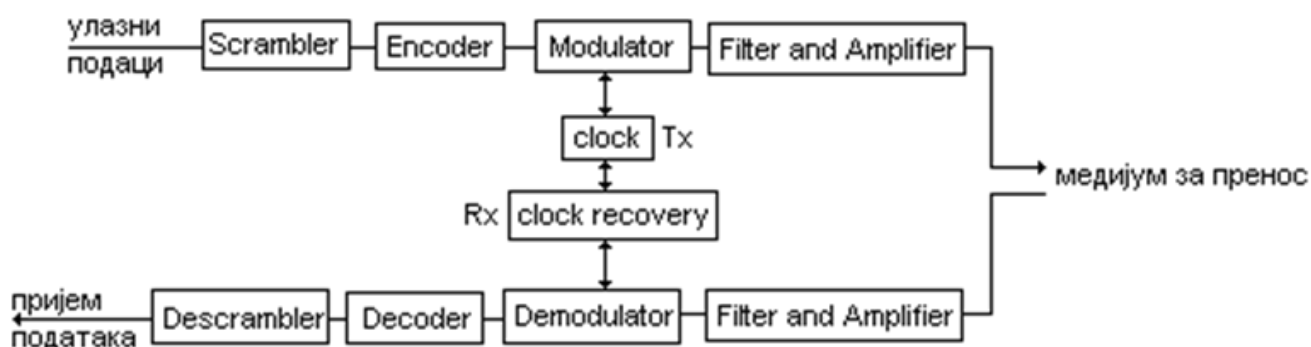
Koncentrator kao i multiplekser je uređaj koji omogućava povezivanje više ulaznih linija na jednu izlaznu liniju. Međutim za razliku od multipleksera koji vrši ravnomernu raspodelu vremenskih slotova svim korisnicima bez obzira da li imaju nešto za slanje ili ne koncentrator tu raspodelu vrši dinamički, odnosno u zavisnosti od potreba samih korisnika. Podatke koji dolaze na njegov ulaz koncentrator smešta u bafere pa na osnovu toga pravi raspodelu vremenskih slotova u zavisnosti od porekla podataka za prenos. Na taj način pokušava da realizuje maksimalnu iskorišćenost kapaciteta linije za prenos (linije veze).

Modem

Modem je uređaj koji služi za prilagođavanje signala medijumu za prenos. Digitalni signal, signal iz računara pretvara se u analogni koji se prenosi već postojećom infrastrukturom. Prenosne linije pate od tri glavne boljke: slabljenje, kašnjenje i šum. Uređaj koji prihvata niz bita kao ulazne podatke i generiše noseći talas modulisan pomoću neke od metoda, i modulisan talas pretvara u niz bita naziva se modem. Smešta se između računara (digitalni deo) i telefonske, kablovske infrastrukture (analogni deo).

Osnovni delovi modema su:

- Scrambler/descrambler
- Encoder/decoder
- Modulator/demodulator
- Filter and Amplifier
- Equalizer
- Clock/clock recovery



Na predajnoj strani:

Scrambler prekodira ulazni niz podataka sa ciljem da ne dozvoli pojavu dugog niza jedinica i nula.

Encoder kodira podatke sa ciljem da obezbedi zaštitu od greške.

Modulator vrši pretvaranje digitalnog u analogni signal.

Filter and Amplifier obezbeđuju da signal koji se prenosi telefonskom linijom (kablovskom) ima odgovarajući opseg i zadovoljavajuću amplitudu u zavisnosti od medijuma za prenos koji se koristi.

Clock i Clock Recovery obezbeđuju uspostavljanje i održavanje sinhronizacije.

Na prijemnoj strani:

Equalizer kompenzuje karakteristike vezane za telefonsku (kablovsku) liniju kao što su grupno kašnjenje i amplituda izobličenja.

Filter and Amplifier ograničavaju opseg da bi se smanjio uticaj šuma i pojačavaju ga do određenog nivoa.

Demodulator prevodi analogni u digitalni signal.

Decoder proverava da li je došlo do greške i izbacuje redundantne bite.

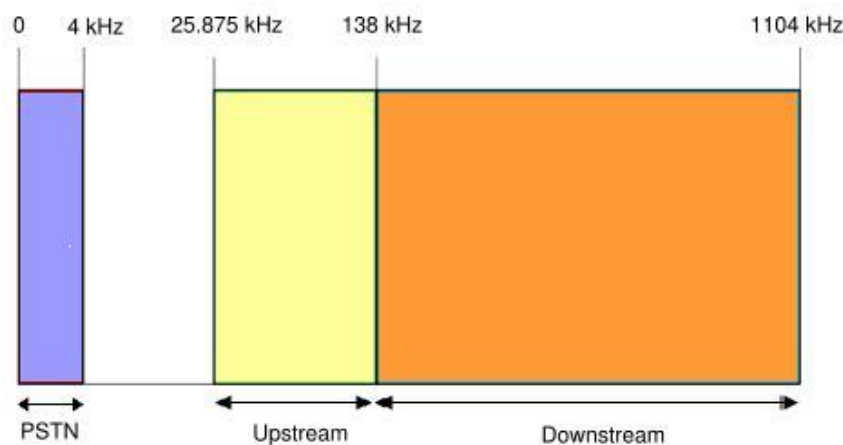
Descrambler vraća podatke u prvobitni položaj.

DSL – Digital Subscriber Line

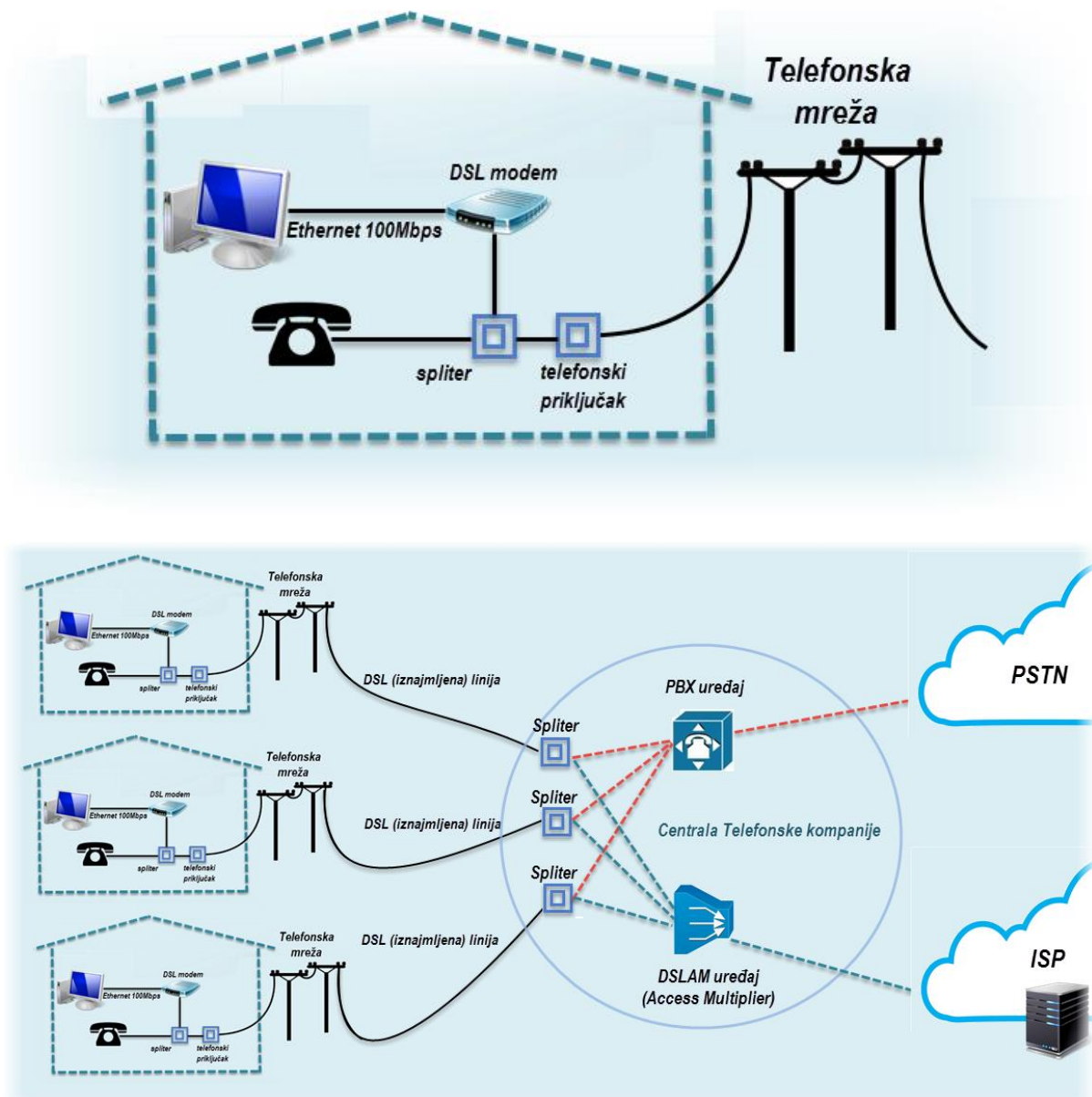
Predstavlja način prenosa digitalnih podataka po bakarnim paricama većim brzinama (144Kb/s – 50Mb/s). To je širokopolasna tehnologija gde se postupcima multipleksiranja i modulacijama omogućava digitalni prenos podataka visokim brzinama po već postojećim bakarnim paricama koje su namenjene klasičnoj fiksnoj telefoniji.

Govorni signal zauzima opseg od 0,3 - 3,4 KHz tako da veliki deo opsega kanala za prenos ostaje neiskorišćen, jer je širina kanala mnogo veća nego što se koristi za prenos govornog signala. Neiskorišćeni deo širine kanala možemo koristiti za prenos nekih drugih signala, u ovom slučaju digitalnih signala iz računara.

0 - 25 KHz koristi se za prenos analognog govornog signala ili prenos preko dial-up modema brzinom od 56Kb/s. Zapravo koristi se opseg do 4KHz za prenos a ostalih 21KHz kao zaštita od preslušavanja. 25 - 138 KHz koristi se u upstream-u, a od 138 - 1104 za downstream.



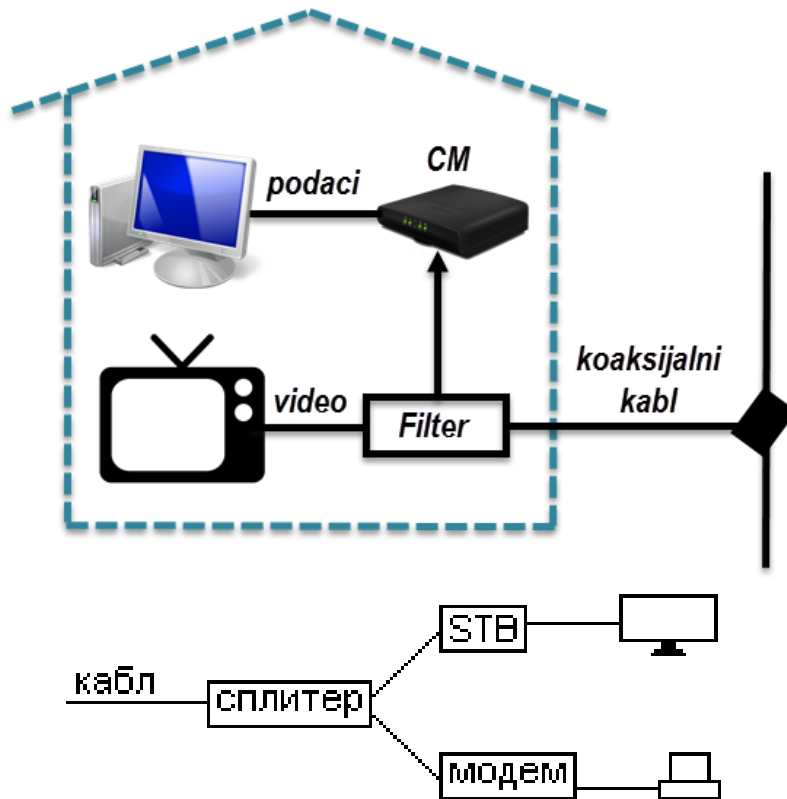
Spliter čine dva filtra koji frekvencijski razdvajaju govorni signal od modemskog signala. Na strani PSTN-a takođe se nalazi spliter da odvoji signale.



Kablovski modem

Kablovski modem je tip modema koji omogućava korišćenje već postojeće infrastrukture za distribuciju kablovske televizije u cilju prenosa digitalnih podataka računara. Primarna upotreba ovih uređaja je za uspostavljanje brze veze sa internet provajderom, koji je ujedno i provajder kablovske televizije.

Princip rada kablovske televizije je sličan principu rada DSL modema. Na postojećoj infrastrukturi, koja je u ovom slučaju kablovska televizija, moduliše se signal za prenos podataka na frekvenciji različitoj od frekvencije prenosa televizijskog kanala. Modem ima ulogu da podatke pristigle od računara moduliše na zadati opseg i obrnuto.



VHF TV 174-230 MHz (širina kanala 7MHz)

UHF TV 470-550 MHz (širina kanala 6 MHz), sve van ovih opsega može da se koristi za prenos podataka.

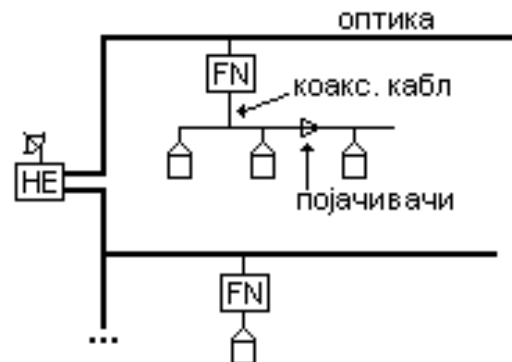
Uglavnom je zastupljen asimetrični prenos. U početku su KDS bili analognog tipa, ali usled mnogo analognih pojačivača i koaksijalnog kabla kao linije za prenos javila se slika slabijeg kvaliteta, polako se prešlo na optičke kablove i digitalizaciju celog sistema. Opseg koji se koristio tada za prenos bio je uslovljen i ograničen osobinama kabla i TV aparata, pa se prešlo na digitalizaciju cele slike i kompresiju. Trenutno se koristi MPEG-2 kompresija i omogućava prenos do 4 Mb/s.

Brzine prenosa su od par stotina Kb/s do par desetina Mb/s. Neki provajderi nude i brzine koje DSL ne može da podrži, simetrični ili asimetrični u zavisnosti od paketa.

Negativna strana je da se svi korisnici na jednoj geografskoj lokaciji (zgrada, ulica, deo grada) nalaze u okviru jednog kolizionog domena. Učestane kolizije u jednom kolizionom domenu mogu dovesti do toga da bez obzira što imamo uplaćen neki paket sa određenom brzinom ne možemo postići tu brzinu. Kupovinom paketa ustvari ne dobijamo zagarantovanu brzinu već

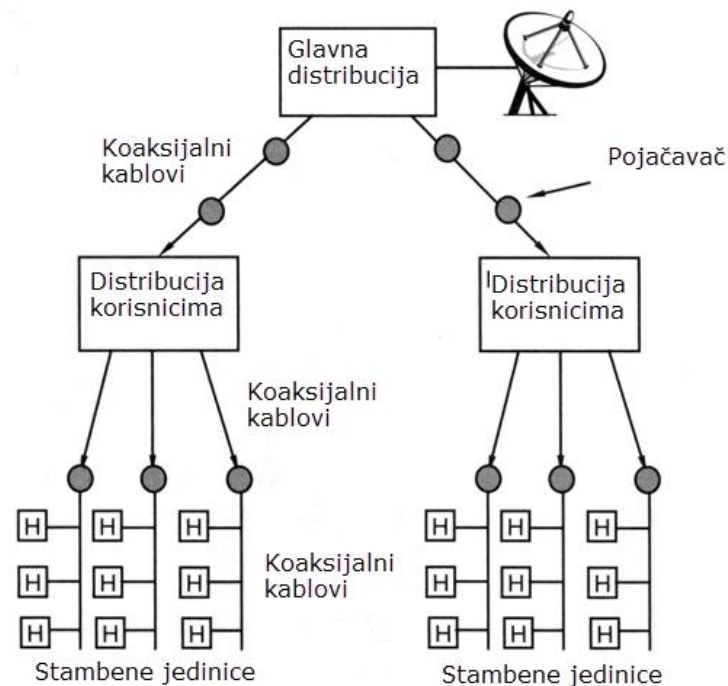
maksimalnu moguću. Kod DSL-a to nije problem jer je to veza point-to-point, kupljena brzina je garantovana.

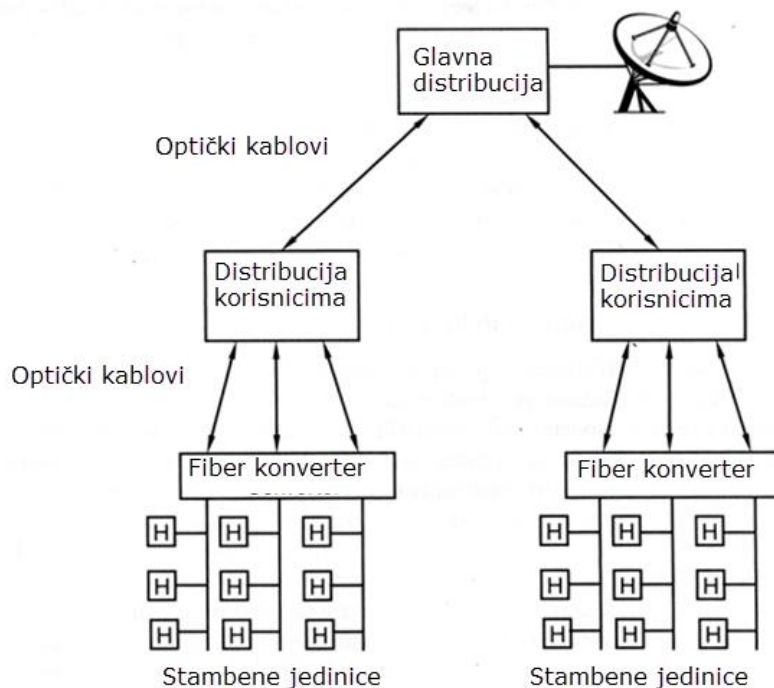
Drugi nedostatak kablovske veze opet je vezan za jedinstveni kolizijski domen, ogleda se u sigurnosti mreže. Kako su svi korisnici vezani za jedinstveni kolizijski domen (fizički sloj) a bilo kakav vid sigurnosti se implementira od drugog OSI sloja pa naviše, sigurnost je prepuštena samim korisnicima.



Da bi dobili dvosmernu mrežu operateri su morali da centralno čvorište (NE) modifikuju za dvosmerni prenos. FN (optičko čvorište) dobija modulator optičkog signala, a u koaksijalnom delu jednosmerne pojačivače menjaju dvosmernim.

Stari i novi sistem:





HUB

Hab je mrežni uređaj koji funkcioniše na prvom OSI sloju referentnog modela (fizičkom sloju). Sadrži više konektora (obično RJ-45) tako da se njime može povezati više segmenata mreže u jedan segment, povezuju se radne stanice, serveri i dr. uređaji. Funkcija haba je slična kao i ripitera, sve što primi na jednom svom portu hab emituje na svim ostalim portovima. Može se posmatrati kao višeportni ripiter.

U Ethernet mrežama sa UTP i optičkim kablovima hab je čvor koji povezuje stanice i servere. Svi uređaji povezani na hab dele isti kolizioni i brodcast domen, što povlači da samo jedan uređaj povezan na hab može u jednom trenutku vršiti transmisiju podataka. U suprotnom dolazi do kolizije. Često se koristi kao centralna tačka u topologiji zvezda.

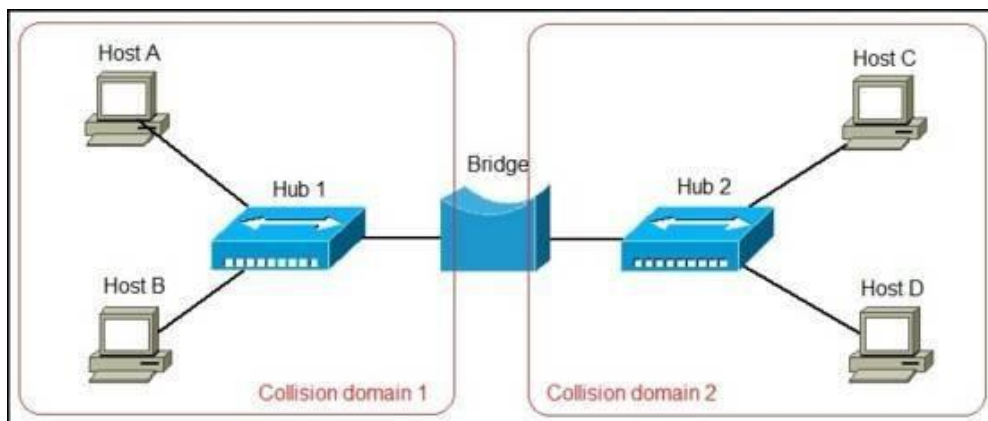


Uglavnom sadrži 6-24 porta i mogu se menjati po potrebi. Sadrži i još jedan uplink dodatni port za povezivanje dva haba, i to tako što se uplink jednog haba spaja sa običnim portom drugog haba.

Hab pojačava signal, vrši regeneraciju signala, čisti od šumova. Komunikacija je Half-Duplex. Topologija upotrebom haba dozvoljava razdaljine između pojedinih elementat mreže do 100 m, razdaljine između habova može se povećati upotrebom ripitera.

BRIDGE

Mrežni most radi na drugom sloju OSI modela, sloju veze podataka, i povezuje udaljene mrežne segmente. Segmentacija mreže vrši se mrežnim mostom u cilju istovremenog komuniciranja stanica u dva različita segmenta. U okviru segmenata samo jedna stanica može slati podatke, dok između segmenta podeljenih mostom dve različite stanice šalju istovremeno podatke.



Ima skoro sve karakteristike ripitera osim jedne dodatne koja ga izdvaja. Most proverava sadržaj zaglavlja primljenog okvira padataka da bi saznao MAC (fizičku) adresu izvora i odredišta. Na osnovu toga formira MAC tabelu adresa za svaki port. Kada dobije Broadcast adresu ne pamti MAC adresu već ga prosleđuje na sve portove. Deli celu mrežu na dva koliziona domena.



Mrežni most unosi malo kašnjenje jer proverava zaglavlje okvira pa nije pogodan za postavljanje između dve stanice koje često komuniciraju.

Ako treba da povezuje dve mreže različitih tehnologija Ethernet i Token-Ring, ili Ethernet i Wireless mora znati izvršiti konverziju protokola, pa mora raditi na višem sloju OSI modela i biće mnogo skuplji. U slučaju nestanka napajanja izgubiće sve podatke iz radne memorije.

SWITCH

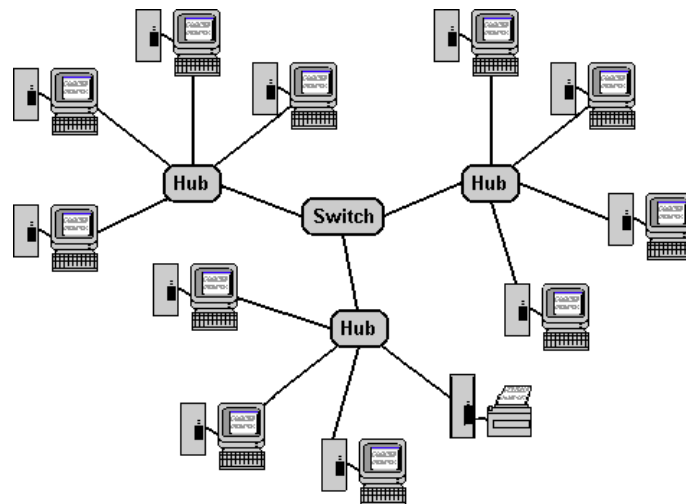
Svič radi na drugom sloju OSI referentnog modema. Uređaj koji prosleđuje podatke od jednog mrežnog segmenta do drugog na osnovu određene MAC adrese svakog rama (frejma). Pristigli podaci na portu se regenerišu i vrši se retransmisija frejmova, i odgovarajuća MAC adresa se upisuje u tabelu prosleđiva.

Za razliku od haba svič šalje pakete samo onim korisnicima kojima su namenjeni, upućeni prema određenoj MAC adresi, ne svima. Na svaki port sviča se priključuje stanica (krajnji korisnik, host), ne segment kako je to kod haba. Svaki port obrazuje jedan kolizioni domen, pa imamo razdvajanje kolizionih domena upotrebom sviča.

Svič sadrži više portova, koristi integrisana kola specifična za aplikaciju za pravljenje i održavanje MAC tabele prosleđivanja. Svičevi su brži od rutera zato što ne gledaju informaciju zaglavlja paketa, već samo hardversku (MAC) adresu pre nego što odluče da li će ram da prolsede ili odbace. Svaki port je nezavisan kolizioni domen i obezbeđuje nezavisan propusni opseg na svakom portu. Što znači da imamo full-duplex komunikaciju.



Najčešće se javljaju problemi preopterećenja. Brzina kojom okviru pristižu na svič regulisana je upotrebom neke od ARQ (Automatic Repeat Request) tehnika između dolaznog porta i uređaja koji na svič šalje te pakete. Ukoliko postoji mnogo podataka upućenih na neki od portova može doći do nedostatka kapaciteta bafera u kome se skladište podaci, pa dolazi do odbacivanja paketa. U zavisnosti od kvaliteta sviča i cene imaćemo odgovarajuću veličinu bafera.



Osnovne funkcije sviča su:

1. Učenje adresa: svič pamti izvorišnu MAC adresu i tu informaciju unosi u MAC tabelu prosleđivanja (sem ako već nije upisao tu adresu i vezao je za odgovarajući port). Ukoliko ne zna na koji port da prosledi paket na osnovu odredišne MAC adrese, odnosno ukoliko ta adresa nije upisana u tabelu svič šalje okvir na sve portove, osim na port sa koga je taj ram stigao.
2. Filtriranje: ako zna odredišnu adresu svič šalje ram samo na taj port, u suprotnom šalje na sve osim na onaj sa koga je stigao ram.
3. Izbegavanje petlje: redundantne veze između uređaja za komutiranje mogu sprečiti pad kompletne mreže ukoliko dođe do pucanja nekog linka, ali pored korisnosti mogu izazvati neželjene negativne posledice, odnosno pojavu beskonačne petlje, beskonačnog kruženja paketa. Svič ima sposobnost izbegavanja petlje.

RUTER

Ruter je mrežni uređaj koji radi na trećem sloju OSI referentnog modela. Osnovna uloga rutera je rutiranje (usmeravanje) paketa u mreži ka svom odredištu. Ova funkcija se obavlja korišćenjem IP adrese smeštene u zaglavlju paketa.

Od pristiglog paketa ruter dobija odredišnu IP adresu i na osnovu tabele rutiranja koju poseduje odlučuje na koji će port da prosledi paket. Ovaj proces pregledanja tabele rutiranja i odlučivanja na koji da se prosledi paket naziva se *lookup*. Po dobijanju ove informacije vrši se proces komutacije (switching) gde se paket komutira sa ulaznog porta na odgovarajući izlazni port.

Pored ovih funkcija ruter vrši i druge funkcije kao npr. provera ispravnosti paketa, obrada kontrolnih paketa. Ide se ka tome da ruter obavlja funkcije security protokola i kvaliteta servisa

(QoS). Pošto se dodavanjem novih računarskih korisnika i sve zahtevnijih aplikacija, potrebe za sve većim protokom povećavaju, potrebni su linkovi sve većeg kapaciteta, od nekoliko desetina Gb/s pa sa tendencijom do terabitnih brzina.

Ruteri se sastoje od četiri osnovne komponente:

1. Ulazni port
2. Komutatorska mreža
3. Izlazni port
4. Procesor rutiranja

1. Ulazni port izvršava nekoliko funkcija: funkcije fizičkog sloja, funkcije sloja veze podataka potrebne za saradnju sa funkcijama sloja veze podataka na drugoj strani ulaznog linka. Izvršava funkcije pretraživanja tabele i prosleđivanja paketa tako da paket prosleđen kroz komutatorsku mrežu rutera prosledi, izađe na tačno odgovarajući port.

2. Povezuje ulazne portove rutera sa njegovim izlaznim portovima. Cela komutatorska mreža se nalazi u ruteru.

3. Čuva pakete koji su mu prosleđeni kroz komutatorsku mrežu, zatim ih predaje na izlazni link. Izvršava inverzne funkcije prvog i drugog sloja u odnosu na ulazne portove. Ako je link dvosmeran izlazni port tog linka obično će se nalaziti na istoj linijskoj kartici na kojoj se nalazi i ulazni port za taj link.

4. Izvršava protokole rutiranja, održava informacije o rutiranju ažurira tabelu prosleđivanja, obavlja funkcije upravljanja mrežom u samom ruteru.

Ruter je takav uređaj da razdvaja kolizione i brodkast domen.



Konfigurisanje i održavanje tabele rutiranja

Po prijemu paketa prvo se proverava IP adresa odredišta i izvora da li se poklapaju, ukoliko dođe do poklapanja znači da je došlo do greške i paket se odbacuje. Ukoliko poklapanje ne postoji ruter na osnovu tabele rutiranja i adrese odredišta paketa, u zavisnosti gde se korisnik sa datom IP adresom nalazi u mreži, ili prosleđuje direktno odredištu ili do sledećeg rutera koji je na putu do krajnjeg odredišta.

Ruta se sastoji od tri elementa: odredišna destinacija, sledeći uređaj na putanji i rastojanje. Rastojanje predstavlja cenu ukupne rute do odredišta i naziva se još i metrika. U nekim protokolima cena (metrika) se računa pomoću broja linkova koje paket prolazi do krajnjeg odredišta, u nekim pomoću vremena u sekundama, a u nekim pomoću propusnog opsega linkova na toj putanji.

Prosleđivanje paketa do mreža sa kojima ruter nije u direktnoj vezi može se vršiti na dva načina:

1. Statičkim rutiranjem: administrator manuelno konfiguriše rute za svaku mrežu na svakom ruteru. Jednostavna je za realizaciju, konfiguraciju, pogodno za manje mreže, ne zahteva dodatne resurse, sigurnija je. Mana: nije skalabilna i neadaptivna je.
2. Dinamičkim rutiranjem: administrator konfiguriše protokole rutiranja, implementira (instalira) protokole rutiranja na svakom ruteru, rute se dobijaju razmenom informacija između rutera korišćenjem nekog protokola rutiranja. Skalabilno je, adaptivno, ali su potrebni dodatni resursi i zahteva pažljivo dizajniranje mreže.

Default ruta je podrazumevana ruta za određene udaljene mreže koje se nalaze u routing tabeli rutera. Ona predstavlja vezu sa korisnicima koji se nalaze u drugim mrežama, odnosno pokazuje IP adresu rutera preko koga moramo da pošaljemo saobraćaj kako bi uspostavili sesiju (komunikaciju) sa korisnicima u drugim mrežama.

ARP (Address Resolution Protocol) automatski određuje MAC adresu na osnovu IP adrese. Ruter radi na trećem nivou, ali IP paket koji se šalje do odredišta, korisnika koji je u istom LAN-u mora da se enkapsulira u ram. U ovom slučaju uređaj zna MAC adresu izvora, ali je nepoznata MAC adresa odredišta pa je potrebno na osnovu IP adrese odrediti i MAC adresu koja je uparena.

Paketi kroz mrežu putuju na osnovu IP adrese, odnosno odlučivanje na koji port treba paket da se pošalje kroz mrežu vrši se na osnovu IP adrese odredišta, tako da se u paketu odredišna i adresa izvora ne menjaju dok paket putuje kroz mrežu. Međutim na samo jednom linku ili vezi paket se svaki put enkapsulira u okvir sa odredišnom i izvorišnom MAC adresom samo za taj link. Pri svakom sledećem slanju opet IP adrese ostaju iste ali se MAC adrese promene u okviru za svaki link.

Protokoli rutiranja

Protokoli rutiranja ne služe za rutiranje poruka već da ruteri nauče kako da rutiraju poruke, odnosno služe za uspostavljenje ruting tabele i određivanje optimalne putanje do svakog dela mreže.

Osnovne funkcije protokola koje sprovode ruteri su:

1. Prikupljanje ruta (prikuplja informacije o drugim podmrežama od drugih rutera)
2. Oglašavanje ruta (obaveštavanje drugih rutera o podmrežama za koje oni imaju informacije)
3. Izbor najpovoljnije rute (ako postoji više ruta do odredišta bira se najpovoljnija, izbor i način određivanja najpovoljnije rute vrši se na osnovu datog implementiranog protokola, odnosno metrike i administrativne distance i one se upisuju u ruting tabelu)
4. Oglašavanje promene topologije (ako dođe do promene topologije drugim ruterima se oglašava novo stanje i ponovo se biraju najpovoljnije putanje)

Sve protokole možemo podeliti na:

- Interni protokoli su protokoli koji služe za rutiranje unutar autonomnih sistema, jedinstvenih administrativnih domena računarske mreže
- Eksterni protokoli za rutiranje su protokoli za rutiranje između administrativnih domena

Interne protokole možemo podeliti na:

1. Distance Vector Protocol (Vektor udaljenoisti) : susedni ruteri razmenjuju informacije o podmrežama na osnovu kojih saznaju metriku, odnosno distancu do određene podmreže i *next hop router*, sledeći ruter na putu do određene podmreže. Ruteri poznaju samo susedne rutere, a ne celu topologiju mreže. Rute se periodično razmenjuju.
2. Link-State Protocol (Stanje veze) : tokom razmene informacija ruter spoznaje celu topologiju. Informacije se ne razmenjuju periodično već samo prilikom promene topologije.

RIPv1 - Routing Information Protocol

Ovaj protokol spada u grupu Distance Vector algoritama, odnosno metrika se računa na osnovu udaljenosti od suseda.

Za beskonačnu vrednost metrike usvojena je vrednost 16 (smatra se da ovaj protokol nije dobar, efikasan za velike mreže). Cena svakog linka je 1, ukoliko administrator ne izvrši promenu.

Ovo je klasni protokol, što povlači sa sobom da se ne prenose informacije o subnet maski već samo mrežna adresa, odnosno podmrežavanje nije dozvoljeno.

U slučaju da postoji više ruta u isto vreme do nekog odredišta, neke podmreže, u rutinng tabeli čuva se ono sa najmanjom metrikom.

Tabela rutiranja se oglašava na svakih 30 sekundi. Svaki ruter sakuplja tabele rutiranja od drugih rutera i formira sopstvenu najoptimalniju tabelu i dužan je da je prosledi na svakih 30 sekundi. Ako se neki ruter ne oglasi 6 puta uzastopno, odnosno 180 sekundi, proglašava se nedostupnim i sve rute koje sadrže na svom putu i taj ruter se brišu. Oglašavanje se vrši IP Broadcast porukama. Da bi se promene u mreži što pre oglasile, svaki ruter mora da šalje Routing Update poruku čim dođe do promene u tabeli rutiranja.

Kao informacija u ruti se mogu pojaviti adrese hosta, mreže (u skladu sa klasnim adresiranjem), podmreže (subnet maska se uzima od prijemnog interfejsa), default ruta.

Ruta se briše iz tabele kada je isteklo 180 sekundi ili kad je oglašena ruta sa metrikom 16.

Prednosti:

- Jednostavna implementacija
- Neograničen broj rutera u mreži
- Ruteri mogu da osluškuju RIP oglašavanje bez potrebe da se sami oglase

Mane:

- Velika količina saobraćaja u mreži zbog broadcast poruka i RU
- Spora konvergencija
- Loša sigurnost
- Ograničena maksimalna veličina mreže
- Klasne adrese
- Ne podržava podelu saobraćaja

RIPv2

Spada u besklasne protokole, što podrazumeva da podržava promenljive dužine Subnet maske. Pri oglašavanju šalje se informacija o Subnet-u i Next hop-u. Zadržana je maksimalna moguća kompatibilnost sa RIPv1.

U verziji 2 uvedena je autentifikacija oglašavanja u cilju sprečavanja lažnih paketa, ali je ona relativno slaba.

Tabela rutiranja se šalje preko RU poruka na svakih 30 sekundi (kao i u RIPv1). U cilju smanjenja opterećenja u mreži (količine saobraćaja), umesto Broadcast poruka koriste se Multicast. Beskonačna metrika je 16.

Prednosti:

- Besklasno rutiranje
- Autentifikacija update paketa
- Korišćenje Multicast poruka

Mane:

- Ista metrika
- Relativno slab mehanizam autentifikacije

OSPF - Open Shortes Path First

OSPF spada u grupu Link State protokola. Podržava besklasno rutiranje, autentifikaciju korisnika, raspodelu saobraćaja (load balancing) i korišćenje neadresiranih interfejsa za serijske linkove. Zahteva male komunikacione resurse u stacionarnom stanju.

Za metriku koristi cenu linka (putanje). Najoptimalnija putanja je putanja sa najmanjom cenom. Kod OSPF cena se izračunava na sledeći način:

$$CENA = 1 * 10^8 / PROTOK$$

Za 100 Mb/s CENA=1 kao i za veće protoke

Npr. za 64Kb/s C=1562, za 256Kb/s C=390 i td.

Dozvoljena je promena konstante zbog prelaska na veće protoke.

Osnovni pojmovi OSPF protokola:

- Status linka – opis interfejsa koji se sastoji od IP adrese i Subnet maske, tipa mreže na koju je povezan (B-cast, PTP, M-cast), rutera koji su povezani na tu mrežu i metrike (baza podataka o linkovima)
- Router ID (32 bita) – identifikacija rutera u okviru OSPF oblasti. To je obično najveća IP adresa Loopback interfejsa ili najveća IP adresa ostalih interfejsa. U slučaju pada interfejsa menja se Router ID

Način rada

Ruteri šalju svima, svim ruterima u mreži kompletnu bazu podataka o linkovima pomoću LSA flooding-a (Link State Advertisement). Na osnovu ovih podataka ruteri računaju i generišu svoje tabele rutiranja korišćenje OSPF algoritma. Po formiranju tabele svaki ruter šalje kratki HELLO paket kojim signalizira da je još u funkciji, odnosno da je još aktivan u mreži.

LSA paket šalje se, generiše se na svakih 30 minuta. U slučaju promene topologije šalje se odmah. U slučaju velikih i kompleksnih mreža proračun tabele rutiranja zahteva značajne resurse. Zbog toga se velike mreže dele na oblasti. Ovim postizemo da se prilikom promene topologije proračun vrši samo unutar jedne oblasti.

Jedna oblast se proglašava za okosnicu (Backbone) i ona dobija identitet 0. Ostale oblasti dobijaju ID od 1 pa naviše. Sve oblasti moraju imati direktnu vezu sa okosnicom. Razmena informacija o dostupnosti pojedinih mreža se obavlja kroz oblast okosnice.

Štampač

Štampač je periferni uređaj čija je osnovna namena pravljenje trajne kopije teksta i/ili grafike, od dokumenata sačuvanih u elektronskoj formi. Koristi se uglavnom kao lokalna periferija, tj. kao izvor podataka koristi personalni računar, dok ga je moguće uključiti u LAN, kako bi u tom slučaju opsluživao više korisnika. Takođe, mnogi štampači mogu podatke čitati sa raznih vrsta prenosivih medija (Fleš memorije, memorijske kartice, digitalne kamere).

Moramo pomenuti da su takođe kućni štampači često MFP tj. Multi Function Printer uređaji, sa integrisanim mogućnostima za skeniranje tj. kopiranje dokumenata.

Moderna tehnologija štampe

Sledeće tehnologije se koriste u najvećem broju štampača:

- InkJet štampači sa tečnim mastilom

InkJet štampači rade po principu nanošenja mikroskopskih kapljica boje na stranicu bilo koje veličine. Trenutno predstavljaju najrasprostranjeniju tehnologiju u privatnoj primeni, zbog niske cene izrade i jednostavnosti korišćenja. Njihova popularnost opada zbog velikih troškova održavanja u odnosu na laserske štampače.

- Štampači sa čvrstim mastilom

Štampači sa čvrstim mastilom, takođe poznati kao štampači sa promenljivom fazom, su jedna od podvrsta termalno prenosivih štampača. Oni koriste čvrste štapiće CMYK mastila (po gustini sličnog vosku), koji se tope i putem glave štampača sa piezo elementima prenosi na nauljeni valjak koji prenosi boje na papir. Njihova najšira primena je u ulozi kolor kancelarijskih štampača, zbog izuzetne efikasnosti štampe na različitim medijima (folija i drugi neporozni materijali), kao i zbog cenovne efikasnosti, koja se može porediti sa onom kod laserskih štampača. Negativne strane ove tehnologije su velika potrošnja energije, kao i veliko vreme zagrevanja prilikom početka štampe.

- Štampači zasnovani na upotrebi tonera (laserski štampači)

U slučaju laserskih štampača, proces štampanja se znatno razlikuje od tradicionalnih InkJet/Hard ink štampača. Laserski znak se projektuje na valjak obložen selenijumom, koji zbog toga na usmerenim takčkama postaje naelektrisan. Čestice suvog mastila (tonera) se elektrostatički „lepe“ na naelektrisana područja valjka, i zatim se putem direktnog kontakta i toplote prenose na papir. Glavna prednost laserskih štampača jesu brzina, kao i niska cena održavanja, zbog čega je njihova popularnost sve veća.

- Matrični štampači

Matrični štampač funkcioniše uz pomoć glave štampača koja, krećući se po vertikali ili horizontali u zavisnosti od modela, štampa pomoću kontakta, tako što traku natopljenu mastilom pritiska uz papir na tačno određenim mestima, poput staromodne pisaće mašine. Međutim, za razliku od pisaće mašine, slova se formiraju od matrice tačaka, i shodno tome, omogućava štampu različitih fontova kao i grafičkih elemenata. Matrični štampači se uglavnom koriste za monohromatsku štampu, jer se implementacija traka sa više boja pokazala kao neefikasna metoda štampe, sa veoma niskim kvalitetom štampe i većim troškovima održavanja. Značajne prednosti matričnih štampača su izdržljivost i niska cena štampe, po kojima im nema konkurencije. Ukoliko dođe do kvara, to će najverovatnije biti usled čistog zamora materijala ili usled greške korisnika.

- Termalni štampači

Termalni, tj. toplotni štampači rade tako što zagrevaju određene regione posebnog papira osetljivog na toplotu. Monohromatski termalni štampači se koriste u fiskalnim kasama, bankomatima i nekim faks uređajima. Različite boje se dobijaju korišćenjem modernijeg papira uz različite nivoe zagrevanja.

- Ploter

Ploter za štampanje koristi uređaj najbliži olovci nalačenoj na glavu štampača, što ga ograničava na iscrtavanje samo linijskih vektora, dok štampanje samog teksta čini jako sporim procesom zbog komplikovanih pokreta glave koji su neophodni za različite fontove. Oni što je nama danas najpoznatije kao ploter jeste standardni InkJet štampač, predimenzionisan radi operacije sa većim formatima papira.

Istorija štampača

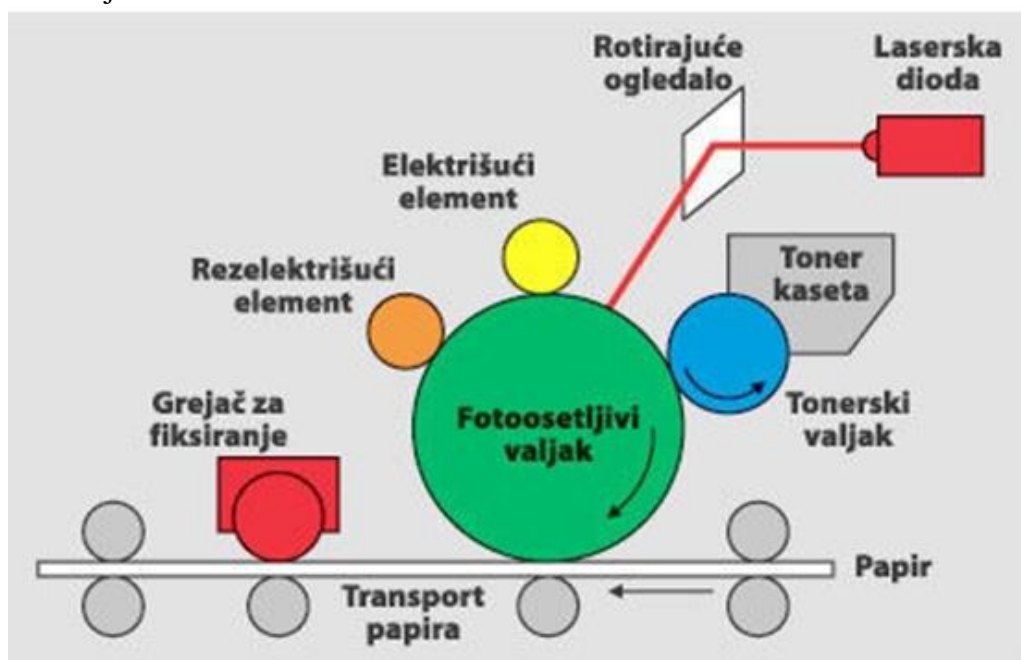
- 1867. Princip rada Ink-Jet štampača patentirao Lord Kelvin.

- 1951. Simens je napravio prvi komercijalni Continuous InkJet štampač za medicinske EKG uređaje.
- 1969. Xerox je, zaslugom svog inženjera Gerija Starkvedera, napravio prvi laserski štampač po ugledu na modificovane kserografske kopir mašine.
- 1970. Napravljen prvi matrični (Matrix Impact) štampač.
- 1971. Xerox je uspostavio prvu mrežu sa funkcionalnim štampačem koji su mogli da koriste svi računari u toj mreži.

Laserski štampač

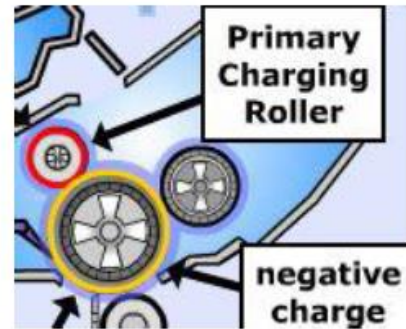
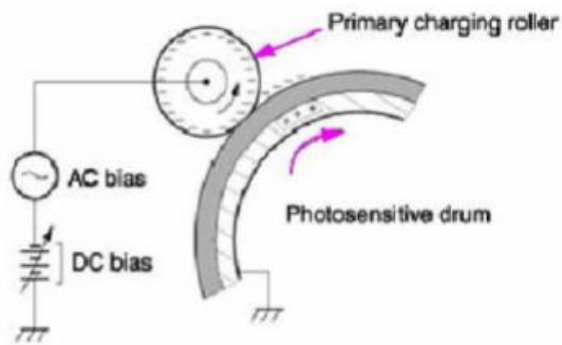
Laserski štampači se zapravo zasnivaju na staroj tehnologiji, budući da je ona izmišljena davne 1938. godine, a prvi put je implementirana 1971. godine. Međutim, oni su postali popularni tek odnedavno, zahvaljujući padom cena. Ovi štampači umesto trake (*ribbon-a*) ili kertridža sa mastilom koriste tonerski prah iz toner kasete. Ključni element na kome se zasnivaju laserski štampači uopšte nije laserski zrak, nego *statički elektricitet*.

Čitav mehanizam štampanja se sastoji iz valjaka između kojih prolazi papir: od ovih valjaka, najvažniji su štampajući (fotoosetljivi) valjak, elektrišući valjak, tonerski valjak i valjak za fiksiranje.

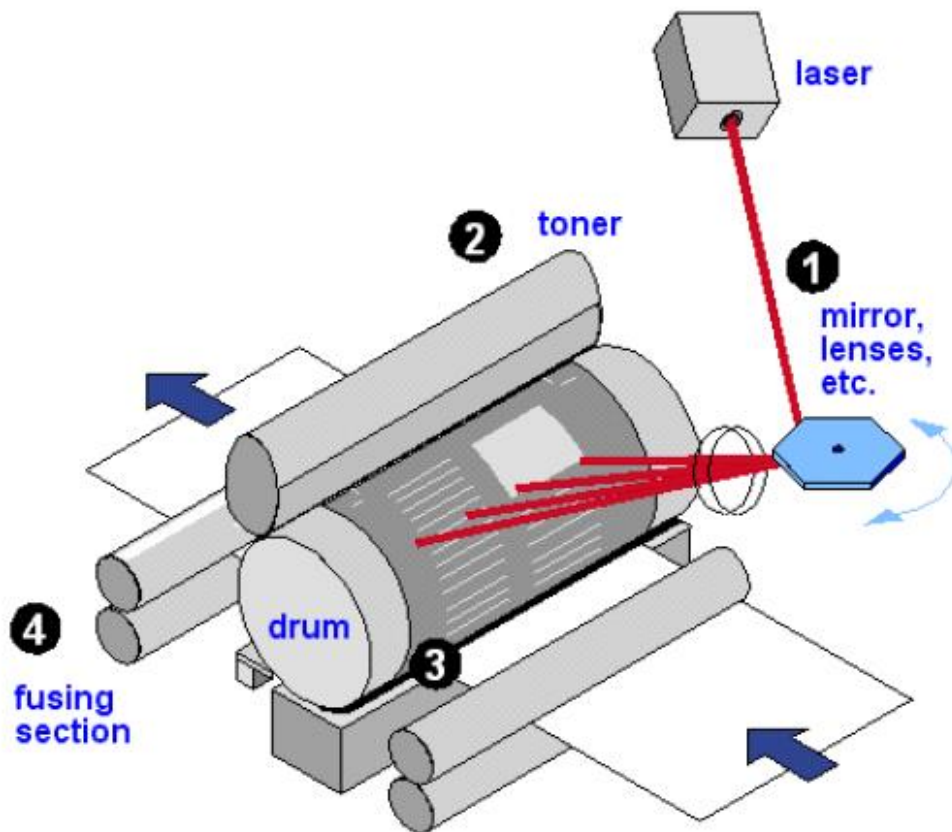


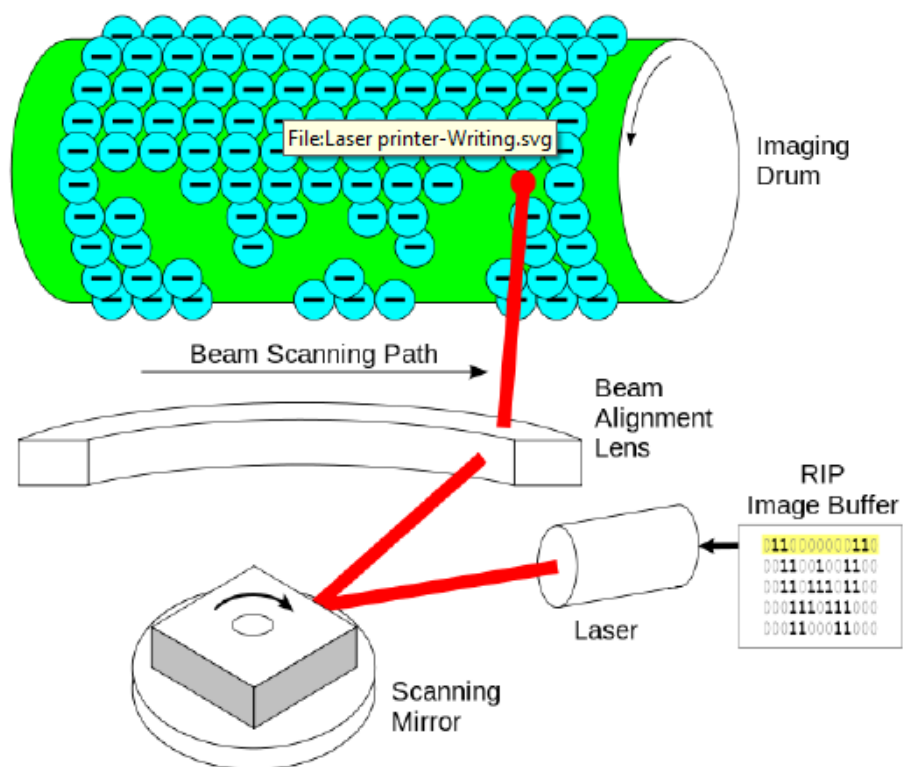
Celo štampanje se sastoji iz nekoliko koraka. Prvi korak je da se sadržaj dokumenta pošalje ka štampaču i smesti u *RAM* štampača. Važno je da cela stranica bude u ovom *RAM-u*, budući da je laserski štampač tzv. „stranični“ štampač, znači, papir kroz štampač prolazi konstantnom brzinom, bez zaustavljanja (matrični i mlazni štampači nisu „stranični“ štampači, jer kod ovih štampača papir prolazi kroz štampač postepeno – red po red).

Sledeći korak je naelektrisanje *valjka za štampanje (fotoosetljivog valjka)*. Ovaj valjak je izrađen od fotoosetljivog materijala koji je u stanju da zadrži naelektrisanje dok je u mraku. Ovo negativno naelektrisanje se vrši pomoću posebnog tzv. *elektrišućeg valjka*.

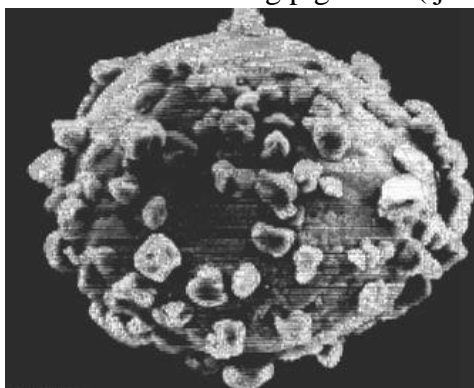


Zatim sledi ispisivanje: naelektrisani valjak se selektivno osvetljava *laserskim zrakom*, pri čemu se osvetljavaju samo oni delovi valjka koji pripadaju belinama na papiru koji se štampa. Na ovim delovima valjka će nestati negativno naelektrisanje. Laserski zrak se usmerava na odgovarajuća mesta na valjku pomoću rotirajućeg *ogledala* i sočiva, formirajući pojedinačne linije dokumenta. Ovako pripremljen valjak je spreman za razvijanje slike.

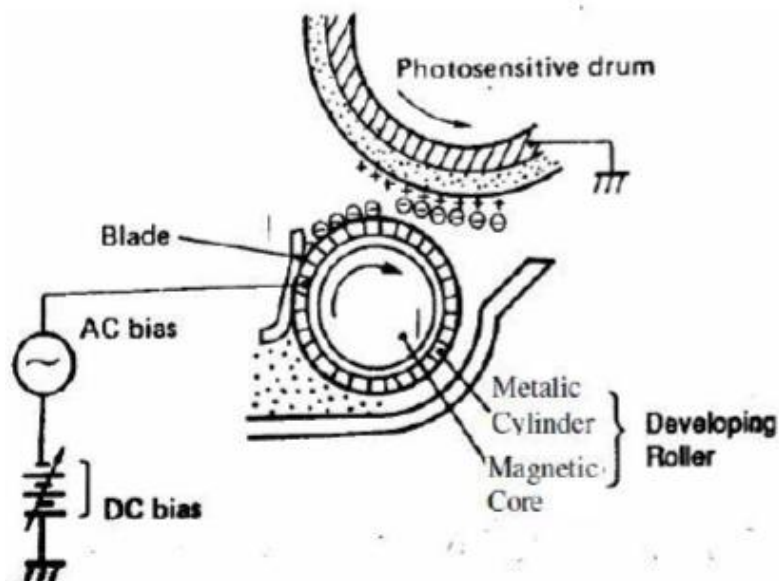




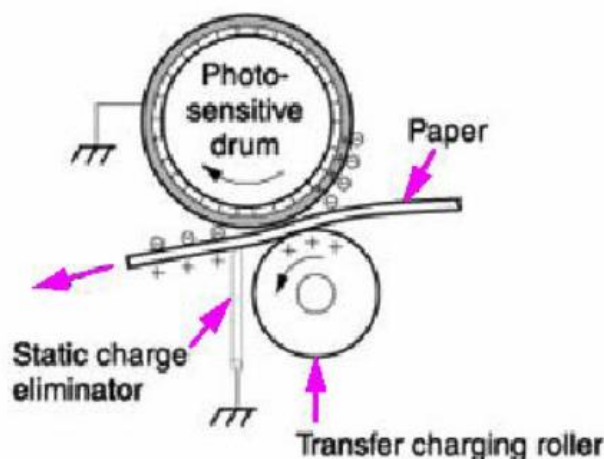
Razvijanje se sastoji u prenosu tonera iz *tonerske kasete* na štampajući valjak. Toner je zapravo prah, i svako zrno se sastoji iz dva dela: od tvrdog pigmenta (tj. boje) i od smole ili plastike.



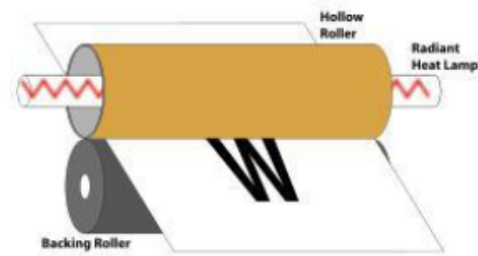
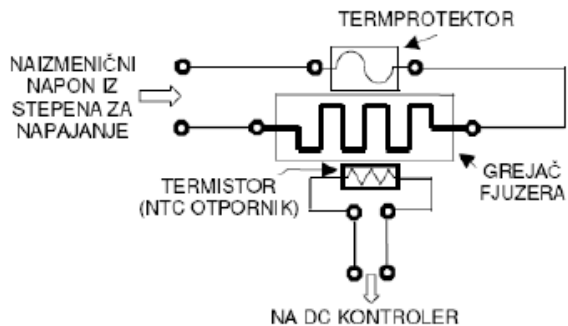
Koristi se poseban *tonerski valjak*, koji zahvata prah iz tonerske kasete i daje mu pozitivno naelektrisanje koje se zadržava zahvaljujući smoli ili plastici u prahu. Sa tonerskog valjka, usled različitog pola naelektrisanja, toner ravnomerno prelazi na štampajući valjak, ali samo kod onih delova, gde je ostalo negativno naelektrisanje.



U sledećem koraku, valjak sa zalepljenim tonerom prelazi preko papira koji je ranije takođe postao naelektrisan isto kao i štampajući valjak, ali većeg intenziteta. Budući da je papir intenzivnije naelektrisan u odnosu na štampajući valjak, papir zgrabi tj. krade tonerski prah od valjka. Štampajući valjak se zatim *razelektriše* posebnim valjkom, čime valjak postaje spreman za ponovno naelektrisanje.



Međutim, još uvek fali poslednji korak – *fiksiranje*. Naime, prah nanesen na papir u prethodnom koraku nije postojan (tj. stabilan), i može se otkloniti sa papira običnim duvanjem. Prema tome, papir prolazi kroz još jedan valjak koji se zove *valjak za fiksiranje*. Ovaj valjak u sebi ima grejač, a njegova površina je presvučena teflonom koji onemogućava zalepljivanje praha na površinu valjka. Grejač zatapa smolu ili plastiku zajedno sa pigmentom, i tako nastaje otisak na papiru.



Danas postoje i laserski štampači u boji koji zapravo imaju četiri toner kasete za svaku osnovnu boju posebno. Kod kolor modela, štampajući valjak se posebno naelektriše za svaku boju i fiksiranjem svih četiri sloja tonera na papir se dobija kolor slika.

Skener

Bilo zbog čiste zabave ili radi prepravki i dalje obrade, skoro svi smo u jednom trenutku imali potrebu da neku sliku ili tekst sa papira na neki način prebacimo u kompjuter. Kada je tekst u pitanju, postoji mogućnost prekucavanja, ali to je, kao što znamo, sporo i nepouzđano, a takođe je i u potpunoj suprotnosti sa razvojem trendova i načinom razmišljanja savremenog korisnika računara.

Za ovu vrstu poslova koristimo posebne uređaje koje nazivamo skenerima. Princip na kojem rade gotovo svi skeneri u suštini je krajnje jednostavan – svetlost koju emituje lampa odbija se od skeniranog uzorka i pada na poseban senzor koji je pretvara u električnu struju. U slučaju transparentnih originala (foto-negativi, slajdovi, filmske trake...) senzor prihvata svetlost koja prolazi kroz original. Osnovni delovi skenera su kontrolna kola, nosač uzorka, lampa, senzor i eventualno sistem ogledala koji reflektovanu svetlost projektuju na senzor. Prema konstrukciji, međutim, razlikuje se više tipova skenera.

Prva podela skenera tiče se načina na koji skener snima površinu uzorka. Kod skenera sa bubnjem (drum scanners) uzorak se postavlja na rotirajući bubanj, dok su senzor i lampa statični. Pored njih, razlikujemo i – najpopularnije – skenere sa pločom (flatbed scanners), kod kojih se uzorak postavlja na providnu ploču ispod koje se lampa i senzor sa pratećim sklopovima pomeraju po uzdužnoj osi. Ovakvi skeneri omogućavaju i skeniranje knjiga i predmeta, što ih je učinilo izuzetno popularnim kod širokih krugova korisnika. Kod treće vrste skenera (sheet fed scanners) lampa i senzor su statični, dok se skenirani uzorak provlači kroz skener jednostavnim sistemom valjaka. Poslednja vrsta skenera su tzv. ručni skeneri (handheld scanners), kod kojih su lampa i senzor spakovani u uređaj koji korisnik mora sam da prevlači preko uzorka. Zahtev za mirnom rukom pri upotrebi ovih skenera bio je izvor frustracija mnogih korisnika pa se oni zato generalno smatraju lošom idejom.

Senzori i lampe

Druga podela skenera vrši se po izvedbi lampe i senzora. Kada su lampe u pitanju, razlikujemo skenere koji koriste ksenonske lampe, fluorescentne cevi, cevi sa hladnom katodom (koje se takođe koriste i kao pozadinsko svetlo za LCD ekrane), kao i svetleće diode. Najkvalitetniji izvor svetlosti je, naravno, ksenonska lampa, dok su svetleće diode najkompaktnije. Većina

komercijalnih skenera, međutim, koristi fluorescentne cevi ili cevi sa hladnom katodom kao kompromis između dimenzija, potrošnje struje i kvaliteta reprodukcije.

Kada su senzori u pitanju, najstariji senzor je posebna elektronska cev koja se zove fotomultiplikator (photomultiplier tube, PMT). Ova vrsta senzora se odlikuje visokim kvalitetom reprodukcije kao i mogućnošću postizanja izuzetno visokih rezolucija. Posebna pogodnost PMT senzora je mogućnost nezavisne promene veličine skeniranog elementa i blende samog senzora, što omogućava postizanje izuzetno visoke rezolucije skenirane slike. PMT senzori se koriste kod skenera sa bubnjem i njihova osnovna primena je reprodukcija visoke vernosti, na primer za potrebe muzejskog arhiviranja fotografija ili skeniranje filmskih traka pri telekino obradi.

Međutim, PMT senzori su skupi, pa je u komercijalnim skenerima najzastupljeniji CCD senzor. CCD (Charged Coupled Device) je poluprovodnički element koji pri pobudi svetlošću (fotonima) na svom izlazu daje struju (elektrone). Ovi senzori se koriste u fotoaparatom i TV kamerama, kao i u astronomskim teleskopima i većini fotometrijskih uređaja. Prednost CCD senzora je zadovoljavajući kvalitet uz znatno nižu cenu, a osnovna mana je to što zahtevaju sistem ogledala za fokusiranje svetlosti, jer je sam senzor mnogo manji od dimenzija skeniranog uzorka, što otežava dalje smanjivanje dimenzija skenera. CCD senzori se koriste u *flatbed* i *sheet fed* skenerima, kao i u skenerima sa bubnjem koji se koriste za brže arhiviranje dokumenata.

Najnoviji, najjeftiniji i najkompaktniji senzori su kontaktni senzori (Contact Image Sensor, CIS). Ovi senzori koriste jednostavan sistem sočiva za fokusiranje svetlosti i mogu da budu u kontaktu sa uzorkom. Kontaktne senzore se sastoji iz niza detektora koji određuju rezoluciju skenera. Kao izvor svetlosti, CIS koristi crvene, zelene i plave svetleće diode. Osnovna odlika skenera sa kontaktnim senzorom je izuzetno mala potrošnja električne energije, kao i mogućnost konstrukcije veoma malih komponenata, što ih čini pogodnim za primenu u prenosnim uređajima. Osnovna mana im je znatno niži kvalitet reprodukcije u odnosu na CCD skenere.

Princip rada skenera

Bez obzira na vrstu, najvažniji deo svakog skenera je glava skenera koja se sastoji od nekoliko delova: od ogledala, sočiva i senzora. Skeniranje se vrši na sledeći način: izvor svetlosti (najčešće fluorescentna lampa) osvetljava dokument, i svetlost se odbija od površine dokumenta, a zatim i od ogledala koje usmerava svetlost u sočivo. Sočivo zatim fokusira svetlost ka senzoru. Senzor u skenerima je zapravo kolekcija jako malih elektroda (tj. dioda osetljivih na svetlost) koji konvertuju fotone (tj. svetlosne zrake) u elektrone. Sve je svetlosni zrak svetliji, elektrode će se više naelektrisati. Na osnovu intenziteta naelektrisanja kod svake elektrode, može se dobiti digitalna reprezentacija tačke skeniranja. Međutim, još ostaje da se vidi kako se mogu reprodukovati boje. Koriste se kolorni filteri. Budući da imamo tri osnovne boje (crvenu, zelenu i plavu), koriste se tri filtera. U ovom slučaju, sočiva glave razdele svetlosne zrake na tri dela tj. tri zraka. Svaki razdvojen zrak tada prolazi kroz odgovarajući kolorni filter, nakon čega stiže u senzor.

Rezolucija, interpolacija i boje

Osnovna vrednost koja definiše kvalitet skenera je njegova rezolucija. Prosto rečeno, skener sa većom rezolucijom biće u stanju da reprodukuje sitnije detalje uzorka. Rezoluciju skenera izražavamo, kao i kod štampača, u broju tačaka po dužinskom inču – dpi (engl. dots per inch,

dpi). Kod skenera se može razlikovati horizontalna i vertikalna rezolucija. Horizontalna rezolucija zavisi od izvedbe senzora. PMT senzori mogu da postignu rezoluciju od 12.000 dpi, CCD senzori mogu da ostvare rezoluciju od 1200 do 5400 tpi, dok je CIS obično ograničen na 600 dpi. Vertikalna rezolucija određena je preciznošću koračnog motora koji pokreće glavu ili uzorak i obično se ne navodi kao podatak, jer ne predstavlja problem.

Da bi povećali rezoluciju, proizvođači skenera su izmislili zanimljivu stvar po imenu interpolacija. Naime, kako bi se povećala rezolucija dobijene slike, skener između postojećih piksela umeće one čije su boje proračunate na osnovu boja susednih piksela. Ova metoda se obično koristi kod skenera sa CCD senzorom da bi se njihova rezolucija povećala do 19.200 dpi. Međutim, upotreba interpolacije nailazi na negodovanje profesionalnih korisnika, jer su rezultati obično suviše loši i dobijena slika ima previše šuma.

Druga, ali ništa manje važna osobina skenera jeste njegova paleta, odnosno dubina boja (color depth). Paleta, jednostavno rečeno, predstavlja broj boja koje skener može da reprodukuje, i izražava se u bitima potrebnim za predstavljanje jednog piksela. Standardna *true color* paleta koristi 24 bita za predstavljanje jednog piksela, odnosno po 8 bita za svaku od osnovnih boja. Kvalitetni skeneri, međutim, često imaju veću dubinu boja i koriste do 48 bita za predstavljanje piksela. Pošto se tolika dubina boja ne koristi često u obradi fotografija, osnovni razlog za njihovu upotrebu jeste mogućnost skenera da samostalno izabere najpogodniju boju iz 24-bitne palete. Još jedan važan parametar skenera koji određuje njegov kvalitet je i gustina (density), to jest sposobnost skenera da reprodukuje tamne i svetle detalje uzorka.

Broj bita koje skener koristi i broj boja povezani su na sedeći način gde je: n broj bita, a c broj boja.

Broj bita (n)	Broj nijansi
1	2
2	4
4	16
8	256
16	65536
24	16777216

Odabir skenera i način skeniranja

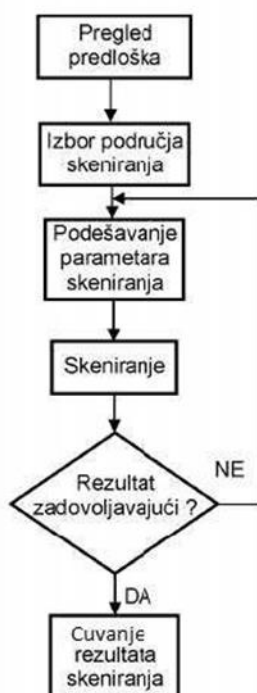
Najvažnije komponente skeniranja i najbitnije stavke su brzina, rezolucija, volumen skeniranja, uvlačenje dokumenata, poboljšanje kvaliteta slike, automatska obrada skenova i odabir digitalnog formata. Jedna od osnovnih karakteristika skenera je njegova brzina odnosno broj listova koje može obraditi u jednoj minuti. Brzine skeniranja se kreću se od nekoliko desetaka dokumenata u minuti pa do nekoliko stotina u minuti. Brzina skeniranja u karakteristikama skeniranja navodi se kao pages per minute – ppm (broj listova u minuti) ili images per minute – ipm (broj slika u minuti). Na brzinu skeniranja utiču i mnogi drugi faktori: priprema dokumenata, učestalost zaglavljivanja papira ili dvostrukog uvlačenja, orijentacija i rezolucija pri skeniranju, korisničko iskustvo itd.. Rezolucija – odabir skeniranja u boji ili crno3belo zavisi o daljem toku rada. Skenovi u boji daju kvalitetniju sliku pri maloj rezoluciji i ugodniji su za vizuelnu proveru, ali zauzimaju više prostora te nisu pogodne za automatsko izvlačenje informacija.

Odabir rezolucije zavisi o potrebi za kvalitetom slike, veća rezolucija daje sporiji rad skenera.. Osim brzine i rezolucije, podjednako je bitan predviđen dnevni volumen dokumenata za skeniranje, koji se u karakteristikama skenera navodi u broju stranica koje skener može

skenirati na dan. Ovaj podatak zavisi o kvaliteti delova ugrađenih u skener te o njemu zavise i troškovi održavanja skenera. Savremeni skeneri s ADF-om imaju mogućnost detekcije uvlačenja više dokumenata odjednom, što dovodi do zastoja u skeniranju. Takođe su opremljeni delovima za detekciju spajalica koje nisu bile uklonjene pre samog ubacivanja u skener. Komponente za uvlačenje dokumenata podložne su trošenju te ih je potrebno s vremenom čistiti ili menjati. Učestalost održavanja tih komponenti, osim o količini skenova, zavisi i o kvalitetu papira koji se skenira. Softver za poboljšanje kvaliteta slike trebao bi biti obaveznim delom za skeniranje. On može biti ugrađen u sam skener ili može biti deo obrade slike na računaru. Uobičajeno, takav softver ima mogućnost automatske detekcije boje, uklanjanja boje pozadine, "izgladivanja" pozadine, uklanjanja mrlja, automatske orijentacije dokumenata, uklanjanja praznih stranica, ispravljanja ugla pod kojim je dokument skeniran itd..

Osim skenera i softvera za poboljšanje kvaliteta slike, bitan faktor u procesu digitalizacije papirnatih dokumenata jeste i softver za automatsko očitavanje podataka (OCR). Savremeni softverski paketi za OCR odlikuju se velikom tačnošću očitavanja kako sa strukturnih, tako i s nestrukturnih dokumenata te velikom tačnošću automatske klasifikacije dokumenata. Trenutačno najčešće korišćeni formati za spremanje digitalnih dokumenata su TIFF i PDF, iako je primetan trend sve većeg korištenja PDF formata.

Proces skeniranja



Kao što se može videti, sa mehaničke strane skeneri predstavljaju jednostavne uređaje. Imaju mali broj pokretnih delova i uglavnom jednostavnu optiku. Međutim, njihova cena odražava kompleksnost tehnologije korišćene za što verodostojniju reprodukciju, u digitalnom obliku, boja i detalja originala. Širok spektar tehnologija i njihove implementacije znači da se na tržištu mogu naći skeneri za svaku namenu, počev od najjednostavnijeg optičkog prepoznavanja teksta, do skeniranja slika radi njihove obrade i štampanja u velikim formatima.

UPS - Uninterruptable Power Supply

Prvenstvena namena UPS-a je da u trenucima nestanka električna energije obezbedi računaru napajanje za još neki kratki period kako bi se neki projekat koji se u tom trenutku radi mogao sačuvati i kako bi se sistem mogao isključiti bez posledica. Njegova sekundarna primena je radi stabilizacije napona i sprečavanja dovođenja višeg napona od dozvoljenog na vaše elemente u kucistu.

Standardni home/office UPS-evi se koriste (kako im ime kaze) u kućnim ili kancelarijskim varijantam gde postoji samo jedan računar i jedan monitor koje dotični napaja. Tu se koriste UPS-evi kapaciteta do 1000VA. Baterija se preko ispravljača puni jednosmernom strujom, da bi se u trenutku nestanka el.energije preko invertora taj jednosmern napon(DC) pretvorio u naizmenični (AC) kojim mi u stvari napajamo računar. Period za koji se ta promena tj kašnjenje desi moze da bude nekoliko ms, te se može desiti da neka komponenta u racunaru zakaže, mada je to redak slučaj iz razloga sto se u računarima nalazi veliki broj kondenzatora koji će uspeti da napajaju računar tih 4-5 ms kolko treba vremena UPS prebaci napajanje sa mreže, na svoje sopstveno napajanje.

Kod velikih servera koriste se UPS-evi kapaciteta od 5000VA pa navise. Kod njih je karakteristično to sto se napajanje vrši direktno iz UPS-a tj baterija se napuni i iz nje se šalje dalje električna energija, tako da se u toku nestanka el.energije spoljašnji dovod samo prekida a nastavlja se napajanje iz UPS-a, tako da tu nema nikakvog kašnjenja po pitanju napajanja servera.

Prilikom korišćenja i primene UPS-eva se koristi jedinica VA (Volt Amper) koji u stvari pretstavlja proizvod struje i napona napajanja, npr $220V * 8A = 960 VA$

Prilikom kupovine ovog uređaja vodite računa o vremenu trajanja rada, tj dužini koliko će doticni moći da napaja vas racunar. To zavisi od svega što imate u istom, npr. UPS od 500VA neki standardni desktop računar koji "troši" 300W moze da napaja 6-7 minuta, a UPS-evi "kapaciteta" 1kVA(1000VA) mogu isti napajati 15-20 min iz razloga velikog "povlačenja" struje prilikom uključenja UPS-a u rad.

Podela

Uređaj za neprekidno napajanje je sistem čiji je osnovni zadatak da obezbedi nesmetano električno napajanje potrošača, najčešće personalnih računara sa opremom. Obezbeđuje zaštitu od prenapona, podnapona, naponskog udara. Deli se prema načinu rada u tri kategorije: Off-line, Line Interactive i On-line.

- Off-line: najjeftiniji i najviše se koristi. Direktno napajanje potrošača kroz UPS uređaj, a istovremeno se preko ispravljača pune baterije unutar UPS-a. U slučaju varijacije napona korisnik se automatski napaja ispravljenim naponom (strujom iz baterije).
- Line Interaktive: napajanje nije direktno, beć se struja filtrira i ispravlja, i predaje kvalitetnija struja potrošaču, a deo ide na punjenje baterije preko ispravljača.
- On-line: najskuplji i najkvalitetniji. Uređaj sa dvostrukom konverzijom. Uvek se prvo vrši AC-DC konverzija iz naizmeničnog u jednosmerni napon, odakle se koristi za punjenje baterije, a deo ponovo preko invertora konvertuje. DC-AC konvertor pretvara u naizmenični napon ali idealnih karakteristika. U

slučaju kvara invertora ili baterije automatski preusmerava napajanje sa mreže na potrošača.

Faktor snage kreće im se od 0,5 do 0,9 u zavisnosti od cene i kvaliteta.

Npr. ako je faktor snage 0,8, uređaj snage 1000 W može da napaja uređaje do 800 W.

Vrste smetnji

Imamo nekoliko vrsta "*uljeza*" iz električne mreže:

- Podnapon (Brownout, Sag). Spada u najčešće probleme na električnoj mreži. Za podnapon se uzima bilo koji napon 20% niži od nominalnog (u našem slučaju 220V). Prouzrokuje "zamrzavanje" tastature, čudno "pucktanje" diska ili "zaglavljivanje" sistema.

- Prenapon (Surge). Obično traje 1/120 sekunde (1,2ms) i prouzrokovao je uključivanjem/isključivanjem velikih potrošača/elektromotora koji rade u okruženju kompjutera (veš mašina, zamrzivac, lift, rashladni uređaji, kompresori...).

- Udar (Spike). Važi za daleko najopasniji vid problema sa električnom energijom. Prouzrokovao je trenutnim skokom napona i do 100% (pa i više) iznad nominalnog. Javlja se kada grom udari u blizini trafo-stanice.

- Šum (Noise/Interference). Nastaje od blagih poremećaja frekvencije. Postoje dve vrste šumova (interferencija): RF (Radio-frekventna) i EM (Elektro-magnetna).

- Isključenje (Blackout). Deluje dosta pogubno po opremu. Prouzrokuju ga kvarovi, preveliki zahtevi za električnom energijom (preopterećenje), prirodne nepogode (udar groma, oluja...)

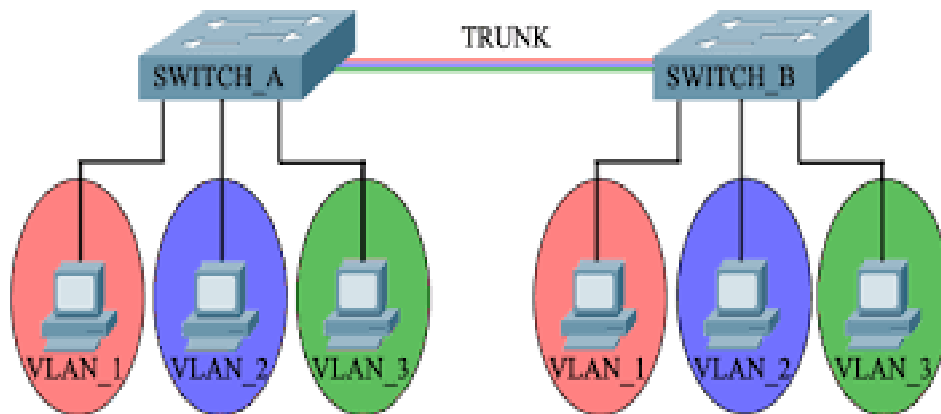
Na kraju bilo bi poželjno navesti najbolje, ili bar najčešće, proizvođače. U najpominjanije svakako spada APC, koji kod nas važi za skupljeg, iako gledajući globalno to zapravo nije. Poznati su još i Best Power, Longtime, Belkin, Emerson, Leadman, IntelliPower, Liebert (posebno poznat po "super-teškoj" kategoriji), kao i svima poznati Mustek. Naravno, proizvođača ima još dosta, jedan od njih je i naš Enel, koji se možda ne odlikuje dizajnom (pošto je UPS spakovan u mini tower kućište), ali zato važi za najizdržljivije (jači modeli bez problema izdržavaju i po nekoliko sati - duplo više od pandana stranih proizvođača; verovatno je to posledica bivše države, koja je gajila ljubav prema industrijskoj elektronici).

VLAN – Virtual Local Area Network

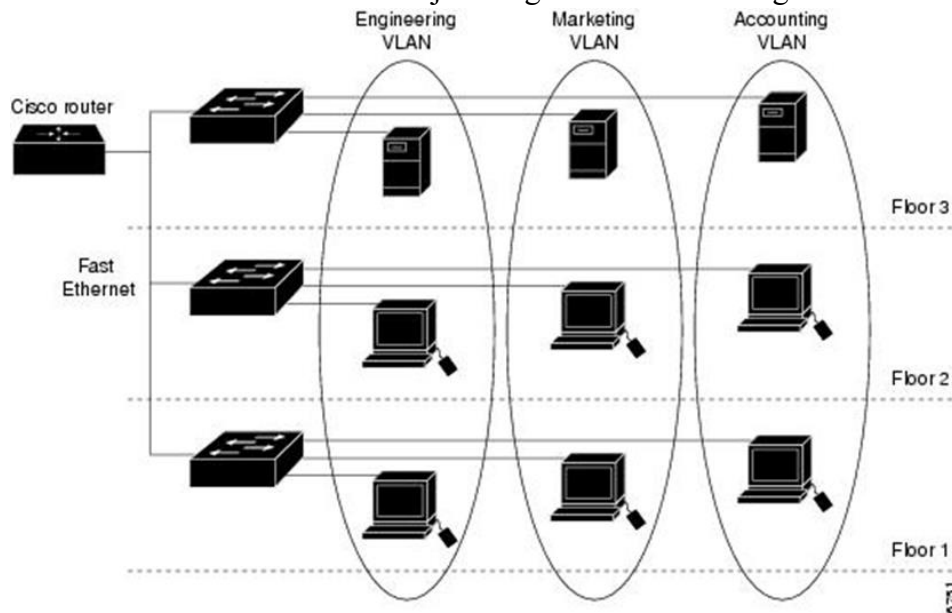
Vlan čini grupu krajnjih uređaja, sa zajedničkim osobinama, nezavisno od toga gde se oni nalaze u mreži. VLAN ima iste osobine kao stvarni fizički LAN, ali dozvoljava da se uređaji grupišu u jedan

VLAN čak i ako oni ne pripadaju istom segmentu.

Vlan dozvoljava da se portovi sviča pregrupišu kako bi se ograničio broadcast i multicast saobraćaj. Prolseđivanje ovog saobraćaja vrši se samo unutar VLAN-a, gde je generisan.



Vlan je logički broadcast domen koji se može prostirati kroz nekoliko LAN segmenata. Svaki port sviča može se pridružiti samo jednom VLAN-u. Portovi unutar jednog VLAN-a pripadaju jednom broadcast domenu. Portovi unutar različitih VLAN-ova su u različitim broadcast domenima. VLAN može da se prostire unutar jednog sviča ili da obuhvata nekoliko svičeva, može da obuhvata hostove unutar jedne zgrade ili nekoliko zgrada.

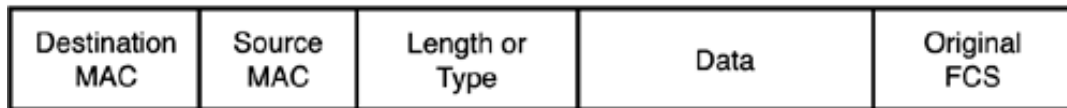


Portovi sviča mogu da rade u access modu ako su za njih vezani krajnji uređaji i ako prosleđuju saobraćaj unutar samo jednog VLAN-a, ili u trunk modu ako predstavljaju vezu između dva sviča (ili sviča i rutera) i prenose saobraćaj više VLAN-ova. Ako administrator ne promeni drugačije po default-u svi portovi se nalaze u native VLAN-u broj 1. Pripadnost korisnika određenom VLAN-u definiše se pripadnošću odgovarajućeg porta za koga je vezan.

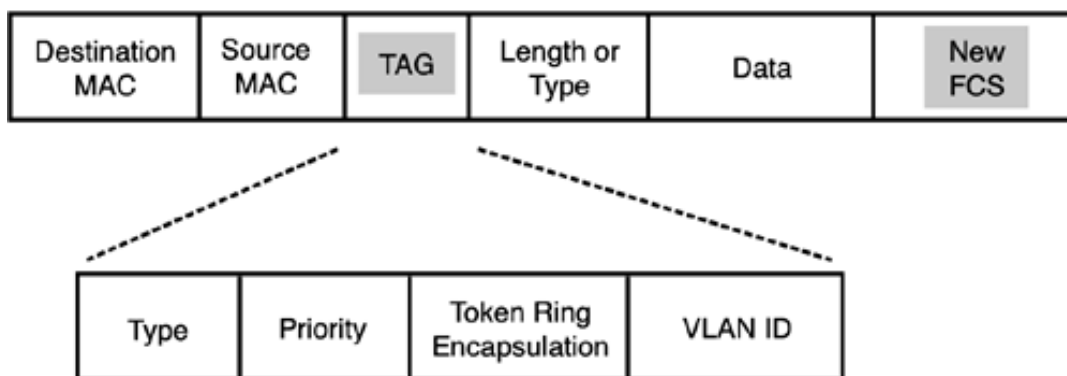
IEEE 802.1Q standard

Komunikaciju između hostova koji pripadaju različitim VLAN-ovima možemo omogućiti dodavanjem rutera i implementacijom 802.1Q standarda, odnosno enkapsulacijom.

Original Ethernet Frame



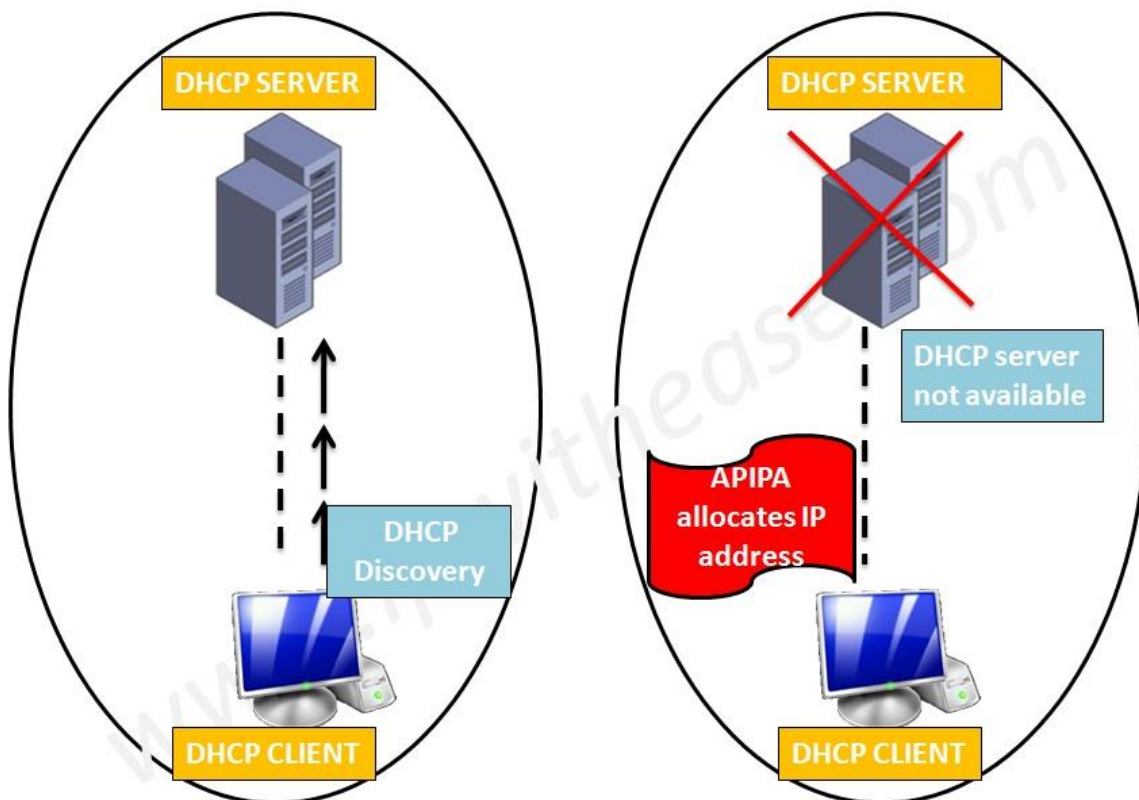
802.1Q Tagged Frame



Tagovanjem Ethernet frejma generišemo 802.1Q frejm. 802.1Q enkapsulacija ne taguje frejmove koji pripadaju native VLAN-u (VLAN 1), a svi ostali frejmovi se taguju. 802.1Q definiše standardni način ubacivanja VLAN pripadnosti u Ethernet pakete. Uređaji u dva različita VLAN-a ne mogu da vide jedan drugoga bez pomoći mrežnog uređaja (rutera).

APIPA – Automatic Private IP Address

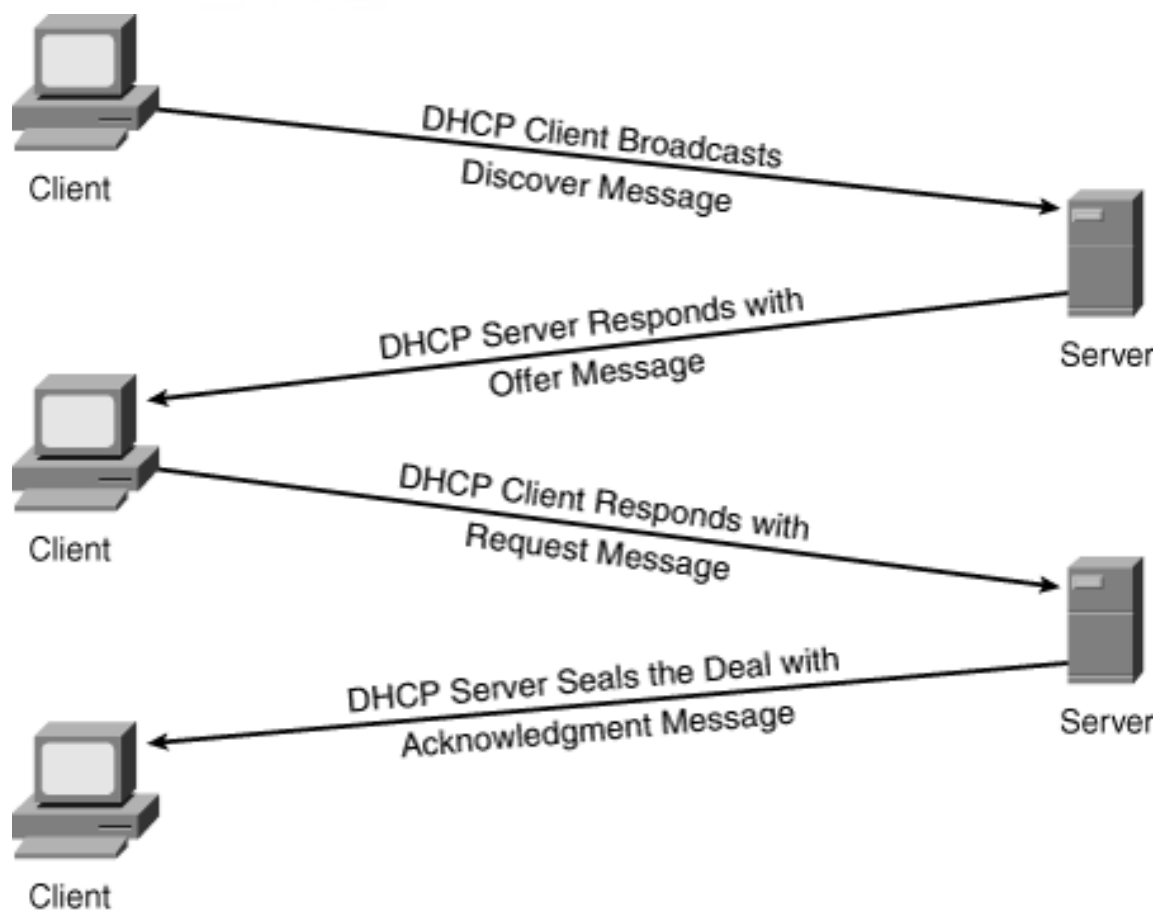
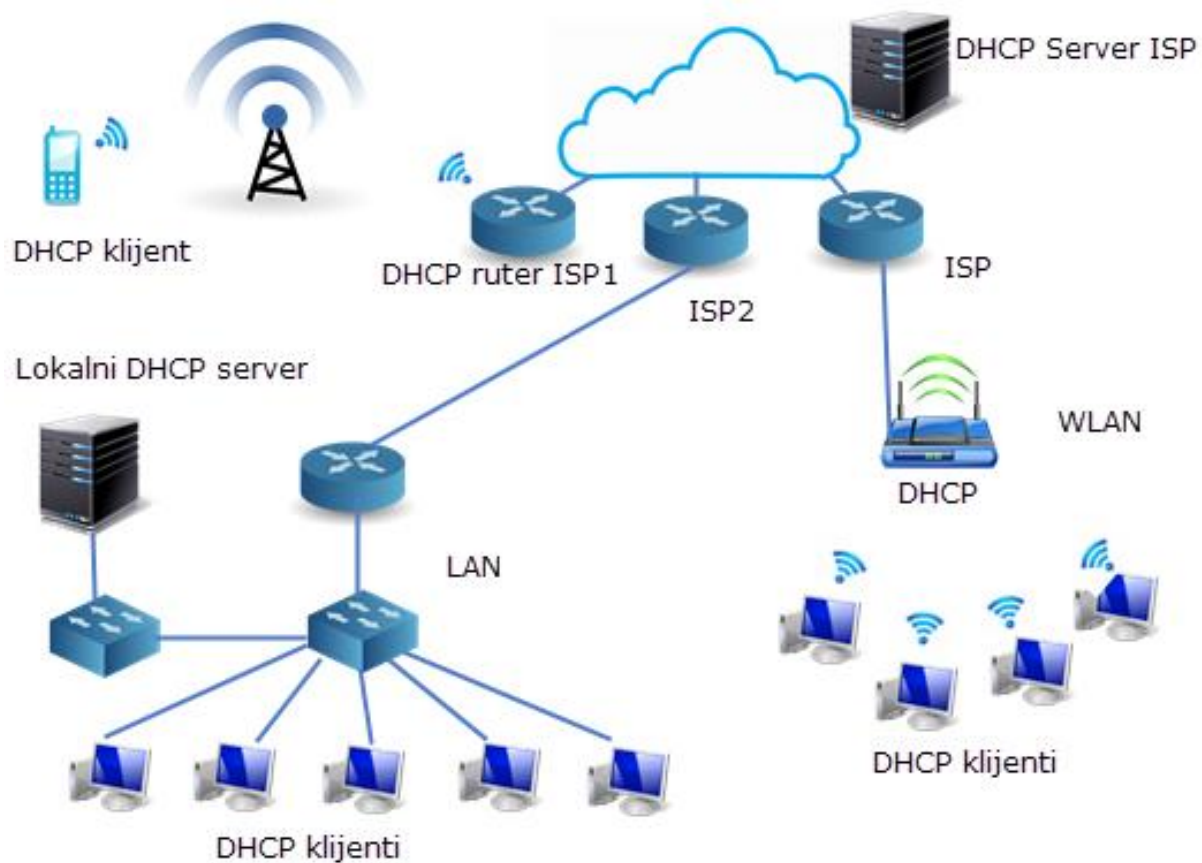
Automatska privatna IP adresa. Ukoliko IP adresa računara nije statički podešena i ukoliko DHCP ne postoji u mreži ili ne radi kako treba računar sam sebi dodeljuje IP adresu iz sledećeg opsega: 169.254.0.0 – 169.254.255.255. To se dešava kako bi računar bio u mogućnosti da se poveže sa nekim drugim računarom bez potreba poznavanja računarskih mreža i načina adresiranja od strane korisnika. Računar sam dodeljuje sebi adresu iz datog opsega.



DHCP – Dynamic Host Configuration Protocol

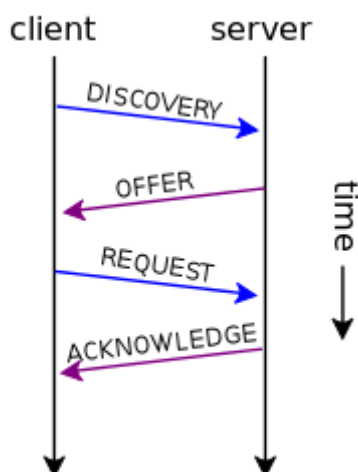
Dinamička dodela IP adrese od strane DHCP servera. Osnovene informacije koje DHCP dodeljuje su: IP adresa, maska, Default Gateway, IP adresa DNS servera.

- IP adresa – sa njom se računar identifikuje u reži
- Subnet mask – identifikuje mrežu kojoj pripada, na koju je vezan računar
- Default Gateway – identifikuje mrežni uređaj preko kojeg računar, mreža kojoj pripada, pristupa udaljenim lokacijama van mreže, komunicira sa računarima iz drugih mreža
- Opciono daje informaciju na kojoj IP adresi se nalazi DNS server



Postupak DHCP mehanizma:

- DHCP Discover – računar šalje broadcast poruku na mrežu u cilju otkrivanja DHCP servera i traži da mu se dodeli IP adresa
- DHCP Offer - poruka stiže do svih, pa i do DHCP servera koji prepoznaje da neki host želi da pristupi mreži, odgovara mu tako što mu ponudi IP adresu iz opsega koji je namenjen za dodeljivanje
- DHCP Request – računar obaveštava da želi da prisvoji tu adresu i šalje poruku DHCP serveru
- DHCP Acknowledgment – DHCP potvrđuje da računar može da prisvoji tu adresu

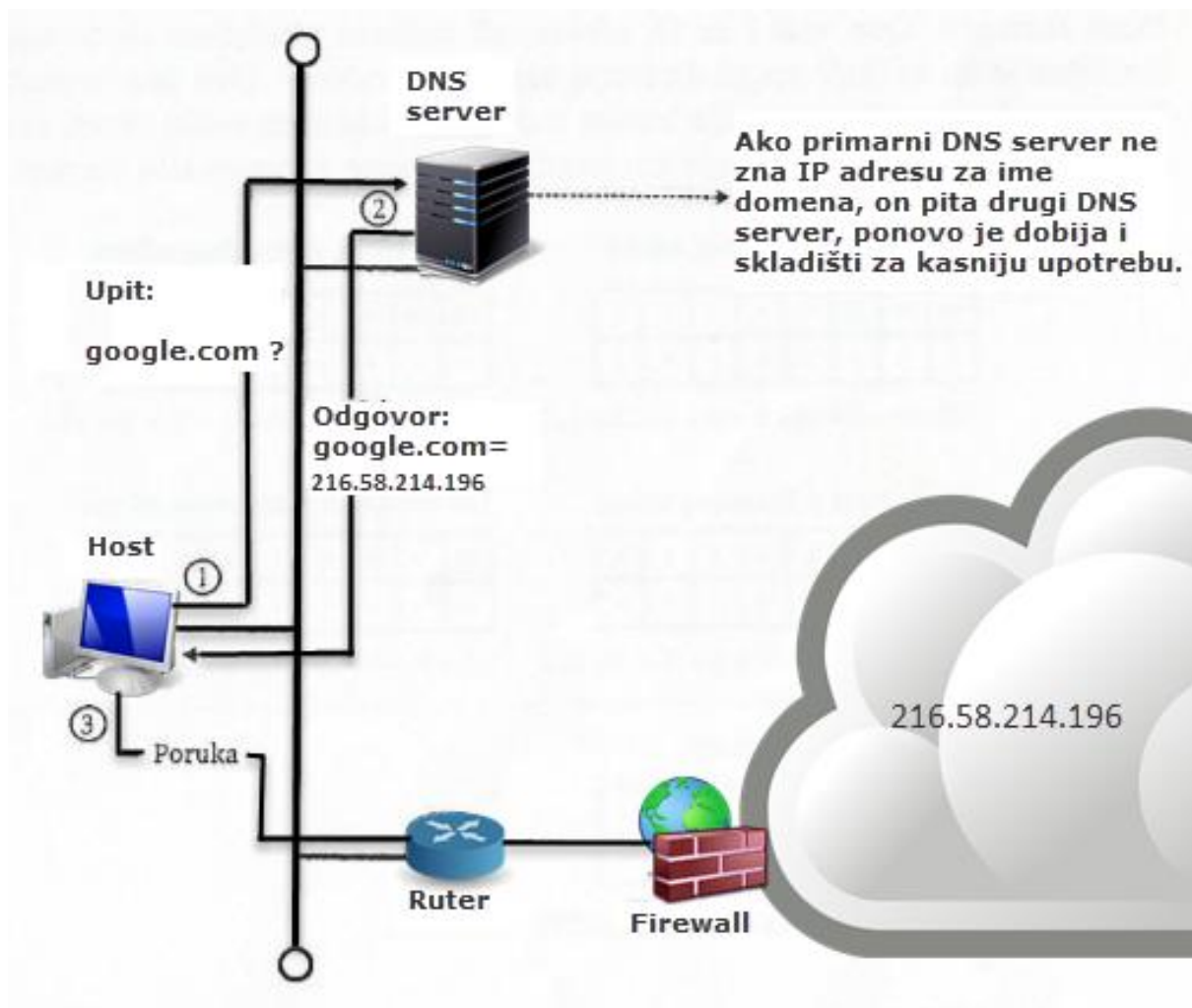


DNS – Domain Name System

Sistem koji prevodi Domain imena u IP adrese. Kada korisnik želi da komunicira sa drugim korisnikom ili serverom (npr. WEB pregledač) neophodno je da zna tačnu njegovu lokaciju u mreži, odnosno IP adresu. Da ne bi pamtili sve adrese u mreži i pravili svoj imenik adresa komunikacija otpočinje tako što znamo ime korisnika ili ime domena.

Kada u Web browser-u ukucamo neku URL adresu, računar ne ide direktno, odmah do tog web servera, ne traži sadržaj tog sajta već prvo kontaktira DNS server. Informacija gde se nalazi, na kojoj IP adresi DNS server uneta je ili ručno, statički, ili je IP adresa dobijena od DHCP servera. Računar se obraća DNS-u i šalje upit da mu DNS server da IP adresu na kojoj se nalazi sajt sa datim imenom. DNS na osnovu dobijenog imena pronade u svojim registrima IP adresu koja je povezana sa datim imenom i pošalje računaru odgovor sa odgovarajućom IP adresom. DNS server prvo pretražuje u svojim registrima, ukoliko ne pronade odgovor šalje zahtev sledećem nadređenom DNS-u i sve tako dok se ne pronade odgovor. Računar kada sazna pravu IP adresu nekog sajta direktno šalje zahtev tom web serveru da mu prosledi njegov sadržaj. Sve ovo dešava se u pozadini rada Web pregledača i računara tako da mi ne vidimo to.

DNS - Registar u kome su Domain imena mapirana IP adresama, svako Domain ime, URL upareno je sa nekom IP adresom. DNS server predstavlja adresar imena i IP adresa.



HTTP – HyperText Transfor Protocol

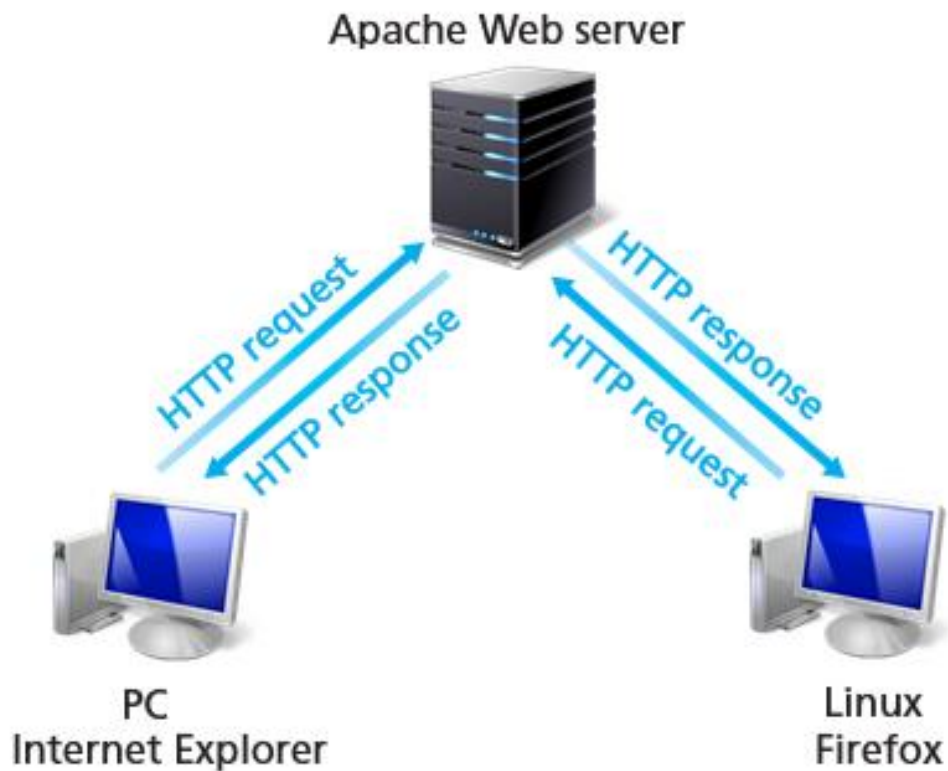
U samom srcu Weba nalazi se protokol HTTP, protokol sloja aplikacija. HTTP se implementira u dva programa - klijentskom i serverskom. Protokol HTTP definiše način na koji web klijenti (Čitači) traže web strane od web servera, kao i način na koji web serveri šalju tražene strane klijentima. Kada korisnik zatraži neku web stranicu (mišem izabere hipervezu), čitač šalje serveru HTTP poruke zahtevajući objekte sa date stranice, server prima ove zahteve i odgovara HTTP porukama u kojima se nalaze traženi objekti.

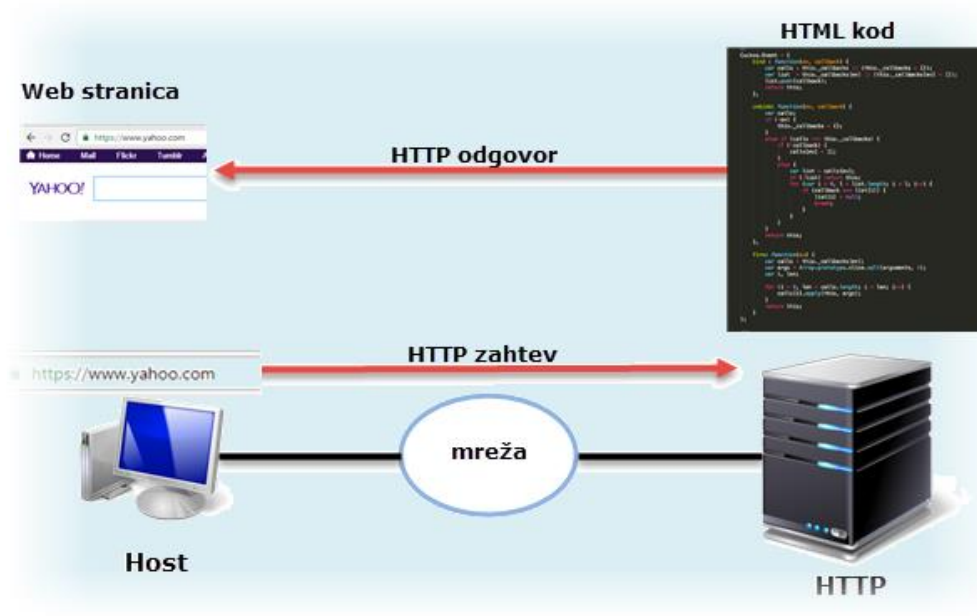
- Web resurse obezbeđuje Web server. Host pristupa resursima koristeći Hipertekt Transfer Protocol (HTTP) ili bezbedni HTTP (HTTPS)
- HTTPS dodaje šifrovanje i servis provere identiteta pomoću Secure Sockets Layer (SSL) protokola ili novijeg Transport Layer Securiti (TLS) protokola
- HTTP radi na portu 80. HTTPS radi na portu 443

Browser interpretira tri dela URL-a:

- 1. http (protokol ili šema)

- 2. www.yahoo.com (naziv servera)
- 3. index.html (zahtev specifične datoteke)
- Pretraživač zatim proverava sa Domain Name Server (DNS) za pretvaranje www.yahoo.com u numeričke adrese, koje se koristi za povezivanje na server. Koristeći HTTP zahtev, pretraživač šalje zahtev na server i traži index.html fajl. Server šalje HTML kod za ovu web stranicu nazad u browser-u klijenta, i na kraju, browser prikazuje formatiranu stranicu HTML koda.





Hypertext Transfer Protocol (HTTP) je mrežni protokol koji pripada aplikativnom sloju OSI referentnog modela mreže. HTTP predstavlja glavni i najkorišćeniji metod prenosa informacija preko Interneta. Osnovna namena ovog protokola je isporučivanje HTML stranica (Web prezentacija). Razvoj i standardizaciju HTTP protokola nadgledaju W3C (World Wide Web Consortium) i IETF (Internet Engineering Task Force).

HTTP je protokol za komunikaciju između servera i klijenta, koji funkcioniše po principu zahtev/odgovor. HTTP klijent, koji je najčešće veb pregledač, inicira prenos podataka nakon što uspostavi TCP/IP vezu sa udaljenim veb serverom na određenom mrežnom komunikacionom portu (uglavnom je to port 80, a ređe, može biti i 8080). Klijent šalje HTTP zahtev serveru. Server, na kojem su smešteni web sadržaji, kao što su HTML fajlovi i slike, vraća odgovor klijentu. Odgovor sadrži statusne informacije zahteva i može sadržati sadržaj koji je zahtevan.

Server konstantno osluškuje zahteve na već pomenutom portu, čekajući da se klijent poveže i pošalje svoj zahtev. Zahtev se sastoji iz osnovne HTTP komande (čija je sintaksa propisana standardom i koja se sastoji iz naziva komande, imena traženom veb resursa i verzije podržanih HTTP-a) i zaglavlja koje se sastoji od određenog broja redova teksta koji bliže opisuju aspekte zahteva.

Zahtev klijenta se obrađuje na serveru i, u zavisnosti od ispravnosti zahteva i mogućnosti zadovoljavanja istog, klijentu se šalje odgovarajući odgovor. Odgovor se sastoji od izveštaja o statusu zahteva (koji se sastoji od tro-cifrenog koda i kratkog deskriptivnog teksta statusa, npr. 200 OK) i od konkretnog odgovora, ukoliko je zahtev moguće zadovoljiti. Odgovor se sastoji od zaglavlja koje je iste sintakse kao i zaglavlje zahteva, i daje osnovne podatke o prirodi odgovora.

Struktura HTTP poruka

HTTP koristi klijent/server mrežni model: HTTP klijent otvara konekciju i šalje zahtev HTTP serveru; server zatim vraća odgovor klijentu, koji obično sadrži resurse koji su traženi. Nakon

slanja odgovora, server zatvara konekciju. Format zahteva i odgovora su slični i imaju sledeću strukturu:

- Inicijalna linija,
- Nula ili više linija u zaglavlju,
- Prazna linija,
- Opcionalno - telo poruke like koje može biti fajl, tekst itd.

Inicijalna linija : Request (Zahtev)

Inicijalna linija je različita kod zahteva i odgovora. Inicijalna linija u zahtevu ima tri dela koji su odvojeni razmacima (spaces):

- HTTP Ime metod,
- Lokalna putanja traženog resursa,
- Verzija HTTP-a koji se koristi.

Evo primera inicijalne linije kod zahtevne poruke.

GET /path/to/file/index.html HTTP/1.0

- GET je najkorišćenija HTTP metoda.
- Putanja je deo URL-a nakon imena hosta. Ova putanja se takođe zove i URI (request Uniform Resource Identifier). URI je sličan URL-u, stim što je URI opštiji.
- Verzija HTTP-a dolazi na kraju zahteva u formatu "HTTP/x.x."

Inicijalna linija: Response (Odgovor)

Inicijalna linija odgovora, koja se naziva statusna linija, se takođe sastoji od tri dela razdvojenih razmacima:

- Verzija HTTP-a koja je korišćena
- Statusni kod
- Opis statusnog koda na engleskom jeziku

Evo primera inicijalne linije kod odgovora:

HTTP/1.0 200 OK

Telo poruke

HTTP odgovor može sadržati telo poruke u kojem se nalaze zahtevani resursi od strane klijenta, a ponekad se u telu poruke može naći i detaljnije objašnjenje o nastaloj grešci. U HTTP zahtevu, telo poruke sadrži resurse koje treba poslati na server.

Ako HTTP poruka sadrži telo, onda moraju postojati i dodatne linije u zaglavlju koje će opisati tekst iz tela poruke. Najčešće su to:

- Content-Type: zaglavlje opisuje tip podataka koje se nalaze u telu poruke, kao što su npr. text/html ili image/gif.
- Content-Length: zaglavlje daje broj bajtova iz tela poruke.

Pimer zahteva i odgovora:

Request

GET /index.html HTTP/1.1

Host: www.example.com

Response

HTTP/1.1 200 OK

Date: Mon, 23 May 2005 22:38:34 GMT

Content-Type: text/html; charset=UTF-8

Content-Encoding: UTF-8

Content-Length: 138

Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT

Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)

ETag: "3f80f-1b6-3e1cb03b"

Accept-Ranges: bytes

Connection: close

HTTP metode

Slede kratka objašnjenja HTTP metoda:

GET metoda zahteva nalaže serveru da klijentu dostavi tražene resurse koje se nalaze na izabranoj URI adresi. Po standardu, zahtevi koji koriste **GET** metodu ne bi trebalo da vrše bilo koju drugu operaciju osim preuzimanja podataka odnosno resursa.

Metoda **POST** šalje podatke serveru na procesuiranje, najčešće preko HTML formi. Podaci se smeštaju u telo poruke zahteva. Ovim se mogu kreirati novi ili pak ažurirati stari resursi na serveru koji se kasnije mogu preuzeti metodom **GET**.

Metoda **HEAD** traži odgovor koji je isti odgovoru dobijenom **GET** metodom ali bez tela poruke. Ovo može biti korisno za dobijanje meta podataka koji se čuvaju u zaglavlju odgovora a da se pri tome ne učitava kompletan odgovor.

DELETE metoda briše izabrani resurs na serveru bez bilo kakvog upozorenja.

Metoda **OPTIONS** će vratiti spisak metoda koje server podržava za izabranu URL adresu.

Metode **HEAD**, **OPTIONS** i **GET** su označene kao sigurne metode jer ne vrše nikakve promene na serveru, tj dopuštaju samo pregled resursa. Za razliku od njih, metode **POST**, **PUT** i **DELETE** mogu dovesti do promena stanja servera te se zbog toga smatraju nesigurnim.

HTTP linije zaglavlja

Linije zaglavlja pružaju informacije o zahtevu i odgovoru kao i objektima poslatim kroz telo poruke. Prikazaćemo listu raspoloživih polja zaglavlja koja su dostupna u verziji HTTP/1.0.

Allow

Allow polje zaglavlja prikazuje listu HTTP metoda koje podržavaju resursi na traženoj URI lokaciji. Osnovna svrha je, dakle, da klijentu jasno prikaže koje metode može da koristi.

Primer: *Allow: GET, HEAD*

Authorization

Ovo polje sadrži podatke o autentifikaciji klijenta.

Primer: *Authorization : credentials*

Content-Encoding

The Content-Encoding entity-header field is used as a modifier to the media-type. Kada je ovo polje prisutno, njegova vrednost pokazuje na koji način je resurs kodiran, kao i način na koji je potrebno izvršiti dekodiranje. Content-Encoding se najviše koristi za obezbeđivanje bezbedne kompresije dokumenta, pri čemu se zadržava podešeni kodni sistem.

Primer: *Content-Encoding: x-gzip*

Content-Length

Content-Length prikazuje veličinu tela poruke, i to u decimalnom broju okteta, to jest u bajtovima

Primer: *Content-Length: 3495*

Content-Type

Content-Type polje zaglavlja prikazuje tip resursa koji se šalje klijentu kroz telo poruke odgovora.

Primer: *Content-Type: text/html*

From

Ovo polje bi trebalo da sadrži e-mail korisnika koji koristi klijent.

Primer: *From: webmaster@w3.org*

Last-Modified

Prikazuje kada je resurs poslednji put modifikovan odnosno ažuriran.

Primer: *Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT*

Location

Prikazuje lokaciju resursa koristeći zahtevani-URI. Za određene odgovore moguće je da ovo polje prikaže URL adresu. Maksimalno jedna URL adresa se može dobiti kroz ovo polje HTTP zaglavlja.

Primer: *Location: http://www.w3.org/NewLocation.html*

Server

Ovo polje zaglavlja sadrži informacije o softveru koji server koristi da bi obradio zahtev.

Primer: *Server: CERN/3.0 libwww/2.17*

User-Agent

Ovo polje prikazuje informacije o klijentu, to jest veb pregledaču korisnika. Ovo polje se uglavnom koristi u statističke svrhe, za praćenje grešaka u protokolu na različitim klijentima, i slično.

Primer: *User-Agent: CERN-LineMode/2.15 libwww/2.17b3*

HTTP statusni kodovi

Već smo pominjali da se u zaglavlju svakog odgovora u inicijalnoj liniji nalazi statusni kod odgovora. HTTP statusne kodove odgovora možemo podeliti u pet grupa:

- **1XX** – Informacije
- **2XX** – Uspeh
- **3XX** – Redirekcija
- **4XX** – Greška na klijentskoj strani
- **5XX** – Greška na serveru

Slede bliža objašnjenja nekih od statusnih kodova koji se često susreću:

200 OK

Standardan odgovor za svaki uspešan HTTP zahtev. Odgovor zavisi od korišćene HTTP metode zahteva. U slučaju GET metode, ovaj statusni kod obaveštava klijenta da je resurs pronađen i prikazan. Ukoliko je korišćena POST metoda, status će obavestiti da su preduzete akcije uspešno izvršene.

301 Moved Permanently

Ovaj i svi naredni zahtevi se redirektuju na datu novu URL adresu.

400 Bad Request

Zahtev ne može biti procesuiran zbog greške u sintaksi.

401 Unauthorized

Slično kao i kod "403 Forbidden" statusnog koda, međutim ovaj kod nam poručuje da bismo mogli pristupiti resursima ukoliko izvršimo autentifikaciju.

403 Forbidden

Zahtev je ispravan ali server odbija da odgovori na. Ovaj statusni kod se pojavljuje kada nisu dozvoljena prava pristupa resursima na serveru.

404 Not Found

Traženi resurs nije pronađen na datoj URL adresi, međutim moguće je da će uskori biti dostupan ponovo.

500 Internal Server Error

Generiška poruka o grešci koja se prikazuje kada server nema drugo "objašnjenje" zašto je greška nastala.

HTTP server

Kada kažemo HTTP server u stvari mislimo na Web server, jer Web server upravo koristi HTTP protokol za rad. Osnovna funkcija Web servera je da dostavlja web prezentacije klijentima, dakle, slanje HTML dokumenata i svega ono što takav dokument može sadržati: teks, slike, video materijal itd.

U današnje vreme, najkorišćeniji Web server na Internetu je Apache server.

Korisne komande

Kuca se u CMD-u (komandnoj liniji):

- *ipconfig /all* – detaljan pregled mrežne konfiguracije (IP adresa, MAC adresa, adresa DNS servera, Default Gateway, naziv adaptera)
- *ipconfig /release* – oslobađanje, odbacivanje već postojeće konfiguracije koju smo dobili od DHCP servera
- *ipconfig /renew* – tražimo od DHCP servera da nam dodeli mrežne parametre
- *nslookup (ime nekog sajta)* – pretražuje DNS zapis i vraća nam tačnu adresu datog sajta
- *ipconfig /displaydns* – prikaz DNS skorijih DNS zapisa koje računar čuva u svojim registrima
- *ipconfig /flushdns* – brisanje postojećeg DNS zapisa na računaru koji su sačuvani
- *ping (ip adresa nekog hosta na mreži)* – slanje malih paketa hostu na datoj adresi i čekanje odgovora, ispitivanje da li postoji konekcija sa udaljenim hostom
- *tracert (ip adresa ili ime sajta)* – popis svih čvorova kroz koji prolaze paketi pri komunikaciji sa datim hostom i odziv paketa
- *pathping (ip adresa ili ime sajta)* - popis svih čvorova koji se nalaze na putanje koju koriste dva hosta i odziv između svaka dva čvora, vreme propagacije, može da se vidi na kom linku postoji zagušenje