

Aktivni mrežni uređaji

Aktivne mrežne komponente su uređaji koji upravljaju saobraćajem na mreži. Neke su sofisticiranije od drugih, ali imaju istu namjenu, da podatke koje šaljete transportuju do odredišta, kao i da podatke koje vi potražujete dopreme do vas.

Aktivni uređaji su funkcijski slični. Razlikuju se po broju portova, modula, tipu mreže za koji su projektovani, ali je filozofija koja stoji iza njih ista.

U nastavku su opisani uređaji koji se koriste u realizaciji mreža, počev od onih neophodnih za realizaciju svih vrsta mreža pa sve do uređaja potrebnih za realizaciju WAN mreža. Tu spadaju ripiteri, habovi, mostovi, svičevi, ruteri i *firewall*-ovi.

Ripiter (Repeater)

Ripiteri su jednostavni uređaji sa dva porta, koji rade na fizičkom nivou. Pojednostavljeno rečeno, na jednom portu (priključku) ripiter prima signal i prenosi na drugi port.

Pojednostavljeno rečeno, na jednom portu (priključku) ripiter prima signal i prenosi na drugi port. Pritom ripiteri imaju tzv. 3R funkcionalnost:

1. obnavljaju amplitudu (*Reamplify*),
2. obnavljaju oblik (*Reshape*) i
3. obnavljaju vremenske reference primljenog signala (*Retime*)

prije nego što signal prosljede na izlazni port.

Ripiter nema informacija o signalu koji pojačava, što znači da se podjednako odnosi i prema ispravnom i prema neispravnom signalu.

Radi na prvom sloju OSI modela. Dobra strana ripitera je u tome što predstavlja jeftin način za povećanje maksimalnih rastojanja u mreži. Međutim, mana mu je što može da počne emitovanje dok je emitovanje paketa sa neke stanice u toku, što dovodi do sudara (kolizije). Zbog toga je dobro da oba porta ripitera imaju (po jednu) diodu za indikaciju emitovanja i diod za indikaciju problema.

!!!

Pošto nemaju aktivnu LOGIČKU ulogu i repiter i hab možemo smatrati dijelom pasivne mrežne opreme.

Hub se može smatrati pasivnom opremom sa gledišta da nema nikakvu logičku funkciju. On samo pojačava primljeni signal i prosljeđuje ga dalje na sve svoje portove.



Hab (Hub)

Hab je mrežni uređaj koji takođe funkcioniše na prvom OSI nivou (fizičkom nivou).

Na habu postoji više konektora (obično su to RJ-45 konektori). Na svaki konektor se priključuje po jedan kabl, preko kojeg se povezuje po jedna radna stanica ili server. Omogućava povezivanje više segmenata mreže u jedan segment.

Hab funkcioniše slično kao ripiter: ono 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.** Može se koristiti kao centralna tačka u topologiji zvijezde.

Habovi sadrže između 6 i 24 porta i mogu se postavljati i uklanjati u zavisnosti od potreba i u skladu sa razvojem mreže. Najčešće se koriste pri konfigurisanju mreža.

Svaki hab ima još jedan dodatni port koji se naziva *uplink* port. On služi za međusobno povezivanje dva haba. Povezivanje se vrši tako što se spaja uplink port jednog haba sa običnim portom drugog haba.



Različite veličine habova

Hab kao uređaj nestaje (bolje rečeno već je nestao) iz računarskih mreža zbog sve niže cijene svič uređaja koji nude znatno bolje performanse.

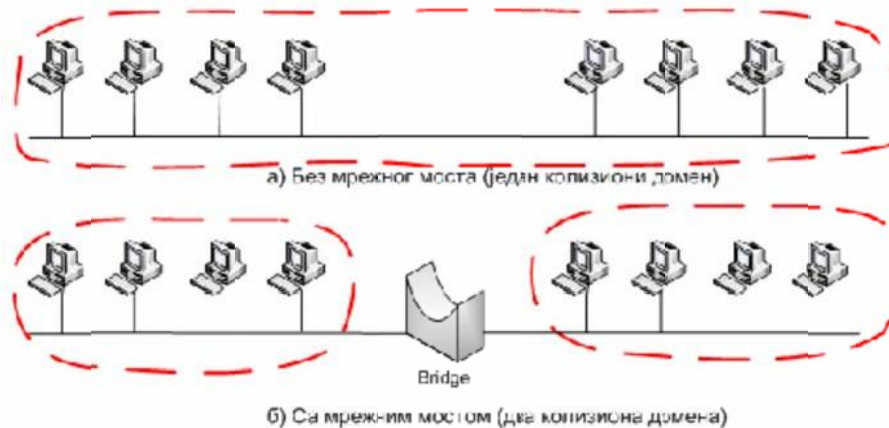
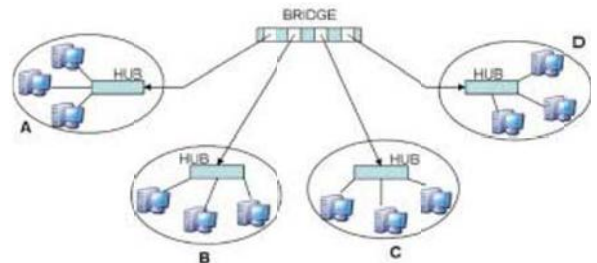
Mrežni most (Bridge)

To je uređaj koji povezuje udaljene mrežne segmente. Radi u drugom sloju OSI modela, tj. u sloju veze podataka. Do sada smo vidjeli da u datom trenutku na mreži može da emituje samo jedna stanica. Ostale stanice osluškuju saobraćaj i kada zaključče da je medijum slobodan šalju svoje pakete. Može se zaključiti da bi bilo veoma zgodno logički **podijeliti mrežu na segmente koji se sastoje iz stanica koje međusobno najviše komuniciraju**. To bi značilo da po dvije stanice u različitim segmentima mogu da komuniciraju istovremeno. Ako stanica iz jednog segmenta šalje podatke stanici u drugom segmentu, tada ostalim stanicama nije dozvoljeno da komuniciraju.

Segmentaciju mreže možemo izvršiti uređajem koji se zove mrežni most. Spolja je sličan ripiteru, a funkciono ima sve njegove osobine uz dodatak nekoliko novih koje su veoma značajne. Most provjerava sadržaj zaglavlja primljenog paketa da bi saznao MAC (fizičku) adresu izvora i odredišta. Na osnovu toga, on **formira tabelu MAC adresa** za svaki port.

Pojedini segmenti mreže se nazivaju kolizioni domeni.

Kada dobije broadcast paket (paket za sve računare u mreži), mrežni most ga samo prosljeđuje i ne pamti MAC adresu iz njegovog zaglavlja. (vidi *Adresovanje*)



Postoji pravilo u segmentiranju mreže po kome 80% saobraćaja treba da se odvija u okviru kolizionih domena, a 20% da ide preko mosta. To znači da ukoliko neke dvijestanice često međusobno komuniciraju (npr. neka radna stanica i određeni server), ne treba stavljati most između njih. Mrežni most unosi određeno kašnjenje kao posledjicu obrade paketa, ali se ono uglavnom ne osjeća.

Svič – skretnica (Switch)

Svič je za mrežni most isto što je i hab za ripiter. Dakle, na sebi ima veći broj portova. Svaki port, kao i kod mosta, ima izvestan stepen inteligencije, odnosno ne vrši samo retransmisiju paketa, već upisuje MAC adrese u odgovarajuću tabelu. Veoma značajna mogućnost koju svič posjeduje je da se na svaki port sviča može priključiti stanica, a ne segment mreže. Kolizioni domen u ovom slučaju čini stanica sa odgovarajućim portom. U ovom slučaju, saobraćaj koji vidi stanica je samo onaj koji je direktno upućen za nju, kao i broadcast poruke.



Svič omogućava podijelu LAN-a na više kolizionih domena

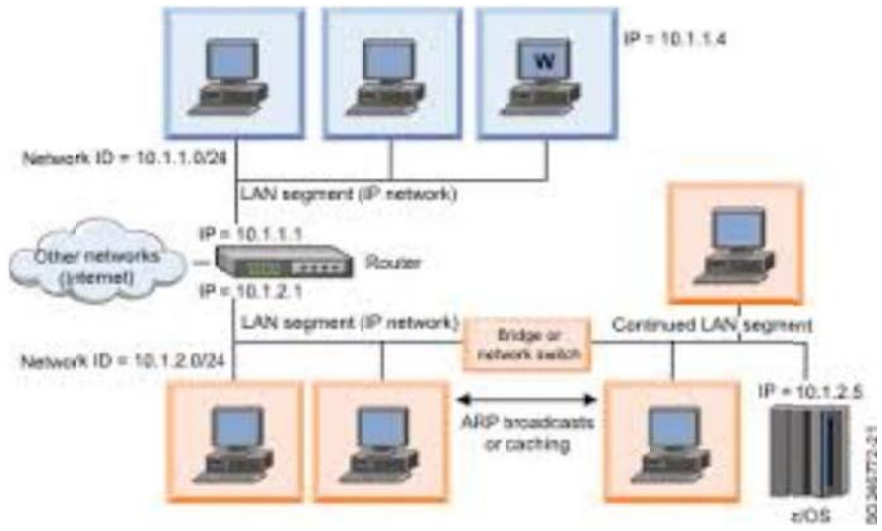
Problem koji se javlja kod upotrebe sviča je preopterećenje. Brzina kojom paketi pristižu na svič je regulisana upotrebom neke od ARQ tehnika između dolaznog porta i uređaja koji na svič šalje pakete. Međutim, može se desiti da je većina dolaznog saobraćaja upućena na neki od portova koji treba da ih proslijedi dalje i koji to nije u stanju da uradi jer kapacitet odlazne veze to ne može da podrži. Paketi koji pristižu mogu da se baferuju do izvesne granice, posle koje se odbacuju. Svičevi se bolje ili lošije nose sa ovim problemom u zavisnosti od njihovog kvaliteta (veličine bafera - memorije i brzine obrade).

Kao što smo vidjeli, mreža ne mora sadržati samo svičeve ili samo habove, već je treba balansirati u zavisnosti od potreba. Na primjer, veoma je čest slučaj u praksi da se na jedan port sviča poveže hab, a na taj hab, naravno, više stanica.

Usmjerivač (Router)

Za razliku od mrežnih uređaja koje smo do sada vidjeli i koji rade na prvom i drugom OSI nivou, ruteri rade na trećem nivou, odnosno mrežnom sloju.

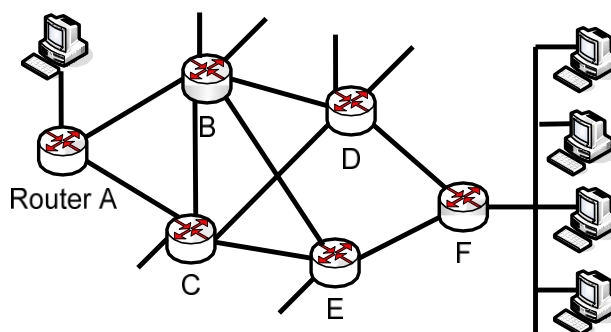
Glavna uloga rutera u mreži je da rutiraju (usmjeravanje) pakete kako bi oni stigli do svog odredišta. Informacija koja se koristi za ovu funkciju je odredišna adresa smještena u paketu. Ruter obavlja ovu funkciju tako što po prispjeću paketa izvuče odredišnu adresu, zatim nađe odgovarajući zapis u tabeli rutiranja gdje su smješteni podaci na koji port treba paket da se proslijedi i odredi adresu sljedećeg rutera na putu ka kojem se paket usmjerava. Ovaj proces se naziva „*address lookup*“. Kada se dobije ova informacija vrši se proces komutacije (*switching*) gdje se paket komutira sa ulaza na odgovarajući izlazni port odakle se šalje dalje.



Pored ovih osnovnih funkcija ruteri vrše i druge funkcije kao npr. provjera ispravnosti paketa, obrada kontrolnih paketa itd. Najnoviji trendovi su da ruteri treba da obavljaju i dodatne funkcije kao npr. „security“ protokoli, kvalitet servisa i sl. koji nameću dodatne zahtjeve ruterima. Takođe, broj korisnika računarskih mreža je u stalnom porastu tako da je saobraćaj koji generišu korisnici sve veći. Saobraćaj se takođe uvećava usljed sve novijih aplikacija koje zahtjevaju veoma velike propusne opsege (npr. prenos videa u realnom vremenu). Da bi se zadovoljili zahtjevi za povećanim saobraćajnim implementiraju se linkovi sve većeg kapaciteta (do nekoliko desetina gigabajta po sekundi) sa tendencijom da se ti protoci podignu na terabitske brzine. To znači da obrada paketa mora biti veoma brza i efikasna jer ruter sada pri takvim kapacitetima linkova mora da procesira milione paketa u sekundi i da ih prosljeđuje na odgovarajuće izlazne portove. Postoji više algoritama (algoritmi rutiranja) koji treba ovaj proces da načine što efikasnijim.

Tabela rutiranja za ruter A

Odrediš	eći skok
A
B	B
C	C
D	B
E	C
F	E



Ruteri usmjeravaju pakete na osnovu tabele rutiranja

Ruter se konfiguriše i održava svoje tabele rutiranja na osnovu mrežnih adresa. Kada primi paket, ruter prvo proveriti da li je adresa odredišta na istoj mreži kao i adresa izvora. Ako jeste, paket se odbacuje. U suprotnom, ruter prosljeđuje paket odredišnom uređaju ako je njegova mreža povezana na ruter ili sljedećem ruteru na putanji do željenog uređaja. Ruta se sastoji od tri elementa: destinacija, sljedeći uređaj na putanji i rastojanje, odnosno cijena ukupne rute do odredišta koje se još naziva i metrika. U nekim protokolima metrika predstavlja samo broj linkova na putanji do odredišta, na nekim vrijeme u sekundama i slično.

Svaki protokol rutiranja koristi različiti algoritam za utvrđivanje kada su dostupne nove rute i koja je ruta najbolja na osnovu metrike.

Prosljeđivanje paketa do mreža sa kojima ruter nije u direktnoj vezi može da se vrši na dva načina:

1. **Statičke putanje** - Reč je o putanjama koje administrator ručno ustanovljava. Kada god topologija mreže iziskuje ažuriranje (na primjer, prilikom kvara na vezi), administrator mreže ovakvu putanju mora da ažurira.
2. **Dinamičke putanje** - Ove putanje ruter automatski saznaje nakon što administrator konfiguriše protokol rutiranja. Za razliku od statičkih putanja, čim mrežni administrator uključi dinamičko rutiranje, informacije o rutiranju se samim procesom rutiranja automatski ažuriraju svaki put kada se od nekog ruteru u okviru mreže primi informacija o novoj topologiji.

Mrežni prolaz (gateway)

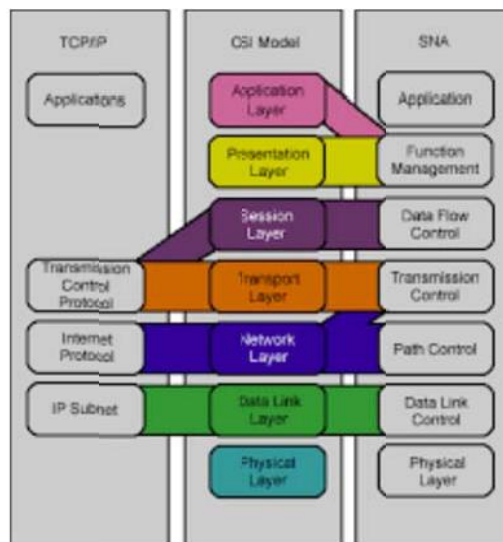
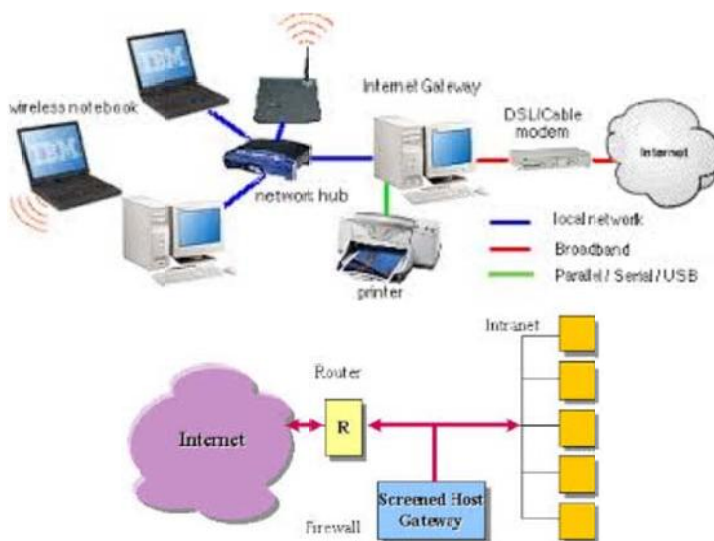
Mrežni prolaz je hardverski uređaj i/ili softverski paket koji povezuje dva **različita** mrežna okruženja. Omogućava komunikaciju između različitih arhitektura i okruženja. Vršiti prepakivanje i pretvaranje podataka koji se razmjenjuju između potpuno drugačijih mreža, tako da svaka od njih može razumjeti podatke iz one druge. Mrežni prolaz je obično namjenski računar, koji mora biti sposoban da podrži oba okruženja koja povezuje. Svakom od povezanih mrežnih okruženja, mrežni prolaz izgleda kao čvor u tom okruženju.

Zahtjeva značajne količine RAM memorije za čuvanje i obradu podataka. Radi u sloju sesije i aplikativnom sloju. Kako povezuje različite mreže, **mrežni prolaz mijenja format poruka** da bi ih prilagodio krajnjim aplikacijama kojima su namjenjene, vrši prevođenje podataka (iz ASCII u EBCDIC kod, na primjer) kompresiju ili ekspanziju, šifrovanje ili dešifrovanje, i drugo.

Drugi naziv za gateway je i **prevodilac protokola**. Dakle, **osnovna namjena mrežnih prolaza je konverzija protokola**.

Radi između transportnog i aplikativnog sloja OSI modela. Danas u svijetu postoji veliki broj autonomnih mreža, svaka sa svojim različitim hardverom i softverom.

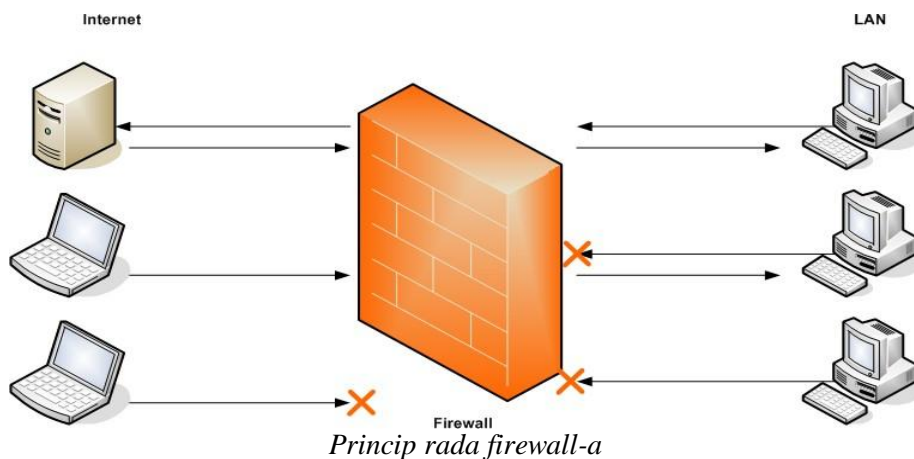
Autonomne mreže međusobno se mogu razlikovati po više karakteristika: algoritmima za rutiranje, implementiranim protokolima, procedurama za administriranje i vođenje politike mreže i dr.



No nezavisno od nabrojanih razlika, korisnici jedne mreže imaju potrebu da komuniciraju sa korisnicima povezanim na drugu mrežu.

Bezbjednosna barijera (firewall)

Firewall je bezbjednosni uređaj ili softver smješten između neke lokalne mreže i javne mreže (Interneta), čija je namjena da štiti podatke u mreži od neautoriziranih korisnika, (blokiranjem i zabranom pristupa po pravilima koje definiše usvojena bezbjednosna politika), što je u direktnoj vezi sa politikom sigurnosti datog informacionog sistema. Vrlo često ne moraju svi korisnici u LAN-u da imaju jednaka prava pristupa mreži. Postavljanjem *firewall* uređaja između dva ili više mrežnih segmenata mogu se kontrolisati i prava pristupa pojedinih korisnika pojedinim dijelovima mreže.



Firewall može biti softverski ili hardverski. Osnovna prednost hardverskih firewall-a je brzina rada i realizacija na specijalizovanom namjenskom operativnom sistemu što ga čini neranjivijim na tom nivou. Osnovna prednost softverskog firewall-a je proširivost. Proširivost u ovom slučaju predstavlja mogućnost proširenja skupa parametra paketa koji se mogu uzeti u obzir pre donošenja odluke šta će se sa paketom uraditi. Osnova rada *firewall*-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smjera.

Odgovoran je za više važnih stvari u okviru jednog informacionog sistema:

- implementira bezbjednosnu politiku,
- beleži sumnjive događaje,
- upozorava administratora na pokušaje napada i pokušaje kompromitovanja bezbjednosne politike,
- u nekim slučajevima obezbjeđuje statistiku korišćenja.

Samo posjedovanje firewall-a (hardverskog ili softverskog) ne znači da je računar/mreža koju on štiti bezbjedan. Naprotiv, firewall predstavlja samo alat koji je moguće iskoristiti za zaštitu ukoliko je dobro podešen (ukoliko su dobro definisana bezbjednosna pravila).

Najbolji način da se firewall podesi (ukoliko administrator nema iskustva u toj oblasti) je da se blokira sav saobraćaj a da zatim za svaku konekciju posebno donese odluka da li je treba dopustiti, trajno ili privremeno, i za koje klijente.

Mrežna kartica

Mrežna kartica je uređaj koji povezuje računar sa računarskom mrežom. Često se naziva: mrežni adapter, mrežni interfejs, *NIC*... Jedan od važnijih elemenata svake mrežne kartice je *MAC* adresa koja čini da ovaj uređaj radi na 2. sloju *OSI* modela. *MAC* adresa predstavlja 48-bitni serijski broj iz opsega koji *IEEE (Institute of Electrical and Electronics Engineers)* dodeljuje proizvođaču.

Mrežne kartice su se ranije u računarima mogle naći najčešće u vidu zasebnih kartica dok se **danas uglavnom integrišu u matične ploče računara**. Ako se koristi odvojena mrežna kartice, obično se uzima kao dodatna kartica (uz integrisanu) zbog mogućnosti priključivanja više mrežnih uređaja (npr. **ADSL** modem (Ethernet) i mrežni hub) , iako neke matične ploče dolaze i sa dva čipa, odnosno priključka. U tom slučaju kartice mogu funkcionisati zasebno ili udruženo.

Mrežne kartice uglavnom imaju *RJ 45* (za *UTP* kablove), *BNC*, odnosno *AUI (Attachment Unit Interface)* konektore. Takođe, na mrežnim karticama se uglavnom nalaze i *LED* diode koje služe za praćenje aktivnosti kartice. Najčešće brzine na kojima rade mrežne kartice su 10, 100 ili 1.000Mb/s. Glavni proizvođači mrežnih kartica su *3Com, Intel, Realtek, Marvell, VIA*...

Danas postoje mrežne kartice u 10, 100, i 1000 Mbit/s (Gigabit) izvedbama, što označava propusnost podataka koju može podnijeti jedna mrežna kartica.

Mrežne kartice pakuju u okvir i prenose podatke iz računara, a potom primaju, pakuju i dekonvertuju primljeno sa mreže.

Mrežne kartice imaju specifičnu arhitekturu dizajniranu posebno za ethernet sa nekim od sledećih ulaza za konektore: *BNC*, *AUI* ili *RJ-xx*, najkorišćeniji *RJ-45*.

Svaka od ethernetskih kartica sadrži jedinstvenu fizičku adresu u svom ROM čipu. Dio ove adrese sadrži

informacije o proizvođaču, a dio je jedinstven serijski broj kartice.

Mrežna kartica se sastoji od tri osnovna dijela:

1. Sprege fizičke sredine za prenos - odgovorna za električno slanje i prijem podataka. Sastoji se od **prenosnika** koji šalje ili prima podatke i **konvertora koda**.
2. Kontrolera linka podataka - odgovara MAC podsloju
3. Računarska sprega

Mrežne kartice možemo podeliti u četiri osnovna bloka: sprega mreže, dekodler, memorijski bafer i računarska sprega.

