

GORNJI SLOJ

Osi model se može podeliti na 2 dela, i to:

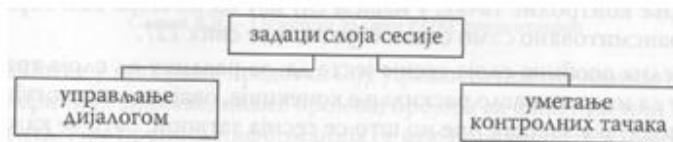
- transparentni deo
- aplikacioni deo.

Transparentni deo sačinjavaju 4 donja sloja OSI modela: fizički sloj, sloj veze, sloj mrže i sloj transporta. Aplikacioni deo sačinjavaju 3 gornja sloja OSI modela: sloj sesije, sloj prezentacije i sloj aplikacije.

Sloj sesije

Termin sesija (session) označava period komuniciranja, tj vođenje dijaloga između procesa. Iako se sloj opisuje kao korisnikov sloj, on je često ugrađen unutar operativnog sistema kao i sistemski softver. Dva osnovna zadatka sloja sesije su:

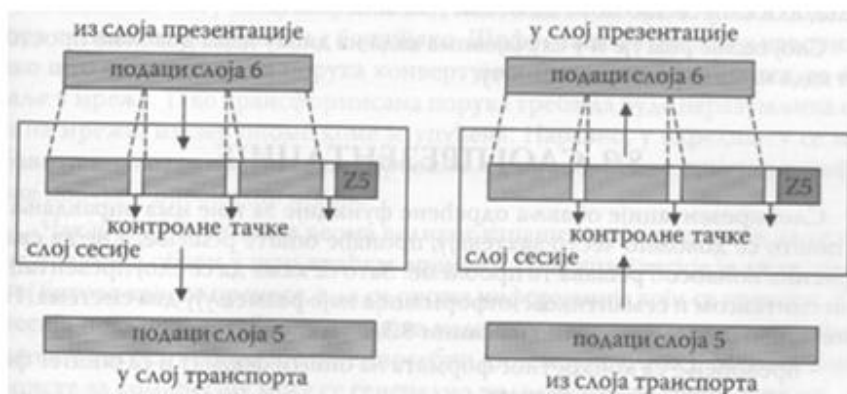
- upravljanje dijalogom
- umetanje kontrolnih tačaka



Jedna od usluga sloja sesije je da upravlja uspostavljanjem, održavanjem i raskidanjem sesije između korisnika i aplikacije, te tako predstavlja neku vrstu regulatora dijaloga, bilo da se radi o poludupleskom ili o dupleskom prenosu. Ako saobraćaj treba da se u datom trenutku odvija samo u jednom smeru, sloj sesije je taj koji vodi računa o tome u kom trenutku koja strana može da se emituje.

Sloju sesije pripada i usluga koja se naziva upravljanje žetonom (*token management*). Za neke protokole je bitno da obe strane ne pokušavaju istovremeno istu operaciju. Da bi se upravljalo ovim aktivnostima, sloj sesije obezbeđuje žetone. Samo ona strana koja poseduje žeton može da izvrši kritičnu operaciju.

Posmatrajmo situaciju do koje može doći kada se prenosi fajl iz jednog računara u drugi, pri čemu se transfer prekine zbog nekog kvara. Pošto je prenos prekinut, trebalo bi komplementan transfer fajla početi iz početka. Da bi se to izbeglo, sloj sesije omogućava da se u poruku unesu kontrolne tačke. Ove tačke se postavljaju na određenom rastojanju.



Još jedna osobina sloja sesije jeste da, za razliku od sloja transporta koji može da izvrši naglo raskidanje konekcije, ovaj sloj onemogućava da se razmena podataka završi pre nego što se sesija zatvori.

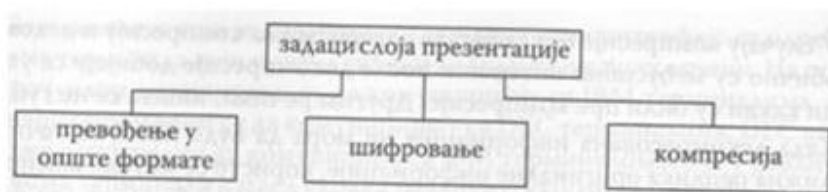
Zato se kaže da sloj sesije obezbeđuje uljudno (graceful) raskidanje sesije. Koliko je ova usluga značajna vidi se iz sledećeg primera:

Neka osoba želi da podigne novac iz bankomata. Ona stavlja svoju karticu u bankomat, zatim unosi svoj PIN, kuca transakciju i koliko novca želi da podigne. Zatim računar proverava ispravnost kartice, PIN i stanje na korisnikovom računu. Kada se svi ovi elementi verifikuju, računar umanjuje stanje na korisnikovom računu za traženi iznos i šalje naredbu bankomatu da korisniku isporuči traženi iznos. Tokom ovog procesa uzimanja novca iz bankomata uspostavljena je sesija sastavljena od čitavog niza različitih poludupleksnih informacija. Predpostavljamo da je baš u trenutku kada je bankomat trebao da dobije naredbu da korisniku isporuči novac došlo do nekog problema (npr. nestanak struje). Korisnikov račun je umanjeno za traženi iznos ali mu novac nije isporučen. To je prednost sloja sesije, jer ne dozvoljava da se transakcija zatvori pre nego što se izvrše svi koraci. To znači da sloj sesije zadržava aržuriranje korisnikovog računa sve dok od bankomata ne dobije informaciju da je korisnik ispaćen. Drugim rečima, sloju transporta dozvoljeno je da se obavi "nešto" od posla, ali sloj sesije mora da se obavi "sve ili ništa".

Sloj prezentacije

Sloj prezentacije se bavi sintaksom i semantikom informacija koje razmenjuju 2 sistema, stoga ovaj sloj je odgovoran za:

- za prevođenje u opšte formate
- za šifrovanje i dešifrovanje
- za kompresiju u dejinoresiju podataka



- Podaci se u programima predstavljaju različitim oblicima: kao nizovi alfanumeričkih znakova, celih brojeva, brojeva sa fiksnom ili pokretnom zapetom... Pri prenosu informacija sa jednog sistema u drugi neophodno je da oni „govore“ istim jezikom. Tj vrši se prevođenje informacija, podaci se prevode u neki opšti format (ASCII, UNICODE). Takav podatak ide na komunikacionu liniju, a zatim se u odredišnom računaru vrši prevodjenje opštog formata u format informacija.

- Neki podaci su od izuzetnog interesa i oni moraju biti zaštićeni od neovlašćenih pogleda drugih korisnika. To su na primer, podaci od banaka ili specijalnih službi (vojska, milicija), zbog toga se ovi podaci šifruju kako bi se onemogućio neovlašćeni pristup. Šifrovanje je utoliko snažnije ukoliko informacija koja se prenosi ima veću težinu.

- Kompresija- većina podataka koje trebamo da distribuiramo kroz mrežu ima zamašnu težinu, na primer, slike, filmovi, audio fajlovi... Da bi se fajlovi koji imaju veliku veličinu lakše prenosili koriste se metode za njihovo sažimanje. Postoje dve osnovne podele za kompresiju podataka, i to:

- kompresija bez gubitka podataka
- kompresija sa gubitkom podataka

Kod prvog tipa stepen kompresije je mali. Prilikom dekompresije podataka, koja je sažeta vraća se u originalan oblik, bez gubljenja podataka. Sa druge strane kod kompresije sa gubljenjem podataka, trajno biva odstranjena određena količina podataka. Ovakav tip sažimanja ima veći stepen kompresije. Uglavnom se koristi kod audio fajlova.

Sloj aplikacije

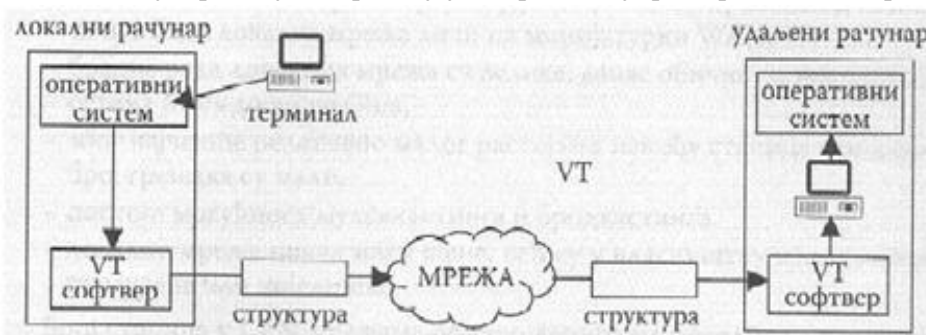
Sloj aplikacije omogućava korisniku da pristupi mreži. Ovaj sloj sadrži sve funkcije koje zahteva korisnik, a to su: e-mail, Remote Desktop Connection, World Wide Web, Use Net, chat... Pored korisničkih aplikacija postoje i nekoliko opštih aplikacija, i to:

- VT (*Virtual Terminal*)
- MHT (*Message Handling System*)
- CMIP (*Common Management Information Protocol*)



Virtual terminal (VT) – predstavlja softversko rešenje za fizički terminal. On ima zadatak da omogući korisniku da se konektuje na udaljeni računar. Prednost VT je što korisnik putem mreže može da se loguje na računar koji je fizički znatno udaljen od korisnikovog računara, pri tome VT prepoznaje udaljeni računar kao svoj sopstveni.

Problem pri kreiranju VT predstavlja različite softverske platforme na koje se vrši logovanje. Da bi se problem prevazišao definišu se opšti virtualni mrežni terminali, odnosno jedan terminal. Ceo softver VT se nalazi u sloju aplikacije. Na posledjoj slici prikazan je princip rada VT, u opštem slučaju.



STANDARDI LOKALNIH MREŽA

- IEEE 802.3 -Ethernet

Lokalne mreže po definiciji predstavljaju mrežu računara koji rade na drugom OSI sloju, odnosno sloju veze.

WAN (*Wireless Arial Network*) je mreža koja radi na trećem OSI sloju, tj sloju mreže. Osnovne karakteristike lokalnih mreža su sledeće:

- u lokalnoj mreži ni jedan računar ne može da se prisilno pokrene, zaustavi ili upravlja radom drugog računara
- sve umrežene stanice uvek su povezane na zajednički medijum, to znači da sve stanice dele propusni opseg medijumu
- brzina rada lokalnih mreža je velika od nekoliko 10-tina Mb/s do nekoliko Gb/s (gigabit po sec). Zbog relativno malog međusobnog rastojanja u mreži kašnjenje i broj grešaka su mali, postoji mogućnost multicasting i broadcasting-a.
- lokalne mreže nikad nisu javne, najčešće su vlasništvo neke ustanove, preduzeće ili pojedinaca
- broj stanica u lokalnoj mreži kreće se od nekoliko do nekoliko stotina računara.

Pošto su lokalne računarske mreže uvek paketske, kod difuznih mreža mora da postoji nekakav mehanizam po kome se dodaje propusni opseg medijuma, tako što svaka stanica može da pristupi medijumu u toku nekog razumnog vremenskog intervala. Na ovaj način se vrši optimizacija iskorišćenja medijuma, sa ciljem da neiskorišćeni medijumi budu na minimumu. Mehanizam pristupa medijumu realizuje se u obliku protokola koji se nalazi u sloju veze. Ranije smo videli da u tom smislu postoji više protokola, i da svi oni imaju prednosti i mane.

Prirodu lokalnih mreža određuju 3 faktora:

1. Medijum kroz koji se obavlja prenos
2. Topologija mreže
3. Protokol za pristup medijumu

Medijum i topologija mreže u najvećoj meri opredeljuju brzine komunikacije. Lokalne mreže mogu da budu žične i bežične, to znači da mogu da rade u osnovnom i u transportovanom opsegu učestanosti. Lokalne mreže najčešće koriste upredenu paricu kao medijum za prenos zbog niske cene. Upredena parica se koristi za mala rastojanja (*maximum 100m*), za veća rastojanja koriste se koakscioni kablovi. On je kvalitetniji i omogućava prenos informacija u osnovnom i transportovanom opsegu učestanosti. Koakscioni kabel takođe koristimo za rad u širokopojasnom opsegu učestanosti. Jasno je da su lokalne mreže koje rade u osnovnom opsegu učestanosti jeftinije od lokalnih mreža koje rade u transportovanom opsegu učestanosti. Ovde treba imati u vidu i kašnjenje signala usled konačne brzine prostiranja. Zbog toga je aproksimativno ustanovljeno da su širokopojasne (*transportne*) mreže 2 puta brže od osnovnih (*uskopojasnih*).

Sa druge strane kada su potrebne veoma velike brzine i velika širina propusnog ospega koristi se optički kabel (optičko vlakno). On ima daleko veći kapacitet od koakscionog kabela. Problem kod optičkih kablova je cena koštanja i montaža, jer su troškovi postavljenja veoma veliki. U poslednje vreme aktuelne su i bežične lokalne mreže sa porastom broja prenosivih računara, raste i potreba za bežičnim umrežavanjem. Na ovaj način korisnik koji ima odgovarajući modem odnosno mrežnu karticu, može lako

da se poveže sa lokalnom mrežom. Za komunikaciju bežičnim putem koristi se radio signali ili infracrveni zraci.

- Mrežni operativni sistemi

Mrežni operativni sistemi (MOS) se dele u dve osnovne grupe, i to na:

- mrežne operativne sisteme koji se koriste u ravnopravnim mrežama (peer-to-peer networking operating system)
- klijent-serverske mrežne operativne sisteme (client-server network operating system)

Mrežni operativni sistemi prema lokalnoj mreži mogu biti:

- lokalne mreže ravnopravnih računara
- klijent-server lokalne mreže.

- Ravnopravne lokalne mreže

- Svaki PC može da radi i kao klijent (da traži informacije) i kao server (da pruža informacije). Npr, ako je u ovakvoj mreži instaliran samo na jednom računaru neki programski paket (recimo Windows Word), onda ovaj program mogu koristiti i sve ostale umrežene stanice. Ovakav sistem je pogodan u malim preduzećima i organizacijama.

- Peer-to-peer mreža može se realizovati bilo u obliku 10BaseT mreže ili tankog eterneta. Na 10BaseT mreži može da se poveže do 16 stanica koje nisu mnogo udaljene, neke od njih mogu biti portbl računari koji mogu privremeno da se isključe.

U većini peer-to-peer MOS-a korisnici mogu da odrede koje svoje resurse da stavljaju na raspolaganje ostalim korisnicima. Peer-to-peer MOS ima prednosti u odnosu na klijent-server MOS, i to:

- nije potreban administrator mreže
- podešavanje i održavanje mreže je jednostavno, pa samim tim i jeftino
- svaki računar može da napravi rezervnu kopiju na drugim računarima i da tako poveća sigurnost podataka

- Klijent-server lokalne mreže

U ovoj konfiguraciji, za razliku od peer-to-peer konfiguracije, informacije su centralizovane. To znači da sve informacije koje se nalaze na serveru dostupni su svim klijentima. Administrator mreže preko MOS da dodeli korisnicima različite nivoe prioriteta pri korišćenju resursa, npr, neki korisnici mogu samo da pregledaju a neki ne mogu da menjaju saržaj fajlova, dok se drugima to dozvoljava.

Klijent-serverski MOS treba da obezbedi pouzdanost, bezbednost, i fleksibilnost mrežnog povezivanja i da omogući brzo rekonfigurisanje, kako hardvera tako i softvera i to bez mogućnosti prekida rada.

Klijent-serverski MOS dobar je za velike organizacije kojima je potreban brz mrežni pristup i operacije nad bazama podataka, tabelama, kao i video i multimedijalni pristup.

- Serverski programi

Serveri i klijenti mogu biti i računari i programi. Serverski program je program kome preko mreže klijent traži nekakav zahtev, pa serverski program postupa po zahtevu klijenta i šalje mu odgovor.

Serverski programi su:

- DNS (Domain Name System) koji se koristi za preslikavanje simboličnih imena računara u IP adrese
- DHCP (Dynamic Host Configuration Protocol), to je softver koji se stvara u serverima i ruterima i

automatski dodeljuje privremene IP adrese klijent stanica u IP mreži

- mail server, itd...

Žične lokalne mreže

Žične lokalne mreže realizuju se najčešće u obliku zvezde, ređe u obliku magistrale ili prstena. Mreže u obliku zvezde definisane su standardom IEEE 802.3, dok su mreže u kojima se pristup obezbeđuje pomoću žetona definisani standardima IEEE 802.4.

Danas se najčešće sreće ethernet mreže tj mreže koje definiše IEEE 802.3 standard.

ZAŠTITA PODATAKA NA MREŽI

Internet bezbednost (*IS – Internet Security*) je širok pojam koji se odnosi na zaštitu računara i računarskih mreža koje su povezane sa internetom. Sistemi za bezbednost (*ISS – Internet Security System*) su uređaji ili softveri koji su razvijeni i svakim danom se sve više i više usavršavaju, kako bi se zaštitili interesi zloupotrebe putem interneta.

Internet po svojoj prirodi nije bezbedna sredina, jer je to otvorena računarska mreža koja služi za laku razmenu informacija. Podaci putuju kroz veliki broj niz računara i linkova, zbog toga zlonamernici i hakeri mogu da se presretnu sa tom porukom i da je promene.

- Najpoznatiji problemi su virusi. Neki od njih u korisnikovom računaru modifikuju programe i tako ih čine ne upotrebljivim, dok drugi oštećuju i uništavaju podatke.

Radi zaštite od virusa razvijeno je mnogo anti-virus programa, koji se svakim danom sve više i više usavršavaju.

- Hakeri se najčešće trude da neovlašćeno uđu u korisnikov računarski sistem i da tako iz unutra menjaju ili krađu informacije. Takođe, pokušavaju da dodju i do lozinke korisnika tako što se trude da pogode lozinku ili koriste programe koje hvataju informacije o lozinci.

- Poseban problem predstavljaju i špijunski programi (*spyware*). To je softver koji se na prevaru instalira u korisnikov računar i da bez znanja vlasnika računara prikuplja informacije o korisniku. Špijunski programi se brzo ugnezde u korisnikov računar, i to obično tokom surfovanja i skidanja podataka na veb sajtovima.

- Jedan od većih problema je i neželjena elektronska pošta tj. spam (obično su to reklamne poruke). Pošto se ove poruke šalju u ogromnim količinama i ogromnom broju korisnika, spamovi znatno usporavaju mrežu i korisnikov računar. U spamovima su namerno ili ne namerno ugrađeni i virusi. Zato je preporučljivo da se ne otvaraju elektronske pošte ako se ne poznaje pošaljilac. Za borbu protiv spamova razvijeni su anti-spam softveri. Ovi softveri odbacuju sve poruke za koje utvrde da predstavljaju spam, tako što ih trajno briše ili ih premešta u *spam folder*.

- Ima više načina da se spreči pristup računarima ne ovlašćenim licima. Najčešća je metoda šifrovanja (postavljanja lozinke). A pošto lozinka može da se ukrade ili da se pogodi, postoje i savremenije metode provere da li je osoba koja traži pristup zaista ovlašćena, to je u stvari softver za prepoznavanje glasa, sistem za skeniranje zenica, i sistemi za prepoznavanje rukopisa.

Jedan od najefikasnijih načina zaštite računarske mreže je zaštitni zid, odnosno mrežna barijera (*firewall*). To je hardverski bezbednosni uređaj koji se postavlja između računarske mreže i interneta.

- Zaštitni zid

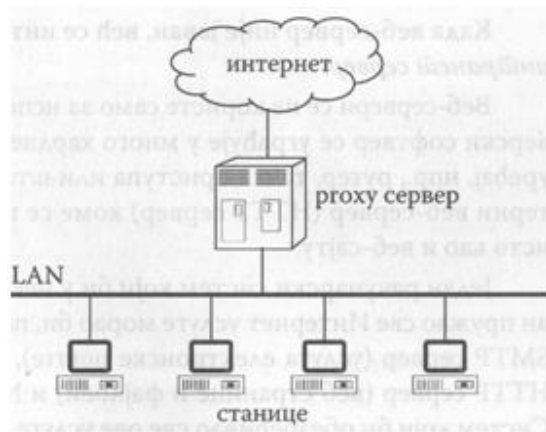
Zaštitni zid (*firewall*) je bezbednosni sistem koji kontroliše protok podataka iz jedne mreže u drugu mrežu. Glavna namena zaštitnog zida je da zaštiti podatke privatne mreže, tako što ne dozvoljava korisniku spoljne mreže (posebno preko interneta) da im pristupi.

Zaštitni zid se veoma mnogo koristi i predstavlja osnovnu bezbednost, jer sa jedne strane omogućava korisnicima bezbedan pristup internetu, a sa druge strane odvaja javni veb server preduzeća od njegove interne mreže.

U kućnim računarima zaštitni zid je instaliran u korisnikovim računarima. Zaštitni zid je ugrađen u operativne sisteme: Windows XP, Windows Server 2003, Windows Vista, i Windows 7.

U organizacijama zaštitni zid je samostalan računar ili softver u ruteru ili serveru. To praktično može da bude ruter koji odbacuje neželjene pakete ili može da bude kombinacija rutera i servera pri čemu svaki od njih obavlja određenu vrstu zadataka.

- Proxy server



Proxy server (skraćeno *proxy*) ima zadatak da spreči neovlašćenom licu da upadne u privatnu mrežu. Proxy server je računar ili ruter koji radi između klijenta i servera, tako što raskida vezu između prijemnika i predajnika.

Kao što i sam naziv kaže proxy server radi po ovlašćenju klijenta i servera. Svaki zahtev klijenta koji je upućen serveru i koji se nalazi na internetu ide pravo na proxy server, proxy server ga procenjuje, a zatim ga propušta na svoj izlazni port ka internetu. Isto tako, odgovor ili zahtev koji stiže sa interneta ide prvo na

procenu u proxy server. Pa onda i klijent i server imaju utisak da zajedno komuniciraju međusobno, a u stvari svaki od njih komunicira sa proxy serverom.

Dakle, proxy server je poveztan u dve mreže, pa ima dve IP adrese. Internet vidi IP adresu sa strane proxija, dok stanica koja šalje zahtev ostaje skrivena za spoljni svet.

Proxy serveri se često koriste zajedno sa NAT (Network Address Translation) softverom.

- Mail server

Internet sistem elektronske pošte (SMTP – Simple Mail Transfer Protocol) se zasniva na principu proxy servera. Elektronska pošta ne šalje se direktno od pošaljioaca do primaoca, već prvo ide na mail server.

Mail server je računar ili softver koji u mreži obavlja poštanske poslove.

Dva najpoznatija standardna interfejsa između e-mail klijenta i mail servera su:

- POP3 (Post Office Protocol 3) i
- IMAP4 (Internet Message Access Protocol 4)

Ove protkole koriste klijenti za slanje elektronske pošte u mail server i da primaju elektronsku poštu iz mail servera.

- Web server

Web server je računar ili softver koji prihvata HTTP zahteve koji stižu od klijenta i vraća im HTTP odgovor u obliku HTML dokumenta.

Kada veb server nije javan već se interno koristi onda se on naziva interni server.

Web-serveri se ne koriste samo za isporučivanje web-stranica, oni se ugrađuju u mnogo hardverskih uređaja. Bilo koji mrežni uređaj (npr, ruter, štamparski server...) može imati interni web-server, i njemu se pristupa preko IP adrese, isto kao i web-sajtu.

Jedan računarski sistem koji u nekom preduzeću ili ustanovi ima sve internet usluge, obavezno bi morao da sadrži:

- SMTP server (usluga elektronske pošte)
- FTP server (skidanje fajlova-download)
- HTTP server (web-stranice i fajlovi)
- NNTP server (diskusione grupe)

Sistem koji bi obezbedio sve ove usluge naziva se Web-server.