Računarske mreže

Dr MiomirTodorović

Mreže za prenos podataka

- Mreže za prenos podataka

  je grupa međusobno povezani komunikacionih uređaja, koji su sposobni da razmenjuju informacije (podaci, glas, slika, video)

- Računarska mreža

  je grupa nezavisnih međusobno povezanih računara

Mreže za prenos podataka

Mreže podataka mogu biti podeljene na:

- Javne mreže

  (Public Data Networks -PDNs)

- Privatne Mreže

  (Private Networks)

Privatne mreže

- na prostoru preduzeća i druge organizacije.
- instaliraju, održavaju i poseduje preduzeća ili organizacije

Javne mreže

- Packet Switched Public Data Networks (PSPDNs)
  npr. Internet

- Circuit Switched Public Data Networks (CSPDNs)
  npr. PSTN, ISDN

PDNs su mreže koje osniva i kojima upravlja nacionalni autoritet za upravljanje mrežama, specijalizovan za prenos podataka

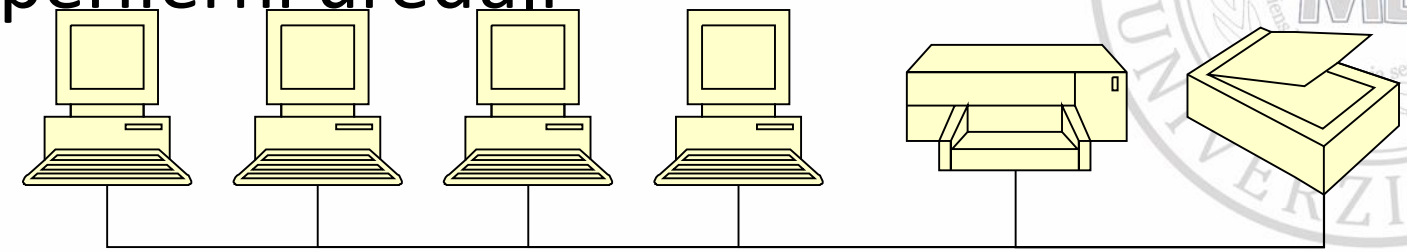
Razlozi za povezivanje

- Postoji nekoliko više računarskih sistema u računarsku mrežu:
- povećanje broja računara,
- ulazno-izlazne transakcije se vrše daleko od centralnog (host) računara,
- stariji tipovi PC-a mogu se koristiti kao interaktivni terminali ili klijent računari moćnijih računara,
- povećanje resursa koji su dostupni korisnicima,
- povećan trend ka distribuiranoj obradi podataka i dr.

Pojam

- **Mreže** su skup međusobno hardverski povezanih računara i perifernih uređaja
- **Umrežavanje** je koncept povezanih računara koji dele resurse

- Resursi koje dele umreženi računari su podaci i periferni uređaji

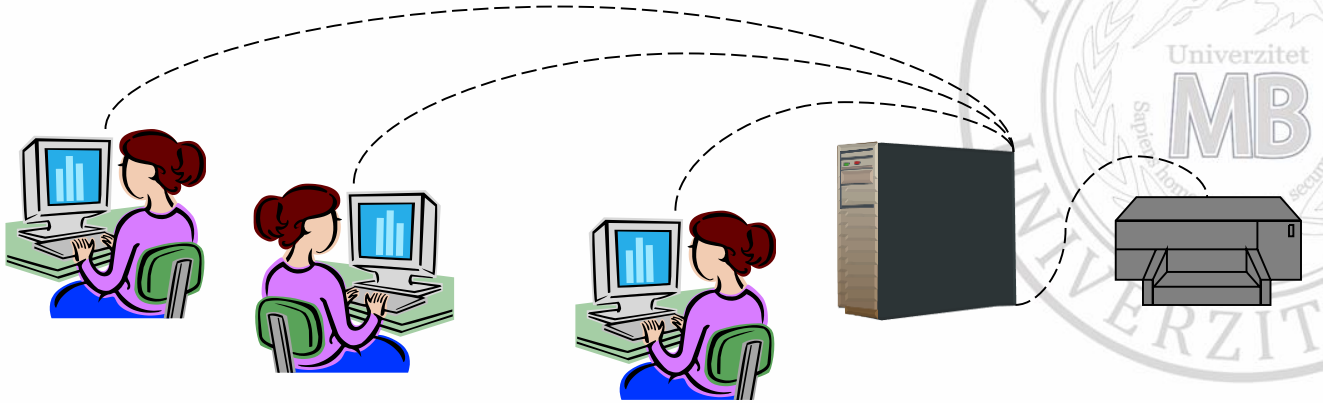


Kompjuterske mreže

- LAN – Local Area Network
  - Povezani kompjuteri i drugi uređaji su relativno blizu, obično unutar jedne zgrade
- MAN – Metropoliten Area Network
  - Povezani kompjuteri i drugi uređaji su u istom gradu
- WAN – Wide Area Network
  - Povezani kompjuteri i drugi uređaji su udaljeni, u različitim gradovima, čak i kontinentima

Prednosti korišćenja mreže

- Smanjenje troškova zahvaljujući deljenju resursa
- Standardizovano korišćenje aplikacija
- Blagovremeno dobijanje podataka
- Efikasnija komunikacija korisnika

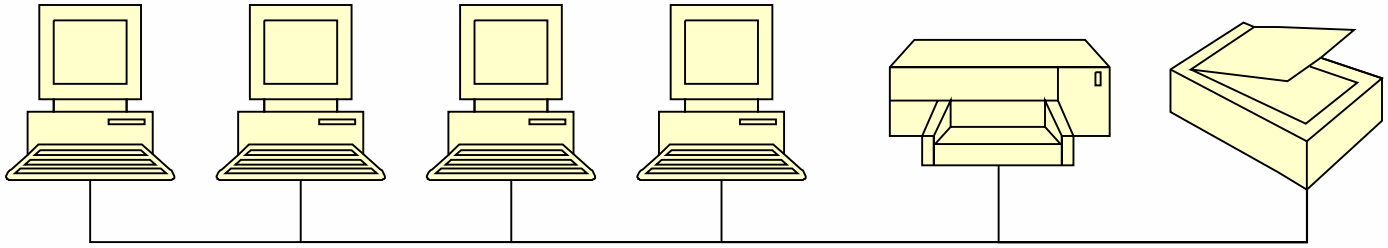


Vrste mreža prema odnosu računara

- Vrste mreža mogu biti:
  - Mreže istog prioriteta (peer to peer)
  - Serverske mreže
  - Multi-server
  - hibridne

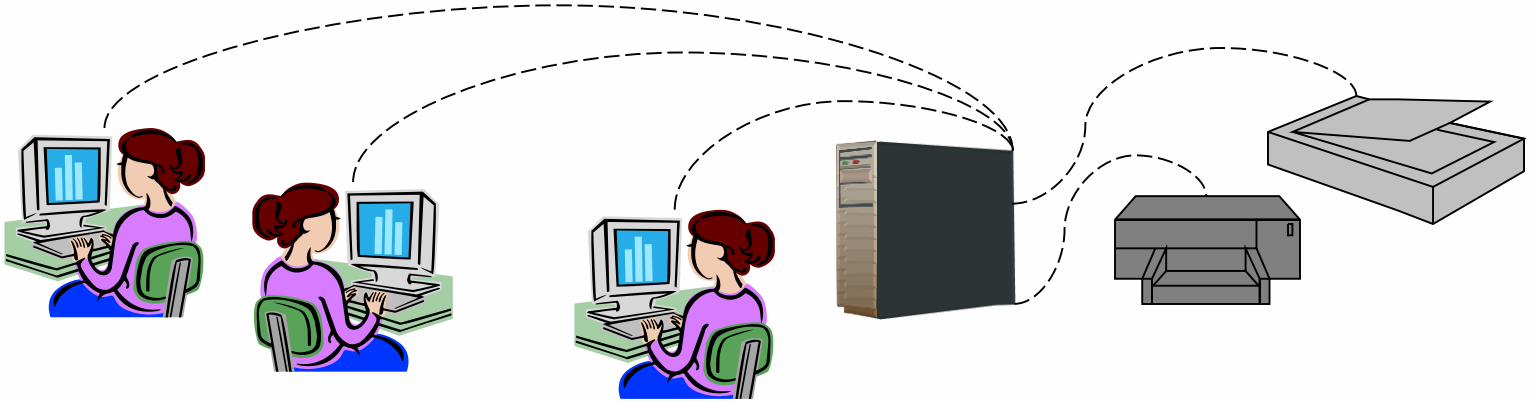
- Koju ćemo vrstu koristiti zavisi od:
  - Broja računara koji se umrežavaju
  - Potrebnog nivoa bezbednosti
  - Vrste posla
  - Budžeta
  - Znanja

Mreže istog prioriteta



- Povezuje se manji broj računara (do deset), a svaki računar istog je prioriteta – istovremeno radi i kao klijent i kao server
- **Server** – računar na kojem se nalaze resursi koje dele umreženi korisnici – klijenti
- **Klijent** – računar koji, preko servera, pristupa zajedničkim resursima

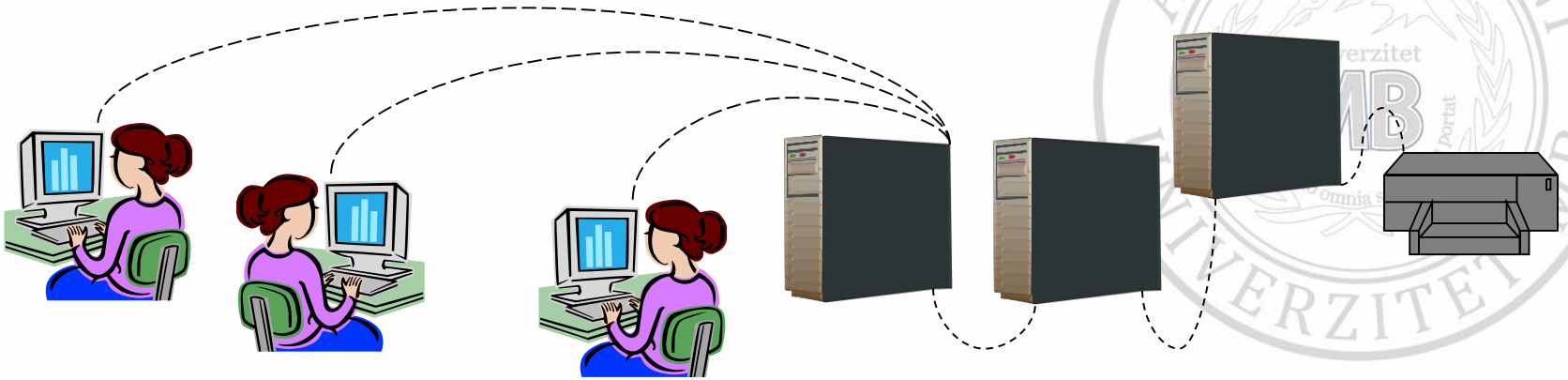
Serverske mreže



- Povezuje se veći broj računara; glavnu ulogu u mreži ima server – namenski server
- Zove se namenski jer je optimizovan da brzo opsluži zahteve mrežnih klijenata i pruži bezbednost datoteka i foldera
- Mrežni server i OS funkcioniše kao celina

Specijalizovani serveri

- U velikim mrežama serveri se specijalizuju za različite namene:
  - Za datoteke i štampanje
  - Za aplikacije
  - Za poštu
  - Fax server
  - Komunikacioni server



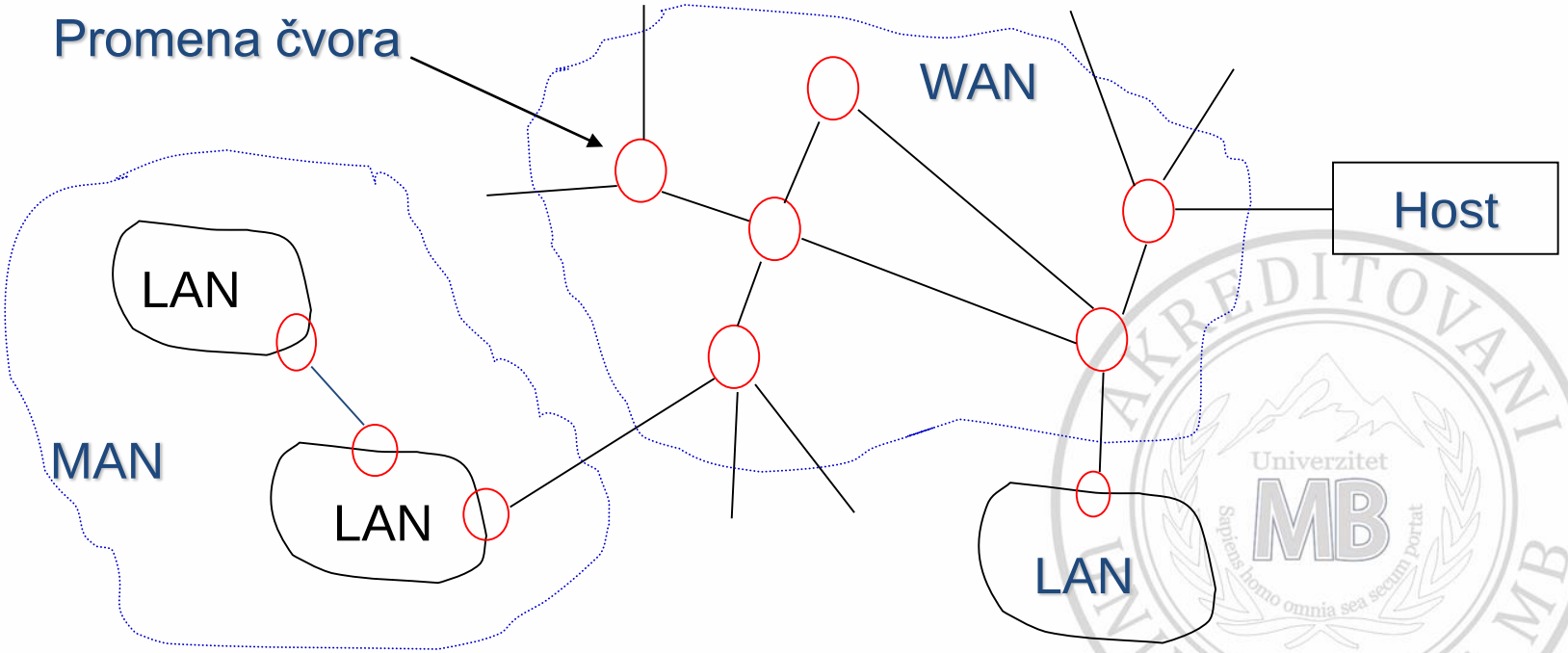
Prednosti serverskih mreža

- Bezbednost podataka (administrator brine i upravlja bezbednošću klijenata i servera)
- Centralizacija i deoba resursa
- Lako pravljenje rezervnih kopija
- Opsluživanje izuzetno velikog broja korisnika (više hiljada)
- Klijentima nije potreban dodatni hardware (memorija, diskovi)

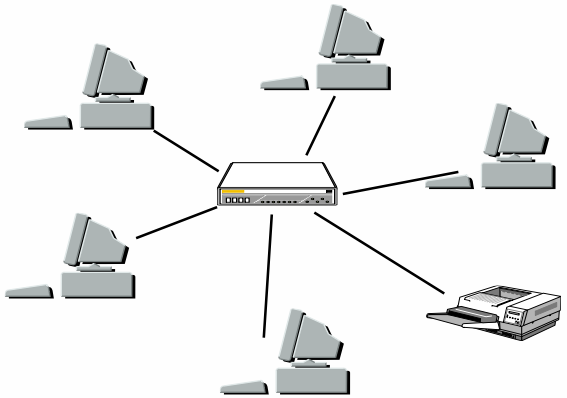
Kombinovane mreže

- Predstavljaju kombinaciju mreža istog prioriteta i serverskih mreža

Generalna struktura mreže

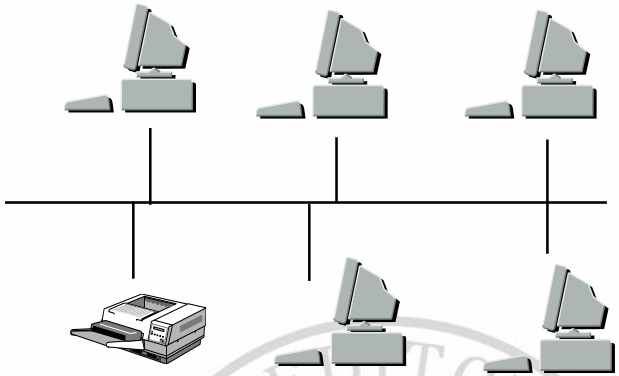


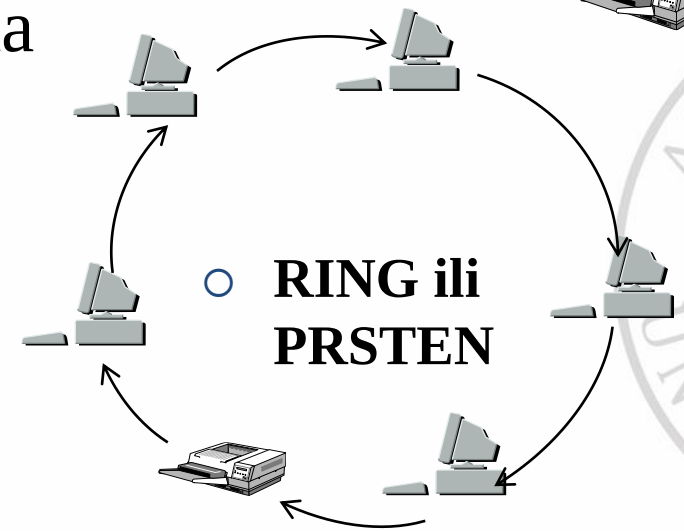
Topologije LAN mreža



Zvezda

“Bus”





- **RING ili PRSTEN**

Metodii rada - BAS topologija

Višestruki pristup zajedničkom medijumu nadgledanjem prisustva nosećeg signala (CSMA / CD)

Kod ove metode pristupa svi računari (server i klijenti) proveravaju da li je kabl slobodan za emitovanje.

Metodi rada

- Metoda **CSMA/CA** – je metoda višestrukog pristupa nadgledanjem prisustva nosećeg signala sa izbegavanjem kolizije.
- Svaki računar najavljuje da će slati podatke - niko ne šalje podatke dok ne prosledi svoju najavu;

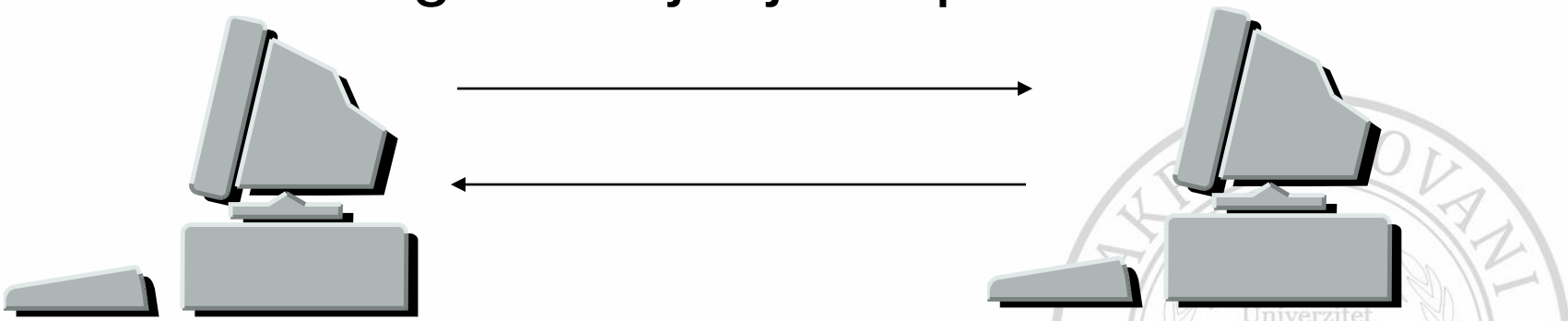
Najava dodatno usporava mrežu tako da metoda nije popularna.

Metoda kontrole pristupa prosleđivanjem tokena

- Koristi se u prstenastim mrežama.
- Specijalna vrsta paketa podataka kruži od računara do računara (token) i kada naiđe na “slobodan” token (bez podataka drugog računara) računar šalje svoje podatke.

Mrežni protokol

Bez obzira na tip mreže, kompjuteri moraju znati pravila koja moraju poštovati da bi mogli razmjenjivati podatke

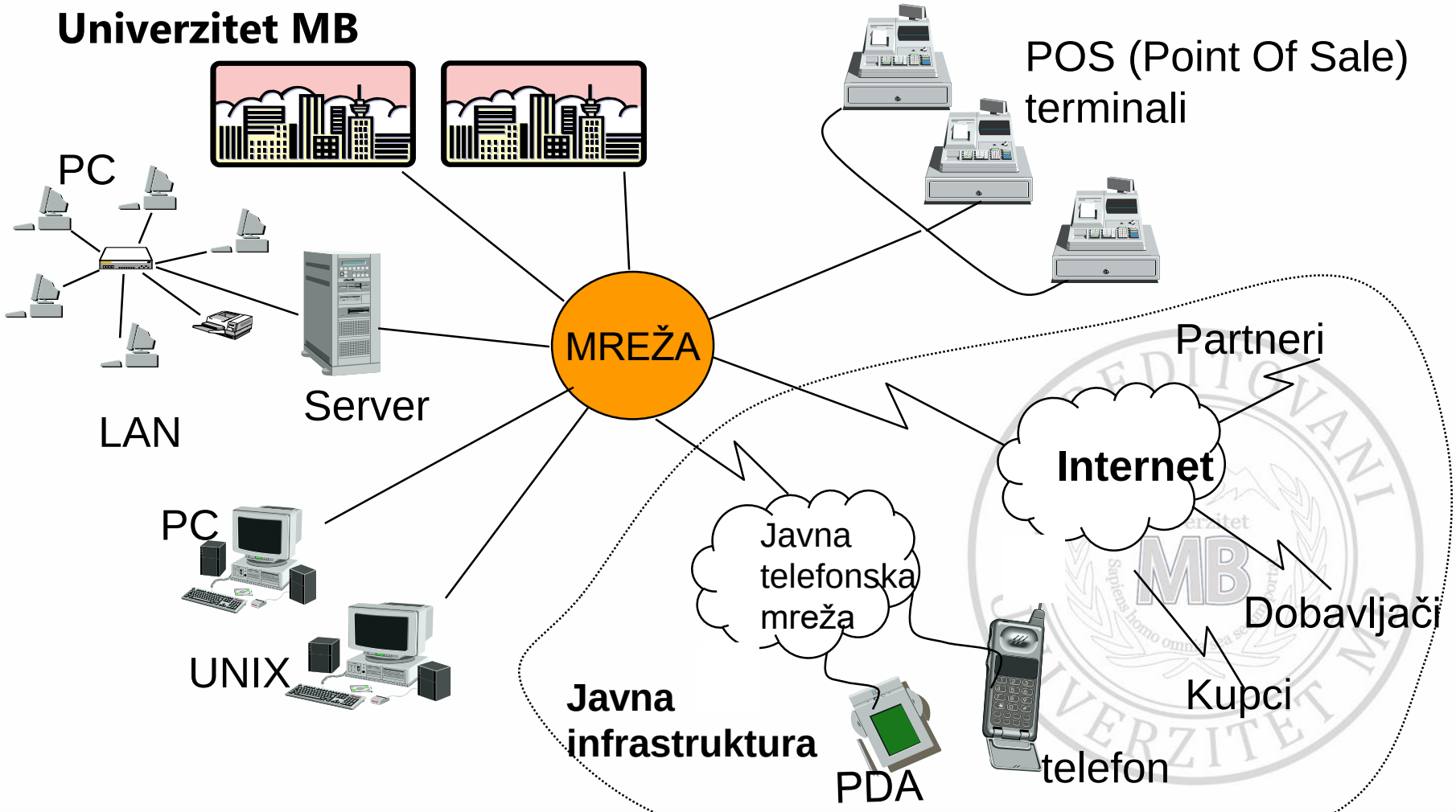


Najpoznatiji mrežni protokol

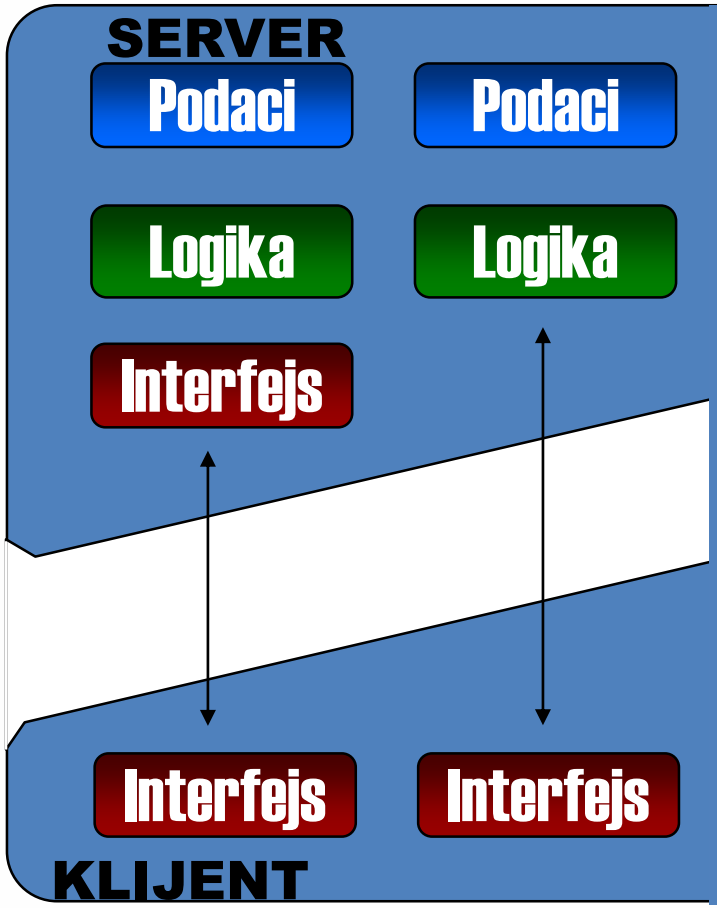
TCP/IP

(Transmission Control Protocol/Internet Protocol)

Organizacijsko umrežavanje
Internetworking – spajanje mreža



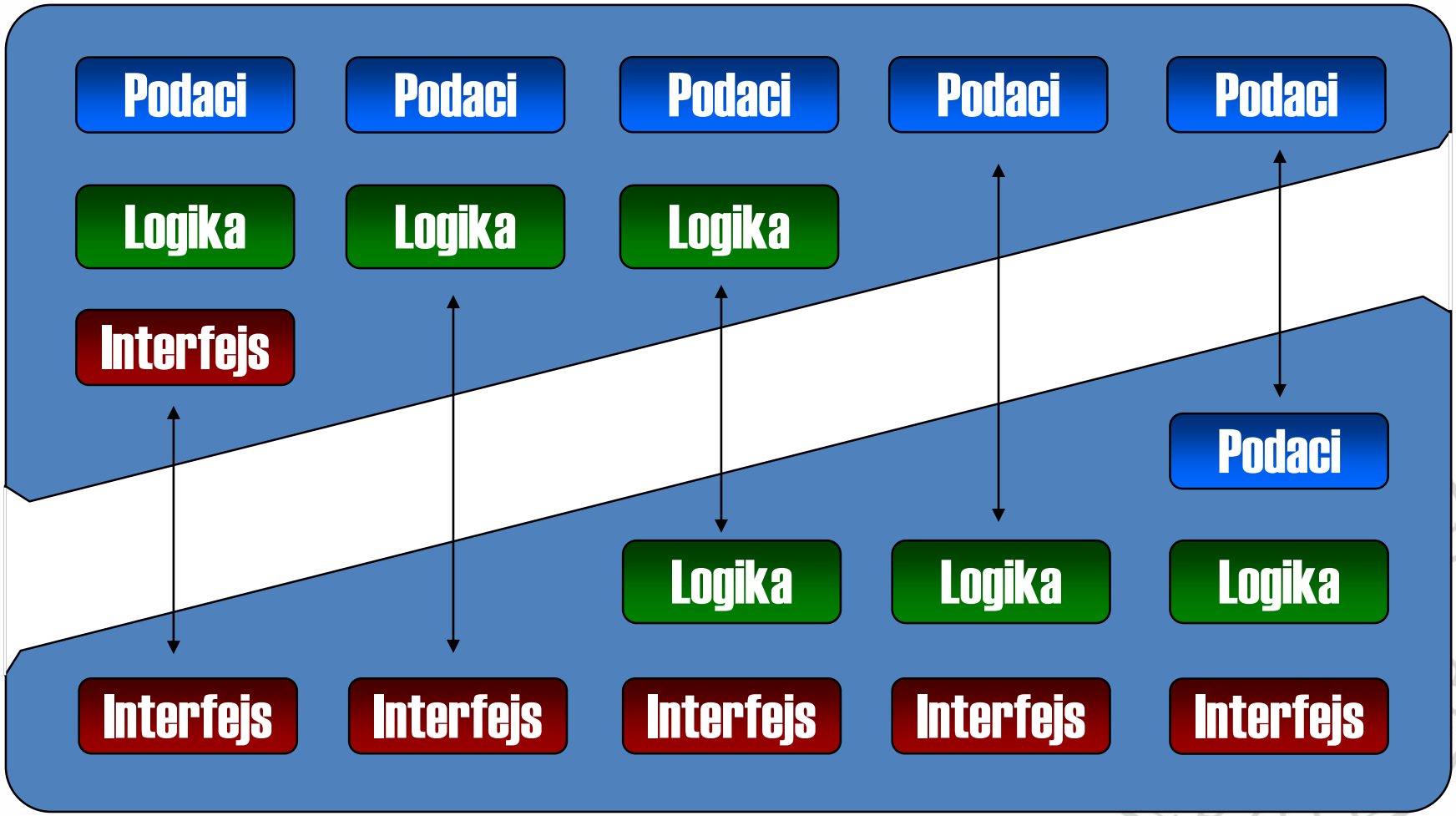
TIP Client – Server(procesiranje)



- Procesiranje je gotovo potpuno smešteno na serveru
- Klijent praktično realizuje samo ulaz i izlaz (interfejs)
- To je moguće postići jefitinim mašima, bez diskova, sa malo memorije, ..

Tipovi klijent/server procesiranja

SERVER (Može da sadržI sledeće "usluge")



KLIJENT (Može da sadrži sledeće "usluge")

Mrežni standardi

- Za povezivanje računara u mrežu postoje proizvodi različitih proizvođača hardware-a i software-a.
- Da bi mreže funkcionisale sa ovakvim proizvodima, neophodno je da se svi proizvođači drže nekih pravila – standarda.
- Više nezavisnih organizacija izradilo je specifikacije standarda za proizvode koji se odnose na umrežavanje računara.

Referentni model za povezivanje otvorenih sistema

- OPEN SYSTEMS INTERCONNECTION REFERENCE MODEL OSI
- Da bi se podaci poslali kroz mrežu računar mora da obavi nekoliko poslova:
  - Da prepozna podatke,
  - Podeli ih na delove kojima može da upravlja,
  - Da doda informaciju o identifikaciji prijemnika i delu segmenta koji nosi korisne podatke,
  - Doda informacije o vremenskoj sinhronizaciji i informaciju koja se koristi za proveru greške i
  - Da pošalje podatke.

OSI MODEL

- Međunarodna organizacija za standarde (International Standards Organization – ISO) izdala je 1987. godine skup specifikacija koji opisuje arhitekturu mreže, a koji se naziva OSI REFERENCE MODEL.

- OSI Reference model koristi se kao međunarodni standard. Model opisuje način na koji mrežni hardware i software omogućavaju komunikaciju.

Slojevi mrežne komunikacije

- Različite funkcije pri prenosu podataka razvrstane su u sedam slojeva.
- OSI model definiše kako svaki sloj komunicira sa slojem iznad i ispod njega.

7	Sloj aplikacije
6	Sloj prezentacije
5	Sloj sesije
4	Transportni sloj
3	Sloj mreže
2	Sloj veze
1	Fizički sloj

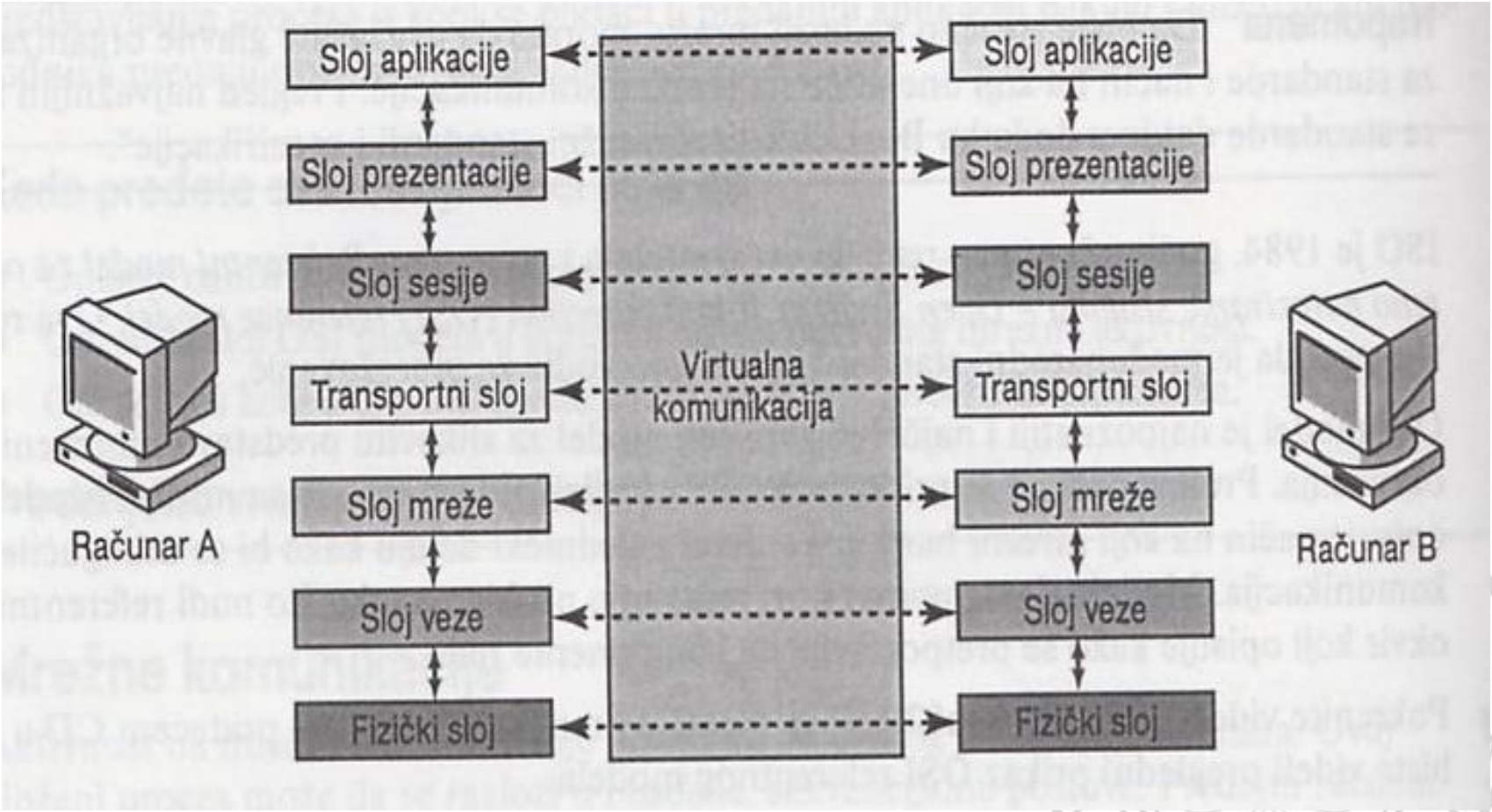
- Svaki sloj ima svoju ulogu i što je sloj viši to je i složeniji;
- Zahtevi jednog sloja prema drugom prosleđuju se interfejsom;
- Svaki sloj oslanja se na standarde sloja ispod;
- Sloj ispod vrši svoju funkciju i obezbeđuje usluge sloju iznad, a pri tome ga ne opterećuje detaljima o načinu svog funkcionisanja;

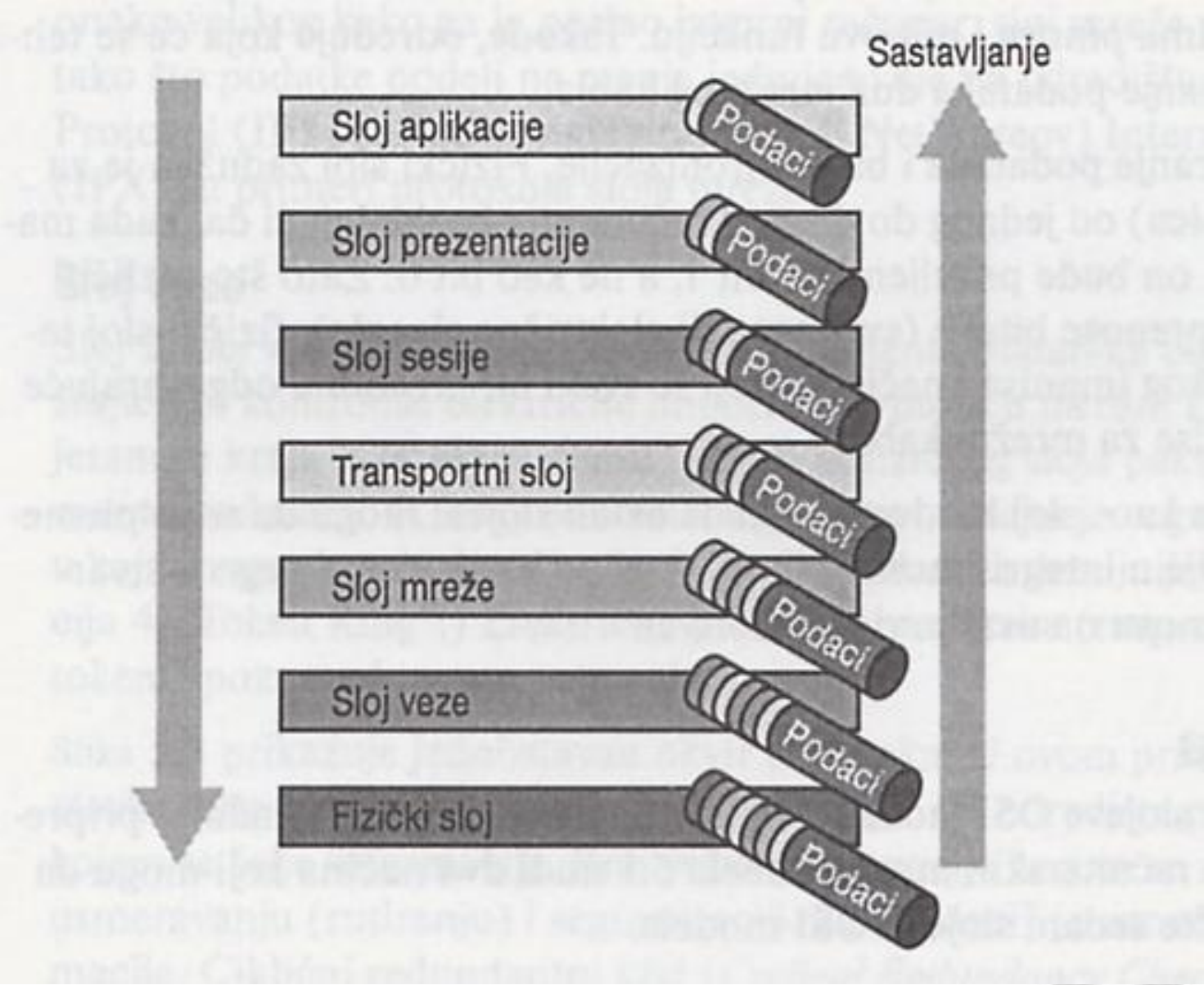
Slojevi OSI modela

- **I fizički sloj** se odnosi na karakteristike U/I interfejsa i to: mehaničke (konektor, kabl), električne (naponski nivoi, tajming) Ovaj sloj je odgovoran za prenos bitova (koji čine podatke), ali ne mari za značenje kombinacije tih bitova
- **II sloj veze** za podatke obezbeđuje uspostavljanje, održavanje (prenos podataka) i raskidanje veze. Sloj je odgovoran za kontrolu protoka podataka i kontrolu grešaka pri prenosu podataka.
- **III mrežni sloj** obavlja sledeće funkcije u računarskoj mreži: komutaciju paketa u čvorovima mreže, maršrutiranje poruka između dva DTE uređaja mreže, prevođenje logičkih adresa odredišta i odgovarajuće fizičke (brojčane) adrese, sprečava zagušenje mreže i sl. Sloj, takođe podržava komunikaciju između dve fizički povezane ali logički posebne mreže.

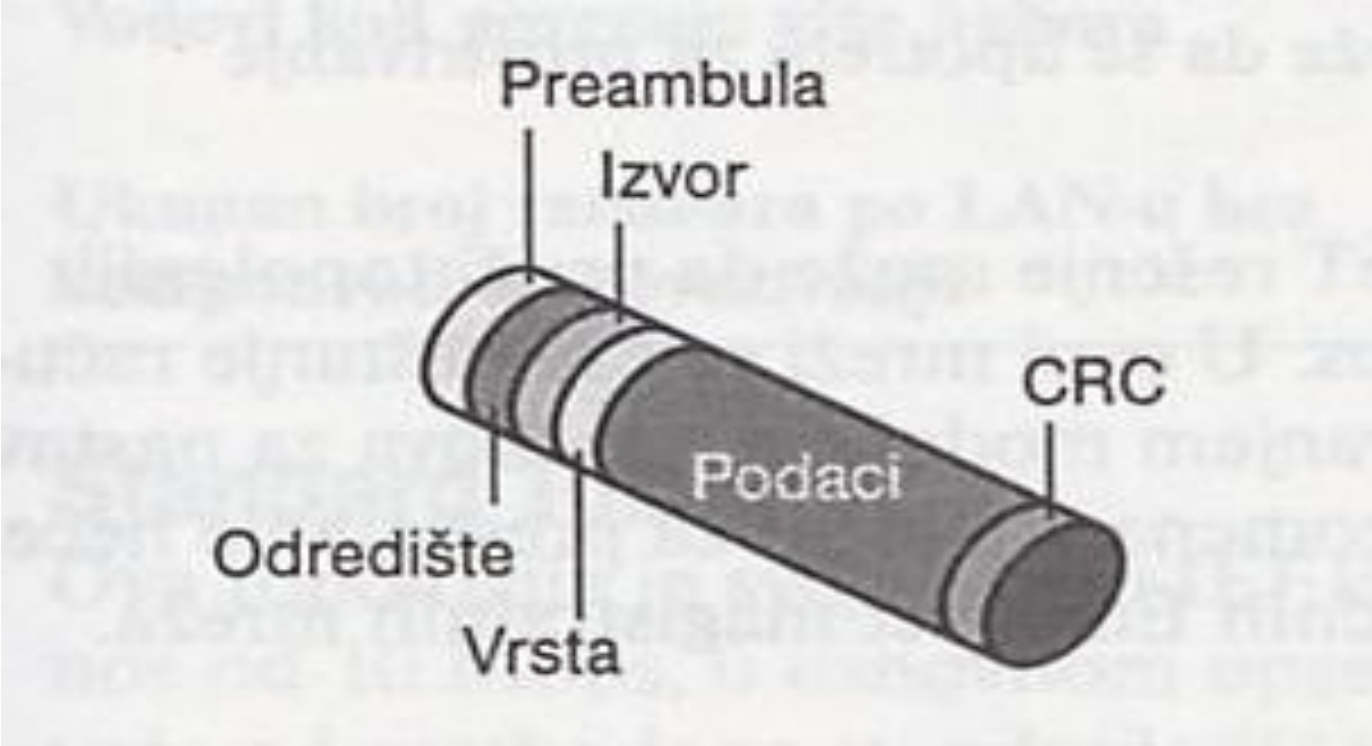
Slojevi OSI modela

- **IV transportni sloj** je najniži sloj koji koristi tzv. "end to end" protokol, tj. transportni protokol (npr. TCP/IP). Ovaj sloj je odgovoran za pouzdanost cele mreže. kreira za jednu vezu više paralelnih kanala.
- **V sloj sesije** (razgovora) upravlja dijalogom među korisnicima. Ovaj sloj logičke nazive (dobijene iz višeg sloja) preslikava u fizičke adrese koje predaje transportnom sloju. Na taj način je aplikacioni softver nezavisan od vrste računarske mreže.
- **VI soj prikaza** (prezentacije) obezbeđuje da se podaci koji se razmenjuju prikazuju korisnicima u njima razumljivom obliku.
- **VII sloj aplikacije** se nalazi na najvišem nivou OSI referentnog modela. On pruža usluge neposredno korisnikovim programima, tako da je za njih transparentna lokacija sistemskih resursa (centralizovani/distribuirani).

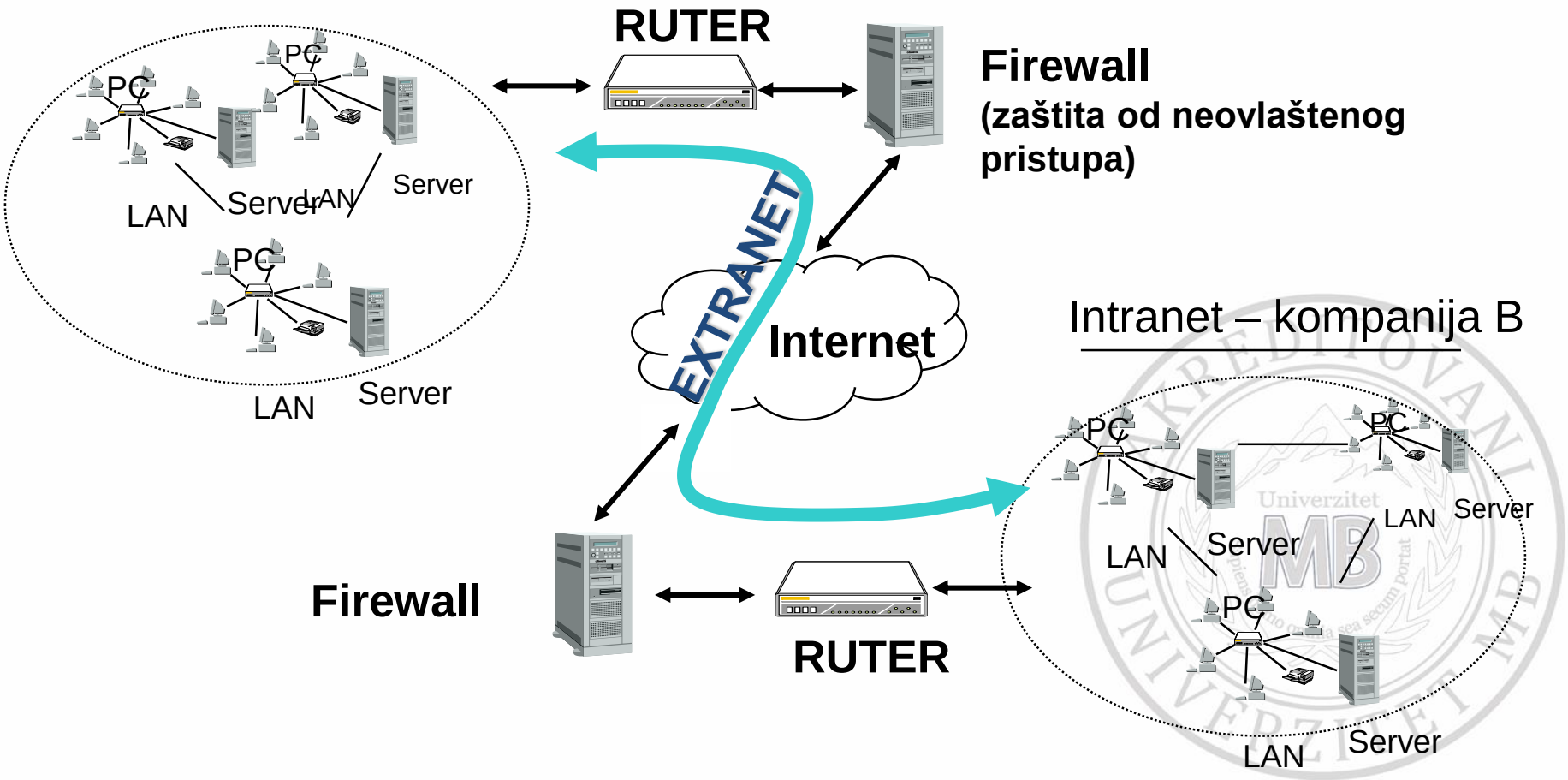

Sloj aplikacije
Sloj prezentacije
Sloj sesije
Transportni sloj
Sloj mreže
Sloj veze
Fizički sloj
Virtualna komunikacija
Sloj aplikacije
Sloj prezentacije
Sloj sesije
Transportni sloj
Sloj mreže
Sloj veze
Fizički sloj
Računar A
Računar B


Sastavljanje
Sloj aplikacije
Podaci
Sloj prezentacije
Podaci
Sloj sesije
Podaci
Transportni sloj
Podaci
Sloj mreže
Podaci
Sloj veze
Podaci
Fizički sloj
Podaci

Struktura paketa



Intranet, a sa partnerima se stvara extranet



Uređaj za povezivanje računarskih mreža

- ***Mrežna kartica***
- ***modem***
- ***Most ("bridge")***

  služi za povezivanje više mreža iste ili različite topologije, tako da one logički funkcionišu kao jedna mreža. Može se implementirati pomoću PC
- ***Ruter ("router")***

  Ruteri za usmeravanje saobraćaja koriste najkraći put, a ako dođe do prekida takvog puta, ruteri će saobraćaj usmeriti ka nekom od alternativnih puteva.
- ***Gejtvej - Prolaz***

  Najbitnije funkcije mrežnog prolaza su:
  - pretvaranje protokola,
  - prevođenje podataka,
  - pretvaranje formata ,
  - multipleksiranje.

Zastita mreze

- Da bi pristupili mrezi treba da otvorimo nalog na nekom od racunara(cvorova)mreze.Nalog otvara lice koje upravlja radom mreze – administrator mreze.
- Prilikom prijavljivanja na mrezu,potrebno je uneti u prozor za dijalog korisnicko ime I lozinku.Prilikom otvaranja naloga administrator mreze daje I odredjena prava
- Za zastitu mreze zaduzen je administrator sistema. On postavlja zastitni zid (firewall)
- Na korisnickom racunaru treba stalno da bude ukljucen antivirus

Telekomunikaciona revolucija

Kolaboracija

- Elektronska pošta
- Telefonija
- Razmena dokumenata
- Diskusioni forumi
- Razmena podataka konferencije
- Audio konferencije
- Video konferencije
- Elektronski sastanci

Trgovina

- On-line procesiranje transakcije sa mesta prodaje
- Prodaja putem Weba
- Elektronska razmena podataka
- Elektronski prenos novca
- Elektronsko bankarstvo
- Interaktivni marketing

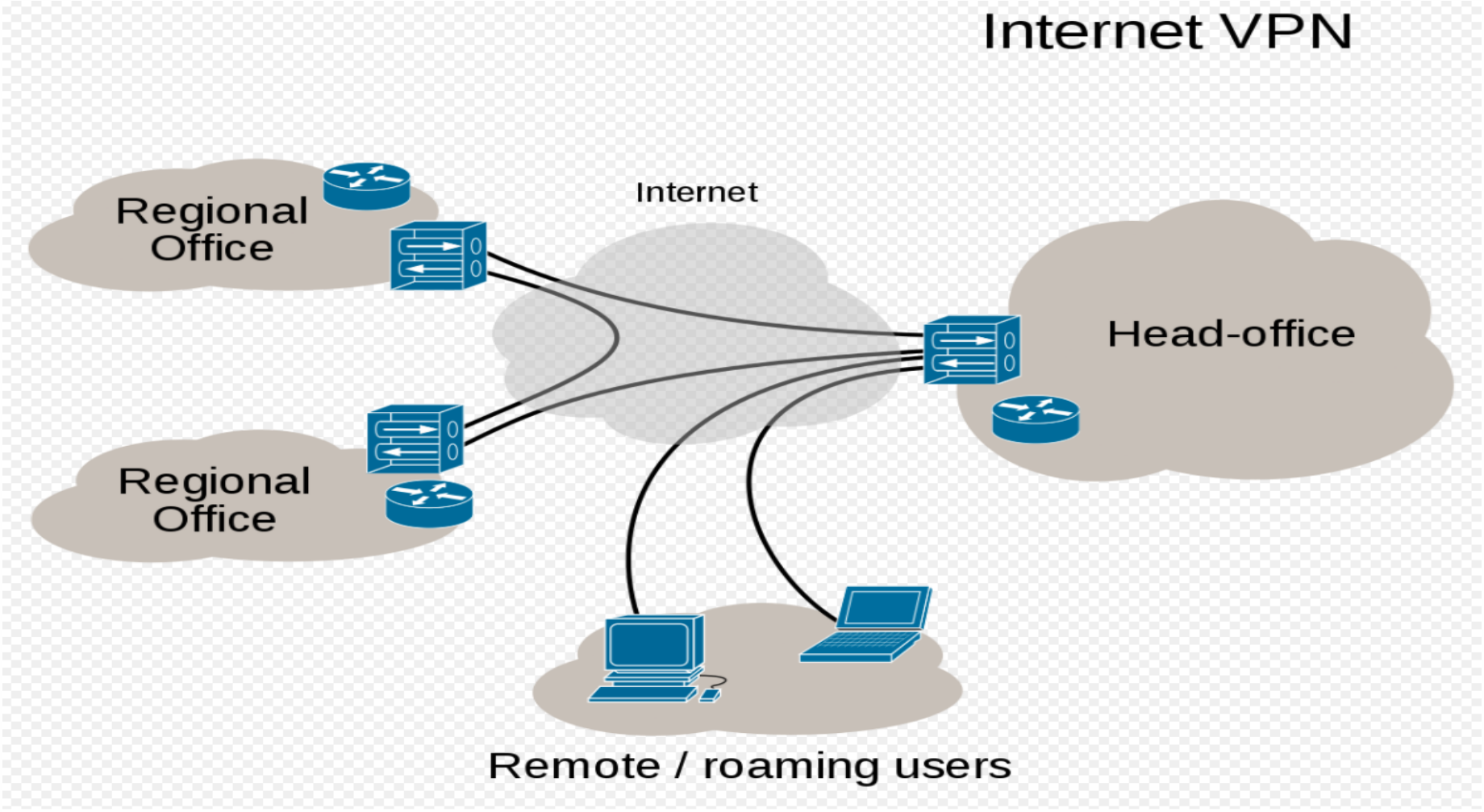
Interno poslovanje

- Interno on-line procesiranje transakcija
- Intranet Web Publishing
- Razmena dokumenata
- Workflow sistemi
- Monitoring
- Kontrola procesa
- Podrška višem menadžmentu

Virtuelna privatna mreža

VPN (енгл. *Virtual Private Network* — **Virtuelna privatna mreža**) je privatna komunikaciona mreža koja se koristi za komunikaciju u okviru javne mreže. Transport VPN paketa podataka odvija se preko javne mreže (npr. Internet) korišćenjem standardnih komunikacionih protokola. VPN omogućava korisnicima na razdvojenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju.

Šema VPN


Internet VPN
Regional Office
Internet
Head-office
Regional Office
Remote / roaming users

Arhitektura VPN

Virtuelna privatna mreža omogućava korisnicima da razmenjuju podatke vezom koja je emulirana kao direktna veza (*point-to-point* link - PPP) između klijenta i servera.
PPP emulacija dobija se enkapsulacijom podataka zaglavljem koje omogućava rutiranje kroz javnu mrežu do odredišta koje je deo privatne mreže. Podaci su šifrovani i paketi koji su presretnuti u okviru javne ili deljene mreže ne mogu se pročitati bez ključa za dešifrovanje. Infrastruktura javne mreže je nebitna jer korisnik logički vidi samo svoj privatni link, odnosno nalazi se logički u lokalnoj mreži, iako je od drugih korisnika razdvojen javnom mrežom.

Tehnologija tunelovanja tunelovanja

- Tunelovanje je najvažnija komponenta tehnologije virtuelnih privatnih mreža i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže.
- Ruteri javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao deo normalnog saobraćaja.
- Tunelovanje ili enkapsulacija je metod pri kome se koristi infrastruktura jednog protokola za prenos paketa podataka drugog protokola. Umesto da se šalju originalni paketi, oni su enkapsulirani dodatnim zaglavljem. Dodatno zaglavlje sadrži informacije potrebne za rutiranje, odnosno usmeravanje paketa kroz mrežu, tako da novodobijeni paket može slobodno putovati transportnom mrežom.

Tunel:

Tunel:

Tunel predstavlja logičku putanju paketa kojom se on rutira preko mreže. Enkapsulirani podaci su rutirani transportnom mrežom sa jednog kraja tunela na drugi. Pojam tunel uvodi se jer su podaci koju putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvorištu i odredištu. Ovi paketi se na mreži rutiraju kao svi ostali paketi.

Početak i kraj tunela nalaze se u VPN mrežama. Kada enkapsulirani paket stigne na odredište vrši se deenkapsulacija i prosleđivanje na konačno odredište. Ceo proces enkapsulacije, transporta i deenkapsulacije paketa naziva se tunelovanje.

Osobine tehnologije tunelovanja

Tehnologija tunelovanja ima osobine čije prednosti značajno doprinose njenoj upotrebi, od kojih su najvažnije:

- Sigurnost – bez obzira što tunel ide kroz nesigurnu javnu mrežu, pristup podacima koji su tunelovani nije dozvoljen neautorizovanim korisnicima što transport čini relativno bezbednim.
- Niska cena – pošto se koriste javne mreže troškovi su dosta niski kada se uporede sa troškovima potrebnim za iznajmljivanje privatnih linija ili implementaciju privatnih Intranet mreža.
- Lakoća implementacije – nema potrebe za promenom postojeće infrastrukture javnih mreža, pa se VPN implementira samo na strani korisnika
- Univerzalnost – zbog enkapsulacije moguće je koristiti i podatke koji pripadaju nerutabilnim protokolima. Takođe se štedi i na broju globalnih IP adresa koje kompanija mora da poseduje, što opet smanjuje cenu implementacije virtuelnih privatnih mreža.

Protokoli koji se koriste pri tunelovanju

Tehnologija tunelovanja koristi tri vrste protokola:

- Protokol nosač - ovi protokoli služe za rutiranje paketa po mreži ka njihovom odredištu. Tunelovani paketi imaju enkapsulaciju ovih protokola. Za rutiranje paketa po Internetu koristi se IP protokol.
- Protokol za enkapsulaciju – ovi protokoli služe za enkapsulaciju originalnih podataka, i koriste se za stvaranje, održavanje i zatvaranje tunela. Najčešće korišćeni su PPTP i L2TP protokoli.
- Transportni protokol – enkapsulira originalne podatke za transport kroz tunel. Najpoznatiji su PPP i SLIP protokol.

Upravljanje

Sa stanovišta upravljanja postoje dva pristupa virtuelnim privatnim mrežama. Razlikujemo VPN kojima upravljaju korisnici, i VPN kojima upravljaju provajderi mrežnih usluga (npr. *Internet Service Provider* - ISP). Virtuelne privatne mreže kojima upravljaju provajderi mrežnih usluga dele se na osnovu toga gde se nalazi oprema koja implementira VPN:

- na strani provajdera (PE - *provider edge*)
- na strani korisnika (CE - *customer edge*).

Bezbednost VPN

Bezbednost je integralni deo VPN usluge.
Postoji veliki broj pretnji VPN mrežama:

- Neovlašćeni pristup VPN saobraćaju
- Izmena sadržaja VPN saobraćaja
- Ubacivanje neovlašćenog saobraćaja u VPN (*spoofing*)
- Brisanje VPN saobraćaja
- DoS (*denial of service*) napadi
- Napadi na infrastrukturu mreže preko softvera za upravljanje mrežom
- Izmene konfiguracije VPN mreže
- Napadi na VPN protokole

Odbrana od VPN napada

Odbrana od VPN napada realizuje se i na korisničkom i na nivou provajdera VPN usluga:

- Kriptozaštita paketa
- Kriptozaštita kontrolnog saobraćaja
- Filtri
- Firewall
- Kontrola pristupa
- Izolacija

- VPN mreže koje koriste Internet ili druge nebezbedne mreže obično koriste razne metode kriptozaštite. Korisnici VPN mreža sa posebnim zahtevima za bezbednost, na primer banke, obično implementiraju i dodatnu infrastrukturu za zaštitu podataka.